10TH ITU ACADEMIC CONFERENCE

ITU KALEIDOSCOPE
SANTA FE 2018

Machine learning for a 5G future

26-28 November
Santa Fe, Argentina

Hosted by

Technically co-sponsored by

Supported by

Organized by

10TH ITU ACADEMIC CONFERENCE

ITU KALEIDOSCOPE
SANTA FE 2018

Machine learning for a 5G future

26-28 November
Santa Fe, Argentina

In partnership with

Hosted by

Technically co-sponsored by

Supported by

Organized by

IEEE Catalogue Number: CFP1868P-ART

ISBN:
978-92-61-26921-0 (electronic version)

Disclaimer

The opinions expressed in these Proceedings are those of the paper authors and do not necessarily reflect the views of the International telecommunication Union or of its membership.

Foreword

Chaesub Lee
Director
ITU Telecommunication Standardization Bureau

ITU Kaleidoscope academic conferences have gained a reputation for addressing 'frontier' topics of growing strategic relevance to ITU membership. Kaleidoscope 2018: *Machine Learning for a 5G Future* exemplified this focus on the future.

Kaleidoscope is ITU's flagship academic event. Now in its tenth edition, the conference supports productive dialogue between academics and standardization experts. I would like to express my gratitude to the Universidad Tecnológica Nacional for stimulating this dialogue as the host of Kaleidoscope 2018 in Santa Fe, Argentina, 26-28 November 2018.

In presentations of academic research on Machine Learning, tutorials on breakthroughs in the field, and the future-looking 'Jules Verne's corner', Kaleidoscope 2018 investigated the development and application of Machine Learning from the perspectives of technology as well as society, law, economics and ethics.

The conference showcased research into Machine Learning's ability to support the smarter use of network generated data, highlighting new opportunities for network operators and service providers to adapt to changes in traffic patterns, security risks and user behavior. These discussions proved of great benefit to ITU's analysis of Machine Learning's expected contribution to ITU standards in areas such as coding algorithms; data collection, storage and management; and network management and orchestration.

I would like to express my great appreciation to the Kaleidoscope community and the larger ITU Academia membership for their enduring support to this series of conferences. With over 150 academic and research institutes now members of ITU, the Kaleidoscope series is certain to continue growing in strength.

My sincerest thanks go to the hosts of Kaleidoscope 2018, the Modernization Government Secretariat of Argentina, the Government of the Province of Santa Fe and the Universidad Tecnológica Nacional, Santa Fe Regional Faculty; our technical co-sponsors, the Institute of Electrical and Electronics Engineers (IEEE) and the IEEE Communications Society; our supporters, the Santa Fe Lottery and NEC; our partners, Waseda University, the Institute of Image Electronics Engineers of Japan, the Institute of Electronics, Information and Communication Engineers of Japan, the Chair of Communication and Distributed Systems at RWTH Aachen University, the European Academy for Standardization, and the University of the Basque Country; our local partners, Comisión Técnica Regional de Telecomunicaciones, Comisión Interamericana de Telecomunicaciones, Centro Internacional de Investigación Científica en Telecomunicaciones, Tecnologías de la Información y las Comunicaciones, Corporación Universitaria para el Desarrollo de Internet, Centro de

Capacitación en Alta Tecnología para Latino América y el Caribe, Universidad Austral, Universidad de Buenos Aires, Universidad de Cuenca, Universidad de Las Américas, Universidad Distrital Francisco José de Caldas, Universidad ICESI, Universidad Nacional de la Plata, Universidad Nacional de Río Cuarto, Universidad Nacional de San Luis, and Universidad Nacional del Sur; and our media partners, Convergencia Latina and the Journal of Big Data and Cognitive Computing.

I would especially like to thank the devoted members of the Kaleidoscope 2018 Steering Committee and Technical Programme Committee, in particular the distinguished General Chairman of Kaleidoscope 2018: Rudy Omar Grether, Dean of the Regional Faculty of Santa Fe, Universidad Tecnológica Nacional, Argentina.

Chaesub Lee
Director
ITU Telecommunication Standardization Bureau

Chairman's Message

Rudy Omar Grether
General Chairman

The growing ability of Machine Learning to bring more automation and intelligence to communications networking has become a very exciting area of research, with potential to generate significant value for the networking industry.

Universidad Tecnológica Nacional is proud to have offered a platform to explore this research at Kaleidoscope 2018: *Machine Learning for a 5G future* in Santa Fe, Argentina, 26-28 November 2018.

The establishment of the ITU Academia membership category in 2011 brought greater significance to Kaleidoscope's role in fostering academic engagement in the work of ITU.

The occasion of Kaleidoscope 2018 marked the 10th anniversary of the Kaleidoscope series of conferences, a tradition that Universidad Tecnológica Nacional will continue to support as an ITU Academia member.

Kaleidoscope 2018 approached its discussions from a wide variety of perspectives, incorporating research from technical as well as social sciences.

The Technical Programme Committee chaired by Mostafa Hashem Sherif selected 15 papers from a total of 47 submissions. Papers were selected through a double-blind, peer-review process supported by 83 international experts. I would like to thank the Committee and the reviewers for selecting high-caliber papers for presentation at the conference and identifying papers eligible for awards.

Our distinguished keynote speaker, Hugo Miguel, representing Argentina's Modernization Government Secretariat, shared insight into the planned deployment of emerging 5G systems in Argentina and the Latin-American region at large, including a special focus on public-sector interest in Machine Learning.

The first Kaleidoscope 2018 invited paper, "*A Machine Learning Management Model for QoE Enhancement in Next Generation Wireless Ecosystems*", was presented by Eva Ibarrola (University of the Basque Country-UPV/EHU, Spain). The paper explored possible methodologies to develop a global Quality of Service management model for next-generation wireless ecosystems exploiting Machine Learning and Big Data. The second invited paper, "*Machine Learning Opportunities in Cloud Computing Data Center Management for 5G Services*", presented by Benjamín Barán (National University of the East, Paraguay) and co-authored with Fabio López-Pires (Itaipu Technological Park, Paraguay), focused on opportunities for applications of Machine Learning to improve critical resource-management decisions, considering in particular resource management for data centres supporting cloud computing.

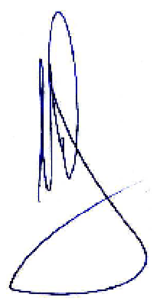
This year's 'Jules Verne's corner' addressed "*The Future of Work and the Future of Privacy in the Era of Artificial Intelligence*", exploring how jobs and privacy will be impacted by Machine Learning and potential strategies to ensure the emergence of a human-centric future technology environment. This dynamic special session was moderated by Ana Rosa Tymoschuk (Secretary of Science and Technology, Universidad Tecnológica Nacional, Facultad Regional Santa Fe, Argentina). Among the panelists, Erica Hynes (Minister of Science, Technology and Productive Innovation, Santa Fe, Argentina) and María Laura Spina (Universidad Tecnológica Nacional, Santa Fe, Argentina).

The Kaleidoscope 2018 programme included also three Tutorials. The first one on "*Artificial Intelligence: pros and cons*" was organized and run by Maria de los Milagros Gutiérrez, Luciana Ballejos and Maria Guadalupe Gramajo (CIDISI Research Center, Universidad Tecnológica Nacional, Argentina). The second one on "*Pattern recognition*" was organized and run by Juan Pablo Martín (Universidad Tecnológica Nacional, Facultad Regional San Nicolás, Argentina). The third one on "*Can artificial intelligence give a mind to machines?*" was organized and run by Hugo Leonardo Rufiner (Universidad Nacional del Litoral, Argentina).

Selected papers from each year's Kaleidoscope conference are considered for publication in a special-feature section of IEEE Communications Standards Magazine. In addition, special issues of the International Journal of Technology Marketing (IJTMKT), the International Journal of IT Standards and Standardization Research (IJITSR) and the Journal of ICT Standardization may publish extended versions of selected Kaleidoscope papers. Authors of outstanding Kaleidoscope 2018 papers have also been invited to contribute to the work of the ITU Focus Group on 'Machine Learning for Future Networks including 5G'.

All papers accepted and presented at the conference will be published in the IEEE *Xplore* Digital Library. The Conference Proceedings from 2009 onwards can be downloaded free of charge from http://itu-kaleidoscope.org.

I would like to thank our technical co-sponsors, supportive partners and Alessia Magliarditi and her team at the ITU for their role in ensuring the continued success of the Kaleidoscope series of academic conferences.



Rudy Omar Grether
General Chairman

TABLE OF CONTENTS

Page

COMMITTEES

Steering Committee

- General Chairman: Rudy Omar Grether (Universidad Tecnológica Nacional, Argentina)

- Héctor Mario Carril (ITU-T Study Group 20 Vice-Chairman, Argentina)
- Christoph Dosch (ITU-R Study Group 6 Vice-Chairman; IRT GmbH, Germany)
- Kai Jakobs (RWTH Aachen University, Germany)
- Mitsuji Matsumoto (Waseda University Emeritus Professor, Japan)
- Mostafa Hashem Sherif (Consultant, USA)

Host Committee

- Chairman: Alfonso Pablo Trevignani (Universidad Tecnológica Nacional, Argentina)

- Diego Angelo Bolatti (Universidad Tecnológica Nacional, Argentina)
- Walter Daniel Justet (Universidad Tecnológica Nacional, Argentina)
- Juan Pablo Martín (Universidad Tecnológica Nacional, Argentina)
- María Celeste Weidmann (Universidad Tecnológica Nacional, Argentina)

Secretariat

- Alessia Magliarditi, ITU Kaleidoscope Coordinator

- Erica Campilongo, Collaborator and Coordinator of Jules Verne's corner and Exhibit
- Nolwandle Simiso Dlodlo, Collaborator
- Emer Windsor, Administrative Assistant
- Pablo Palacios Ochoa, Liaison Officer
- Pascal Borde, Promotional support

Technical Programme Committee

- Mostafa Hashem Sherif (Consultant, USA)

- Marcelo Francisco Abbade (Universidade Estadual Paulista, Brazil)
- Ahmed M. Abdelmoniem (Faculty of Computers and Information, Assiut University, Egypt & Hong Kong University of Science and Technology, Hong Kong)
- Marco Ajmone Marsan (Polytechnic University of Turin and Institute IMDEA Networks, Italy)
- Eyhab Al-Masri (University of Washington, USA)
- Saad Mohammed Ali Taher Al-Momen (Baghdad University, Iraq)
- Waslon Terllizzie Araujo Lopes (Federal University of Paraíba, Brazil)
- Chaodit Aswakul (Chulanlongkorn University, Thailand)
- Luigi Atzori (University of Cagliari, Italy)
- Antoine Bigomokero Bagula (University of the Western Cape, South Africa)
- Paolo Bellavista (University of Bologna, Italy)
- Robert Birke (ABB Corporate Research, Switzerland)
- Michael Bove (Massachusetts Institute of Technology, USA)
- Dario Bruneo (University of Messina, Italy)
- Ryan Budish (Berkman Klein Center for Internet & Society, Harvard University, USA)
- Carlos Caicedo Bastidas (Syracuse University, USA)
- Ke-Jia Chen (Nanjing University of Posts and Telecommunications, China)
- Mingzhe Chen (Beijing University of Posts and Telecommunications, China
- Luca Chiaraviglio (University of Rome Tor Vergata, Italy)
- Sungrae Cho (Chung-Ang University, Korea)
- Laizhong Cui (Shenzhen University, China)
- Nhu-Ngoc Dao (Chung-Ang University, Korea)
- Fabrizio De Vita (University of Messina, Italy)
- Nathalie Devillier (Grenoble Ecole de Management (GEM), France)
- Christoph Dosch (ITU-R Study Group 6 Chairman; IRT GmbH, Germany)
- Tineke Mirjam Egyedi (Delft University of Technology, The Netherlands)
- Erwin Folmer (University of Twente, The Netherlands)
- Ivan Ganchev (University of Limerick, Ireland / University of Plovdiv "Paisii Hilendarski", Bulgaria)
- Joan Garcia-Haro (Universidad Politécnica de Cartagena, Spain)
- Shravan Garlapati (Qualcomm Technologies Inc., USA)
- Katja Gilly (Miguel Hernandez University, Spain)
- Jairo A. Gutierrez (Auckland University of Technology, New Zealand)
- María de los Milagros Gutiérrez (Universidad Tecnológica Nacional Facultad Regional Santa Fe, Argentina)

- Eva Ibarrola (University of the Basque Country, Spain)
- Filip Idzikowski (Poznan University of Technology, Poland)
- Kai Jakobs (RWTH Aachen University, Germany)
- Wei Jiang (German Research Center for Artifitial Intelligence (DFKI GmbH), Germany)
- Ved P. Kafle (National Institute of Information and Communications Technology, Japan)
- Tim Kelly (World Bank, USA)
- Ateeq Khan (Otto von Guericke University Magdeburg, Germany)
- Katarzyna Kosek-Szott (AGH University of Science and Technology, Poland)
- Ken Krechmer (IEEE, USA)
- Dhananjay Kumar (Anna University, India)
- Andreas Kunz (Lenovo, Germany)
- Nam-Tuan Le (Kookmin University, Korea)
- Fidel Liberal (University of the Basque Country, Spain)
- Lu Liu (Illinois Institute of Technology, USA)
- Giovani Mancilla (Universidad Ditrital, Colombia)
- Arturas Medeisis (ITU Arab Office, Riyadh station)
- David Meyer (University of Oregon, USA)
- Luzango Mfupe (Council for Scientific and Industrial Research (CSIR), South Africa)
- Ahmed Mohammed Mikaeil (Shanghai Jiao Tong University, China)
- Kazuhide Nakajima (NTT Corporation, Japan)
- Carlos Natalino (KTH Royal Institute of Technology, Sweden)
- Jimmy J. Nielsen (Aalborg University, Denmark)
- David Palma (Norwegian University of Technology and Science, Norway)
- Jordi Pérez-Romero (Universitat Politècnica de Catalunya (UPC), Spain)
- Benedetta Picano (University of Florence, Italy)
- Gerard Pogorel (Telecom ParisTech ENST, France)
- Antonio Puliafito (University of Messina, Italy)
- Alexander Raake (Technische Universität Ilmenau, Germany)
- Aravinda S. Rao (The University of Melbourne, Australia)
- Mattia Rebato (Università degli Studi di Padova, Italy)
- Anna Riccioni (Università degli Studi di Bologna, Italy)
- Werner Robitza (Ilmenau University of Technology, Germany)
- Mihoko Sakurai (Keio University, Japan)
- Oriol Sallent (Universitat Politècnica de Catalunya, Spain)
- Mostafa Hashem Sherif (Consultant, USA)
- Minrui Shi (Shanghai Telecom, China)
- Ardy Siegert (Ardytectuur, The Netherlands)

- William Simpson (Institute for Defense Analyses, USA)
- Antonio Skarmeta (University of Murcia, Spain)
- Niek Tax (Eindhoven University of Technology, The Netherlands)
- Christian Timmerer (Information Technology (ITEC) Alpen-Adria-Universität Klagenfurt, Austria)
- Elias Tragos (NUI Galway and FORTH, Ireland)
- Manuel Urueña (Universidad Carlos III de Madrid, Spain)
- Taavi Valdlo (Estonian IT Standardization Technical Committee, Estonia)
- Vino Vinodrai (McMaster University & Vinodrai & Associates Inc, Canada)
- Junhua Wang (Chongqing Universtiy, China)
- Remy Wehbe (Virginia Tech, USA)
- Jinsong Wu (Universidad de Chile, Chile)
- Maria Gabriella Xibilia (University of Messina, Italy)
- Zhaohui Yang (Southeast University, China)
- Bo Yin (Illinois Institute of Technology, USA)

KEYNOTE SUMMARY

IMPACT OF MACHINE LEARNING IN 5G PLANNING AND DEPLOYMENT

Hugo Miguel

Under Secretary of Planning, Information and Communications Technologies (ICT) Secretariat, Modernization Government Secretariat, Argentina

4G-deployed infrastructures generate metadata provided by phone registrations systems. This data provides the possibility to predict the behavior of users and the ways that devices are used throughout the day. The definition of a metadata model and the design of artificial intelligence tools with learning has the ability to exploit data and to provide a sample of the type of traffic and demand of services that the user will request in each location visited. With this model we can predict the type of demand needed to support the design of 5G networks.

Keywords – 5G, artificial intelligence, learning, network

Why machine learning?

Machine learning (ML) is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence (AI) based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention.

The core of the issue is the determination of patterns to be identified from 4G network activity as a source of data to determine the behavior of the network as a system and the users as components, with their own will that could modify the needs of services based in their activities.

An extraordinary amount of data is obtained in the exchange of information produced between the network and the user's devices. This scenario gives us the source of different kinds of information that we could combine to obtain conclusions.

Over the system analyzed we must consider multiple variables that we can measure and register from the logs that perform the processes of user registration, calls, hand over, IP assignment, flow of data, and others.

The correlation between the multiple variables we are managing in a single analysis cannot be done without the use of computational aid.

We are looking for patterns that we do not know of, and we need to discover, so the process of learning from this repository of data is a new challenge because at the beginning of the process we have no idea what relationship we are searching for.

The analysis along the timeline reveals the changes in the system and gives us an image of the activities developed on the network, based on the change of values of each variable.

In this scenario, we need the support of machine-learning algorithms to detect and identify the patterns on the network subject to analysis.

What type of machine learning models will be used with applications?

The model of learning will change at each stage of the work; the first step will be the use of the "Supervised" model to validate the calculus that could predict values in a previous model like bandwidth occupation, channel capacity or radio propagation; in this case, the variables must have been identified and labeled previously.

Other searches for patterns will be “Unsupervised”. In these cases, we have no information about the exits that the systems could bring, an example of this are the models of congestion because the call is an aleatory event with no previous information about the channel status.

How do we use machine learning in 5G planning and deployment?

5G is a change of concept in mobile services; this new concept will assume new frequencies to provide different kinds of services routing communications based on the speed needed for the service looking to obtain the maximum performance combining coverage, propagation and the penetration bandwidth compatible with the kind of service to be used. This service will combine different techniques such as frequency allocation, carrier aggregation or MIMO (multiple in multiple out) as an example.

The knowledge obtained from 4G analysis performs the basis for the 5G model.

To design the new model the definition of segmented models is highly significant, where we will test the obtained predictive functions, testing the needs of coverage and based on service areas and demand of services.

Once the type of demand of service can be managed by changing the variable values, we will introduce new frequencies and services looking for the reinforcement of services in the mapped areas where the model shows there is a lack of services.

The definition of this new model gives us the opportunity of introducing two new learning algorithm types, such as reinforcement learning. This introduces feedback to correct and learn the ways to optimize selected variables and to multitask the learning of algorithms using homologous theory where the system learns over other solutions obtained in the past based on similar conditions.

Once this kind of model has been developed, we could develop Bayesian networks to predict the most probable behavior of the designed network.

Network deployment using this tool will allow the measuring of the values predicted for the system and the values obtained will be used to provide feedback to the systems providing new entrances to validate the model and reinforce the learning capabilities of the system based in machine learning.

It is very important to define the scenario of where we are working, starting with the definition of the components of the system identifying the variables with incidence in the work with the functions that predict the behavior of these variables.

All these variables with an undefined standard set of values or logical status will be played using Montecarlo models, Markov chains or other statistical sources, based in the universe of the variable and its statistical patterns.

The use of described techniques will provide three stages of learning: “Grow”, learning from the environment; “Restructuring”, learning from corrections and obtaining new knowledge form this action; and adjustment generalizing concepts and adjusting from the values obtained from the experience sensing of the real world.

5G will need a great quantity of sites with different frequencies and services. This situation will create a complex and multivariable scenario.

Machine learning gives us the tools to define the patterns in this multivariable scenario, showing even those patterns for which we do not know of their existence.

This planification, testing adjustment and network deployment, looking for the better balance between power, height of antennas, location and density of the network crossed with the aleatory demand of services in the universe of individual users and types of devices could not be solved without described tools.

The information obtained from network deployments is being stored and represented in a space data infrastructure, able to show the coverage and availability of each service with their technical parameters.

Once this system has been completed, we will have a tool to evaluate scenarios in terms of frequency, power and geographical information giving us the basis for further simulations and model validation.

Concerning the application of this vision as a tool to plan spectrum use and occupancy we are at an early stage collecting and organizing data sets that we need for exploiting data reservoirs.

The use of geographical interfaces gives us the opportunity to plot different patterns obtained from propagation calculus and contrasted by collaborative sensing provided by handhelds with software applications.

Data ownership regulations

An important issue in all the processes related with AI and ML techniques is of raw data ownership.

The ICT Secretariat is analyzing the type of regulation needed to maximize the use of the raw data produced by telecommunication systems as a part of the systems' work, without the requirement for user consent.

We also have the data produced by software applications which are able to capture information from the telecommunications system which have the previous consent of the user.

The difference between the data sources is data ownership because the idea is to promote data sharing to enable algorithm development.

Data is the fuel of this new ecosystem; that is why we think the government must ensure data availability to produce different initiatives to provide results from looking for new patterns and conclusions in the minimum amount of time.

Data availability will expand innovation in AI development.

The definition of regulation that preserves user privacy is very important for expanding the use of these tools for assuring the user's rights.

It is very important that the definition and registration of variables that can be collected from the different communication systems as a part of the system log, each variable registered combined with any device positioning, will provide us the opportunity to know the different correlations between multiple variables, defining the system's behavior.

The ICT Secretariat is strongly involved in the regulatory definitions that could promote data availability and information sharing because these actions will promote the growth in the marketplace.

Artificial intelligence and machine learning in other national policies

Argentina's Government is encouraging the use of AI and ML to improve actions in several industries, such as energy, telecommunications, transport and agriculture; the use of this technology in these areas will provide the initial scenarios to base the roots of a new economy on.

The ICT Secretariat develops new policies on the Internet under the Direction of Internet and New Technologies, and the Direction of Economic Regulation and Competition studies the impacts of these new applications.

To promote the adoption of emerging technologies, Argentina has a network of public and private institutions studying AI and ML technologies. As an example of institutions that work in this area, the following list shows those related with CONICET (National Council of Science and Technology) that work under the umbrella of the Science and Technology Ministry.

Organization	Role
Centro Científico Tecnológico CONICET Cordoba (CCT-CONICET-CORDOBA)	Advice on the design of applications of natural language processing and machine learning.
Centro de Investigación y Estudios de Matemática (CIEM)	The center works on the analysis of images and video through computer-vision techniques and automatic learning.
Centro Internacional Franco Argentino de Ciencias de la Información y de Sistemas (CIFASIS)	The center works on the development of applications that use automated learning and/or computer vision.
Instituto de Ciencias de la Computación (ICC)	Advice on topics related to artificial intelligence, machine learning, neurosciences and applied High Performance Computing (HPC).
Instituto de Tecnologías y Ciencias de la Ingeniería "Ing. Hilario Fernández Long" (INTECIN)	Provides counseling in data sciences and predictive modeling of technological systems.

SESSION 1

MACHINE LEARNING IN TELECOMMUNICATION NETWORKS - I

A MACHINE LEARNING MANAGEMENT MODEL FOR QoE ENHANCEMENT IN NEXT-GENERATION WIRELESS ECOSYSTEMS

Eva Ibarrola[1], Mark Davis[2], Camille Voisin[3], Ciara Close[3], Leire Cristobo[1]

[1]University of the Basque Country (UPV/EHU), Spain
[2]Dublin Institute of Technology (DIT), Ireland
[3]OptiWi-fi, Ireland

ABSTRACT

Next-generation wireless ecosystems are expected to comprise heterogeneous technologies and diverse deployment scenarios. Ensuring a good quality of service (QoS) will be one of the major challenges of next-generation wireless systems on account of a variety of factors that are beyond the control of network and service providers. In this context, ITU-T is working on updating the various Recommendations related to QoS and users' quality of experience (QoE). Considering the ITU-T QoS framework, we propose a methodology to develop a global QoS management model for next-generation wireless ecosystems taking advantage of big data and machine learning. The results from a case study conducted to validate the model in real-world Wi-Fi deployment scenarios are also presented.

Keywords – Big data, machine learning, QoBiz, QoE, QoS, Wi-Fi

1. INTRODUCTION

The evolution of Internet users' behavior in recent years, along with the increasing variety of free applications and services, has led to Internet access becoming something indispensable for our daily life. As a result, users are turning out to be more and more demanding in terms of Internet coverage, accessibility and mobility, causing Internet service providers (ISPs) to consider alternative business models to fulfill these needs. For this reason, some of the technologies that were originally considered for providing local access to the Internet have now emerged as ubiquitous access technologies, leading to complex scenarios where fulfilling the required quality of service (QoS) will become a real challenge.

The Wi-Fi technology, defined in the IEEE 802.11 standard, is a good example of this. While originally designed to be a wireless local area network (WLAN) technology, today's large deployment of Wi-Fi networks has encouraged ISPs to consider new business models turning this technology into a “ubiquitous access technology for mobile users” [1]. In this way, providers can offer complementary broadband access ensuring the coverage, mobility and accessibility demanded by their users. Consequently, many scientific and industrial researchers [2] envisage 5G as having an agnostic radio access network (RAN) comprising multiple wireless technologies.

Therefore, even though there is still no clear consensus about what the next-generation wireless (NGW) era will embrace, there seems to be a general agreement that 5G will comprise heterogeneous networks (HetNet) cooperating to maintain a user's QoE. Furthermore, the adoption of new business models, quality of business (QoBiz), to integrate all the capabilities that next-generation wireless systems may offer will be crucial. Nonetheless, ensuring the required quality of experience in these complex scenarios will become a major issue.

The ITU’s standardization expert group for future networks (SG-13) has been working towards the definition of 5G systems and the development of new Recommendations related to QoS in the NGW environment [3, 4]. In addition, being aware of the great challenge of managing next-generation wireless networks, new groups, like the “*Focus Group on Machine Learning for Future Networks including 5G*” [5], have been established. ITU-T SG-12 has also focused on updating and defining new Recommendations related to QoS and QoE for adapting to the new NGW scenario [6, 7]. Nevertheless, there is still a need for methodologies that will take advantage of new techniques and mechanisms, such as machine learning (ML) algorithms, for the deployment of QoS management models as defined in the standardized QoS frameworks.

In this paper, a methodology for the implementation of a global QoS management model in NGW ecosystems is proposed. The model takes into account the ITU QoS framework [8] and the methodology aims to include all the aspects that the 5G era will require. Enhancing the quality of experience and the satisfaction of the users through new business models to fulfill their requirements are the main target of the methodology. The identification of the optimal key performance indicators (KPIs) and key quality indicators (KQIs) are essential to achieve this goal.

The proposed methodology represents a major challenge because of the unpredictable nature of the scenarios considered, with networks sharing the spectrum (even working in unlicensed bands) and a response totally dependent on the behavior of users and many other contextual and non-contextual agents not controlled by the providers. Addressing this challenge through ML constitutes the novelty of this proposal.

The remainder of the paper is organized as follows: Section 2 summarizes related work on QoS management approaches in wireless scenarios considering the use of ML-based models, and also standardization-related works are reviewed. Section 3 describes the QoS management model that is adopted and defines the QoS-QoE-QoBiz relations to be considered. In Section 4, the proposed methodology to implement the model in NGW scenarios through ML mechanisms is described. Section 5 illustrates the experiment carried out to validate the proposed methodology and, finally, Section 6 contains some conclusions and final remarks.

2. BACKGROUND

Many studies and standardization efforts related to QoS and QoE have been conducted in recent years. Most of these show that the assessment of QoS has moved away from network performance (NP) in favor of QoE, related to the subjective perception of end users. However, as stated in the Recommendation ITU-T G.1000 on the QoS framework [8], the great challenge to success when deploying a QoS management model is to embrace all the different QoS-related aspects (e.g. NP, QoS, QoE, QoBiz) and, more importantly, quantifying the relationships between them. This may become a difficult task when dealing with next-generation wireless ecosystems, where many unpredictable instances may have an influence on the user´s experience.

In view of this, some recent studies suggest using big data analysis and ML algorithms for modeling the QoE-QoS relationship. ML techniques may be useful to infer rules from big data analysis and identify the KPIs/KQIs that will lead to automatically estimating the quality as perceived by users based on the QoE influence factors. Selecting the suitable learning algorithm may be critical to obtaining reliable results.

2.1 QoE models and machine learning

There is limited research on the modeling of QoE with ML for next-generation mobile scenarios. Nevertheless, there are some recent studies focused on analyzing and using the data captured from the network and the users' surveys to model and to enhance the QoE [9-11].

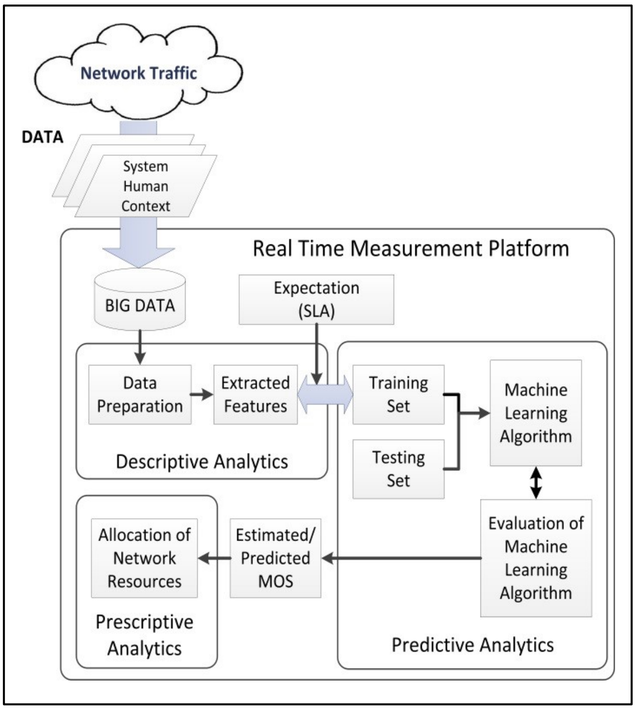


Figure 1. Framework for modeling the perceived QoE using a big-data analytics approach [9]

The framework presented in [9] (Figure 1) is a step ahead of the other works. In the proposed framework, "*the process of estimating or predicting the perceived QoE based on the datasets obtained or gathered from the mobile network to enable the mobile network operators effectively to manage the network performance and provide the users a satisfactory mobile Internet QoE*" is described. The state-of-the-art included in this work covers a large set of experiments in different scenarios and for different applications and services in relation to modeling QoE with ML algorithms. Their study about the dimensions of the QoE influence factors reviews a great number of scientific proposals. After the analysis, the authors concluded that three QoE dimensions (human, system, and context) should be considered when modeling QoE (Figure 2).

Aroussi and Mellouk presented in [10] an interesting survey about ML-based QoE-QoS correlation models. They suggest that supervised or semi-supervised learning models provide a better fit for the QoE-QoS correlation modeling than non-supervised ML.

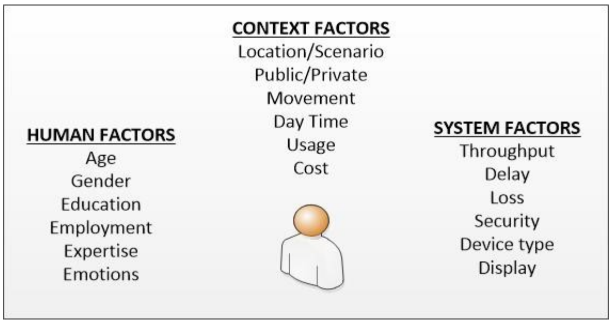


Figure 2. QoE dimensions and influence factors [9]

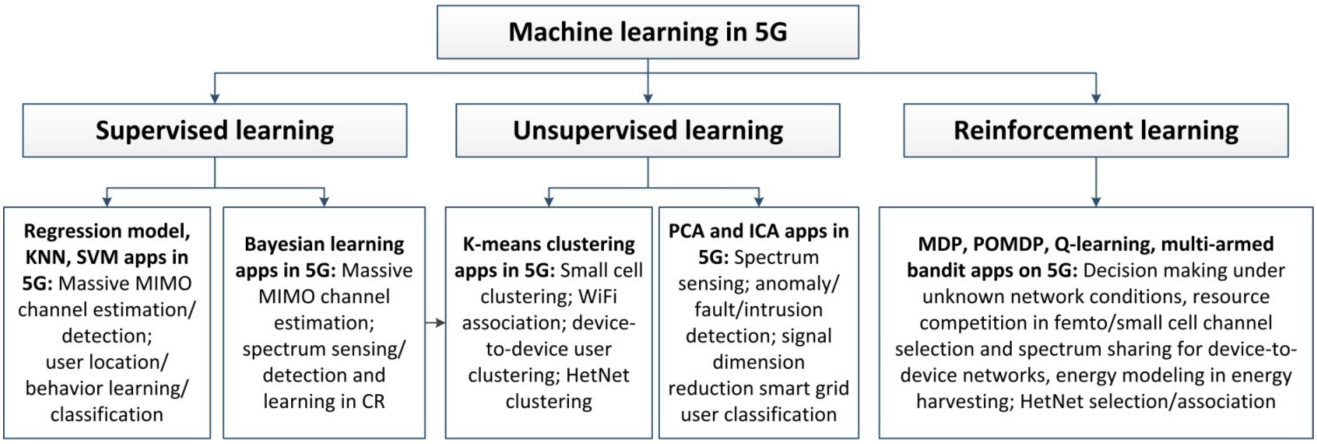


Figure 3. Machine-learning techniques and paradigms in 5G [11]

In this sense, a detailed description of the different ML algorithms and their application in the 5G environment is presented in [11] (Figure 3). The authors of this paper note the importance of selecting the appropriate learning type when using ML techniques since the goal of ML is to predict the output of an input turning observational data into a model that can be used for this prediction. Therefore, depending on the nature of the observational data, different types of learning can be distinguished:

- In *supervised learning*, each input value of the observational data is given with the corresponding output to form a training set. This set is used to learn a predictive function. Supervised learning is useful for classification and for regression problems.
- In *unsupervised learning*, only the input values are included in the observational data. The most common application of unsupervised learning is cluster analysis to find similarities between the input values and extract hidden patterns to group them into clusters.
- *Reinforcement learning* is based on dynamic iterative learning and decision-making processes. The learner is not told which actions to take but instead must determine those that yield the output closest to the target by successive trials.

2.2 Standardization: Key to 5G

Standardization bodies also envision the importance of defining new standards on QoS and ML for NGW ecosystems. In January 2018, a workshop on "*Machine Learning for 5G and beyond*" was held in Geneva (Switzerland) in the context of the first meeting of the recently-launched ITU "*Focus Group on Machine Learning for Future Networks including 5G*" [5]. Three different working groups were established:

- *WG1*: Use cases, services & requirements
- *WG2*: Data formats & ML technologies
- *WG3*: ML-aware network architecture

In this context, ITU-T SG-13 has developed several Recommendations related to 5G QoS frameworks and ML techniques [4, 12] (Figure 4). In addition, ITU-T SG-12, the expert group responsible for the development of international standards for QoS and QoE, has been active in the editing and updating of related Recommendations to work around new mobile scenarios [6, 7]. The 5G-PPP partnership, initiative between the European Commission and European ICT industry, is also working actively to define architectures, technologies and standards for NGW systems.

In spite of the significant advances in the definition of the 5G ecosystem and the identification of new QoE models and ML techniques for this environment, there is still a need for global QoS management models to be deployed in real-world NGW scenarios. In the following sections, an approach to solving this shortage is presented.

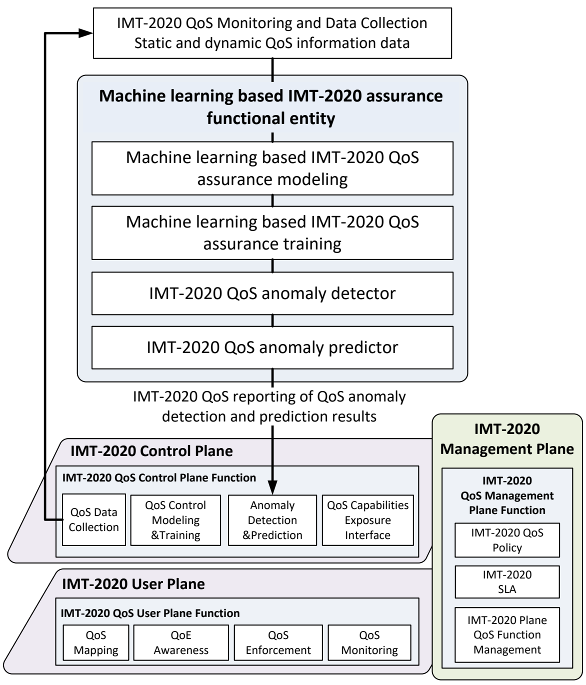


Figure 4. ITU model of ML-based QoS assurance [4, 12]

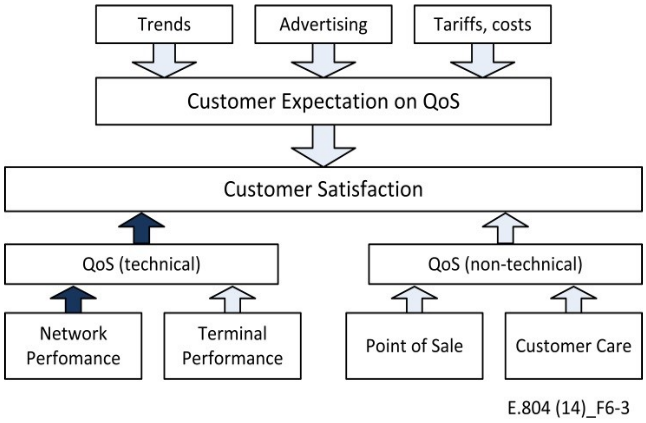


Figure 5. QoS relationships, from Recommendation ITU-T E.804 [6].

3. QOS MANAGEMENT MODEL: QOXPHERE

The QoS management model, QoXphere [13], has been adapted from its original architecture to include the new NGW ecosystem requirements. Nevertheless, the basic principles of the model remains; it still takes into account the four viewpoints of QoS of the ITU-T G.1000 QoS framework [8] and also the QoS aspects for mobile networks, as defined in ITU-T E.804 [6] are considered (Figure 5). Hence, the model is still organized in four different layers (Figure 6), though some of the QoS aspects considered in each layer have been updated (Figure 7) to fit with the new 5G QoS standardized framework.

The intrinsic QoS layer still identifies the KPIs to be used for the evaluation of objective QoS. Based on the specified class of service (CoS), the key performance parameters (KPP) that contribute to each KPI must be identified to evaluate the NP. The results of the first layer analysis feed into the second layer of the QoXphere, where the QoS as perceived by the users (QoP) is estimated. This layer continues considering the ITU-T G.1000 four viewpoints of QoS. The identification of the KQIs of interest for the users is still the crucial challenge at this stage of the model.

The third layer of the model focuses on the evaluation of the assessed QoS. The user's satisfaction is modeled through the feed of the QoE provided by the second layer and the information about a user´s expectations. The user's satisfaction values lead to identifying the key risk indicators (KRIs) to estimate the churn probability and establish the key business objectives (KBOs) that constitute the core of the upper layer of the model and analyses the QoBiz in terms of the profitability of the business models. This analysis may lead to "operational efficiency" actions, like defining new advertising procedures, new billing rates associated with new KQI/KPI objectives that will be reflected in the service level agreement (SLA). The new SLA will feed the user's expectations and requirements (through the required KQIs) that, at the same time, will aid the identification of the required KPIs to be considered and measured.

Figure 6. QoXphere management model

4. MACHINE LEARNING METHODOLOGY

The methodology we proposed is based on previous implementations of the QoXphere management model but has been enhanced for deployment in NGW ecosystems.

Due to the complex and heterogeneous nature of NGW scenarios, ML mechanisms are proposed to identify some of the QoS aspects and to formulate some of the relations between them. Gathering and collecting data to feed the learning algorithms is essential to infer rules to be applied both for the identification of all the key indicators and the specification of the relationships between the QoS aspects in the different layers of the model. In addition, the methodology will provide the procedures to continue feeding the model and find the gaps and "hot points" where intervention is required to improve the QoS and fulfill the QoE requirements. The ITU-T SG-13 QoS framework and ML-based QoS assurance, as proposed in [4, 12], have been taken into account when defining the proposed methodology, together with the ITU-T SG-12 principles of managing QoS, as defined in Recommendations ITU-T E.802[13] and G.1000 (Figure 8).

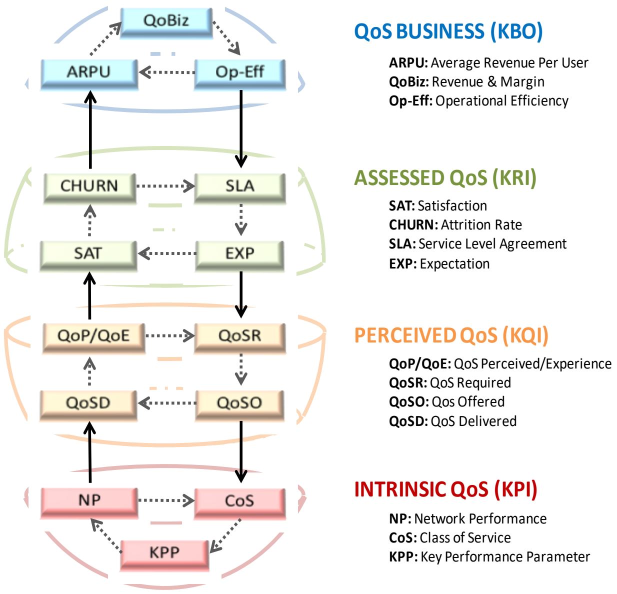


Figure 7. QoXphere: Layer structure

As stated in the framework in Recommendation ITU-T E.802, for any QoS management model to be successful, it is crucial that the identification of the QoS criteria is relevant to the users (based on their requirements/expectations). In our previous work, we have considered the four models proposed in Recommendation ITU-T E.802 for the identification of the QoS criteria. In the various NGW scenarios, it is essential to determine the different QoE dimensions and influence factors that may aid in identifying the user´s requirements. In the 5G wireless scenario, the network´s response will be dependent on the users' behavior and many other contextual and non-contextual agents not controlled by the providers, which may have a considerable effect on the user´s final satisfaction. For this reason, the first step proposed in the methodology is to understand the users' behavior in each of the scenarios to identify their requirements/expectations and determine the relevant QoS criteria. Therefore, since this first step is critical for the QoS management model to succeed, a combination of both contextual and non-contextual information is to be gathered through big data analysis. Unsupervised ML techniques (clustering) are proposed for inferring the different scenarios/profiles and for finding the user's context influence factors (the context extraction in Figure 8). In addition, inductive supervised learning is suggested to infer the rules to identify the QoS criteria and KQI relevant for the users. In this way, the complex procedure of surveying can be avoided except for the initial training period for the ML models to capture influence factors and user's requirements. Thus, the survey results will provide the particular cases of observation to draw the general rules predicted from a training set drawn from the context, system and human influence factors, together with the subjective information about the user's requirements and expectations gathered from surveys (i.e. the training set in Figure 8). Once the KPIs have been determined, the related KPPs will be specified for NP measurements based on the CoS and the ITU-T framework guidelines. At this stage, once the KPPs have been identified, the control of the "intrinsic QoS" may start (Control Plane in Figure 8). It is recommended to enable unsupervised ML techniques from the NP-gathered data to infer adequate radio/channel selection and detect faults and anomalies in the network behavior. This constitutes the first intervention point where corrective actions may be implemented to enhance the QoS (Anomaly Detection/Fault* in Figure 8).

For the study of the QoE (User Plane in Figure 8), the proposed method considers using also both the objective and subjective gathered data. Supervised machine-learning algorithms are suggested (regression model) for the correlation of the NP/QoE [10] using the survey's results and the NP collected data from probes, the correlation function between the QoE and NP can be deduced (see NP/QoE correlation model in Figure 8). The context and non-context influence factors will be also crucial when analyzing the user's QoE and for this reason, they feed again the training set to learn the rules that will provide the predicted QoE. The ML will avoid repeating the surveying complex process except for the time to capture the necessary observation data that will feed the training set process. This training set will be used to deduce the rules that will control the NP/QoE correlation model.

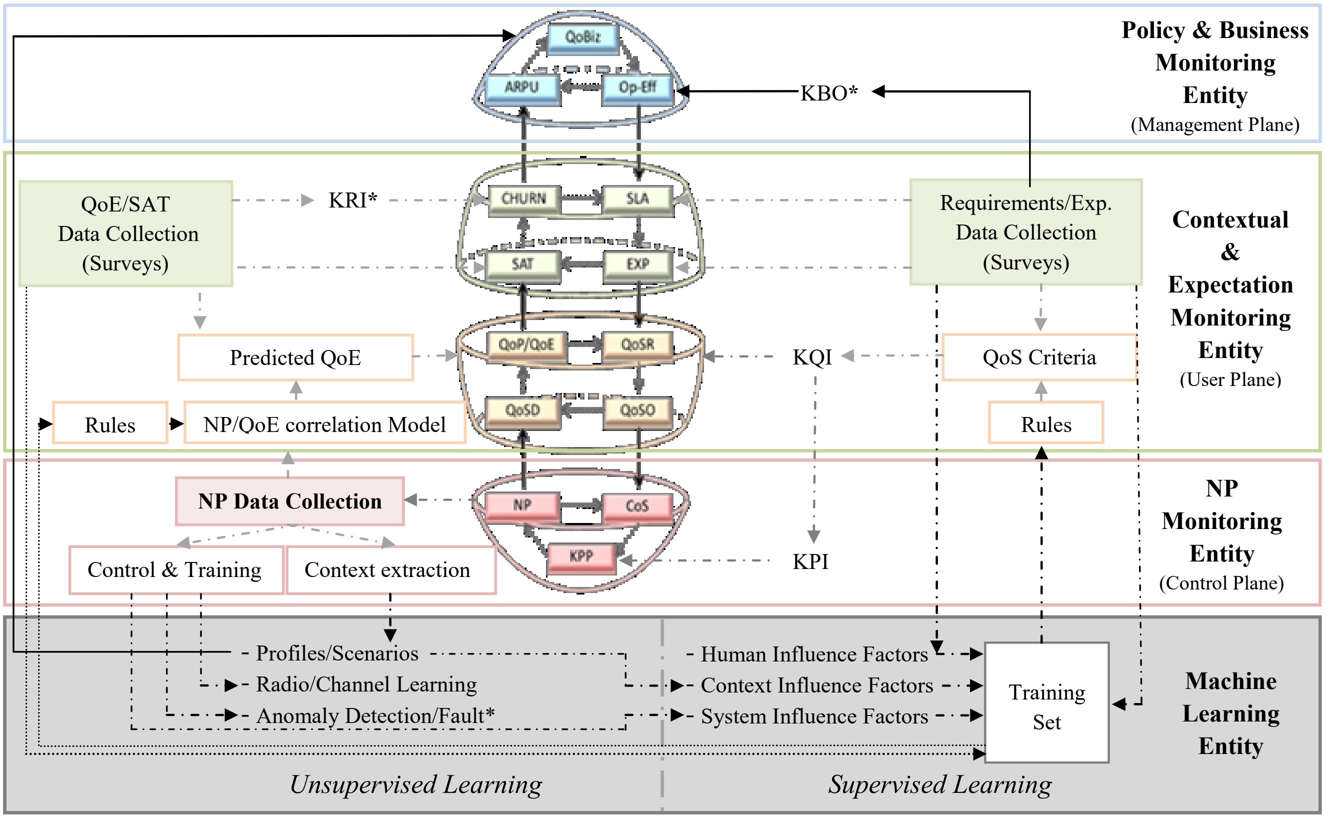


Figure 8. Proposed methodology for machine learning in 5G

Based on the QoE results, the customer satisfaction model (CSAT) described in [14] will estimate the satisfaction of the user with the service. This constitutes the second "hot point" where corrective actions may be necessary based on the detected KRIs that may lead to churn and affect the business model, as shown in Figure 8.

Finally, the KBOs will be updated on a regular basis. As referred to in [15], the KBOs are derived from the business areas that are determined important for each company and they should be adjusted through the operational efficiency to increase revenue, reduce cost and improve customer experience. This constitutes the last intervention point where corrective actions may be required. Billing, advertising, fitting the QoS requirements and other measures should be analyzed to update the SLA, taking into account the outputs of the user plane and the control planes.

5. CASE STUDY: IEEE 802.11 SCENARIOS

In previous sections we have introduced the principles of the QoE enhancement methodology approach. In this section, we present the implementation of the proposal in a real next-generation wireless scenario: the Wi-Fi networks.

5.1 Wi-Fi technology

Wi-Fi technology, also known as IEEE 802.11, was originally designed to be a wireless local area network access technology which is to say intended only for small coverage areas. However, Wi-Fi has become a "ubiquitous access technology for mobile users" [1]. Consequently, it is now being considered as one of the key access technologies in the 5G HetNet ecosystem. Nevertheless, QoS management in this type of "unlicensed radio spectrum" wireless network may become very complex, especially when users' demands in terms of QoE are increasing.

IEEE 802.11e was developed to offer new QoS capabilities to the IEEE 802.11 WLAN networks. Under this amendment, new QoS mechanisms, such as the enhanced distributed channel access (EDCA) mechanism were introduced to Wi-Fi technology at the media access control (MAC) layer, enabling different classes of access categories (AC) in order to support the prioritization of distinct classes of services. Even though numerous research studies can be found for the implementation of this protocol in scientific literature, it is rarely used in real deployments. The reason is quite obvious: Wi-Fi QoS management is completely dependent on the behavior of users, the coexistence of networks and many other aspects that the provider cannot control. That is the reason why most Wi-Fi service providers currently resort to an "over-dimensioning" in the deployment of their access points (AP).

For the above, the Wi-Fi RAN has been selected to validate the proposed methodology to enhance QoE.

5.2 Unsupervised ML: Wi-Fi patterns and scenarios

For the identification of the different scenarios to be considered, DBSCAN clustering ML techniques were used. As a first stage, ML algorithms were applied only to the most relevant parameters from the extensive data set obtained from the probes (bandwidth consumed, transmission rate, number of data frames, frames in failure, etc). The results indicated distinct behavior patterns for, at least, three different types of scenarios:

- *Commercial & Business scenarios*: shopping centers, restaurants, hotels, entertainment venues, etc.
- *Public scenarios*: schools, university campuses, cultural venues, museums, etc.
- *Residential scenarios*: both residential wireless access and shared agreement access.

Therefore, it was decided to carry out the study in three such real Wi-Fi scenarios:

- *The CHQ building (https://chq.ie/)*: to cover both business and commercial scenarios. This building, situated within the heart of Dublin city, holds different food and shopping spaces.
- *Dublin Institute of Technology (http://www.dit.ie/)*: to cover public (e.g. educational campus) scenarios.
- *The Gasworks Area*: to cover residential scenarios.

Subjective and objective measurements were required to validate the methodology. Objective Wi-Fi information was collected through OptiWi-fi network probes described in [16]: NP data, location data, mobility patterns, number of access points (AP), number of clients, connection time, type of devices and other information, according to [17], was captured by the probes. Subjective information was gathered through user surveys: personal information (gender, age, occupancy, Internet expertise) together with the data related to the "Wi-Fi experience", both about the user's requirements/expectations and QoE/satisfaction with the service, were collected in the same survey. The dates of the test field in each of the scenarios are presented in Figure 9 where the surveying process was carried out in a one-week period for each venue due to the complexity of the procedure and at least 50 participants took the survey in each of the scenarios. The network probes were deployed for a month in each of the venues to capture the required information about context and system influence factors.

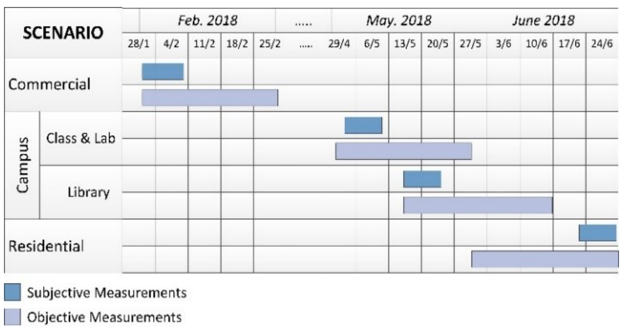


Figure 9. Test plan

5.3 QoS criteria and KQIs

The data collected from the probes and the surveys shed light on the important differences between the users' influence factors in the different scenarios. In addition, the results of the surveys about the user's requirements for each of the scenarios also showed that the relevant QoS criteria and KQIs differ from one scenario to another (Figure 10). Although the use of ML to automatically update the KQIs has not been yet tested, it has been proven that it is essential given the number and changing nature of the influence factors.

5.4 Control plane: Anomaly detector and predictor

The data collected from the probes have been used, not only to learn about the users' behavior and extract the context information, but also to detect anomalies and enhance the channel selection process through unsupervised ML.

5.5 User plane: Supervised ML

Based on previous research studies [10], inductive supervised learning has been employed for the NP-QoE correlation model. The results of the surveys about user's QoE and satisfaction have fed the model to infer the rules to automatically predict the QoE based on NP and the influence factors. In future stages of the study ML techniques will be also implemented to enhance the satisfaction model (CSAT) described in [14].

5.6 Results: Corrective actions to enhance QoE

Though the validation of the methodology is still at a premature stage, the case study has revealed that the proposed methodology can be very useful to deploy the QoS management model and enhance the user´s QoE. In fact, the results have indicated several corrective actions that could be implemented through ML in the scenarios under study:

- *Commercial scenario*: one of the most relevant KQIs in this scenario (streaming video/audio application performance) is affected for NP problems (continuous disruptions of the service). Corrective action: Analysis in NP data of AP capacity and use of ML to enhance the channel selection mechanism.
- *Campus Scenario*: Some client-association problems were found due to bad AP configuration. Furthermore, the students were dissatisfied with one of the KQIs (the ease of login) so the procedures around the login procedure should be revised. Corrective actions: Customize AP performance through ML techniques and revise login procedures according to the learned rules.
- *Residential scenario*: Lower cost and higher network speed were two of the key requirements in this scenario. Corrective actions: Customize residential Wi-Fi APs for optimal throughput through ML and enhance the business model using supervised ML through the survey's observation set.

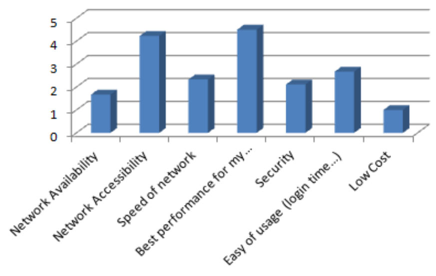
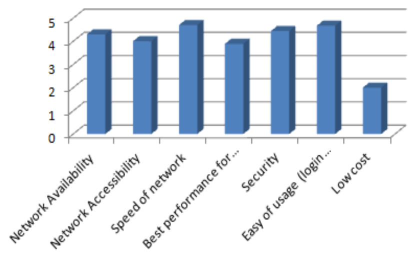
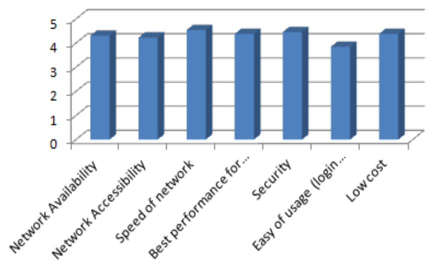
<table>
<tr><th></th><th>Importance of QoS criteria for users</th></tr>
<tr><td>Commercial</td><td>
</td></tr>
<tr><td>Campus</td><td>
</td></tr>
<tr><td>Residential</td><td>
</td></tr>
</table>

Figure 10. KQI relevance in different scenarios

6. CONCLUSIONS

In this paper a methodology to implement a global QoS management model for the next-generation wireless ecosystem, taking advantage of big data and ML techniques, has been presented.

Taking into account international standards, the QoE-centric approach makes use of supervised ML techniques in order to identify the KQIs relevant for the users. Unsupervised ML mechanisms are proposed for the identification of the user's influence factors, network performance anomalies, faults detection and channel selection enhancement. The approach links the NP and QoE via inductive ML techniques and provides the intervention points where corrective actions are required.

Although the definition of the methodology and the validation of the approach is still at an early stage, the results of the case study, carried out on a number of different Wi-Fi scenarios, reveal that the methodology may aid enhanced QoE in next-generation wireless environments. In addition, some recent studies suggest that ML techniques may be applied for customer retention to enhance the QoBiz and this will be also analyzed at future research stages of this proposal.

7. REFERENCES

[1] L. Zhang, L. Zhao, Z. Wang, and J. Liu, "WiFi Networks in Metropolises: From Access Point and User Perspectives," *IEEE Communications Magazine,* vol. 55, pp. 42-48, 2017.

[2] K. Kaur, S. Kumar, and A. Baliyan, "5G: a new era of wireless communication," *International Journal of Information Technology,* pp. 1-6, 2018.

[3] Recommendation ITU-T, Y.3100: "Terms and definitions for IMT-2020 network," Geneva, 2017.

[4] Recommendation ITU-T Y.3170, "Requirements of machine learning based QoS assurance for IMT-2020 networks," Geneva, 2018.

[5] ITU-T. (2017). *Focus Group on Machine Learning for Future Networks including 5G*. Available: https://www.itu.int/en/ITU-T/focusgroups/ml5g/

[6] Recommendation ITU-T, E.804: "Quality of service aspects for popular services in mobile networks," Geneva, 2014.

[7] ITU-T, "Draft new Recommendation ITU-T G.QoE-5G "QoE factors for new services in 5G network", 2018.

[8] Recommendation ITU-T, G.1000: "Communications quality of service: A framework and definitions," Geneva, 2001.

[9] A. W. Yusuf-Asaju, Z. M. Dahalin, and A. Ta'a, "Framework for modelling mobile network quality of experience through big data analytics approach," *Journal of Information and Communication Technology (JICT),* vol. 17, pp. 79-113, 2018.

[10] S. Aroussi and A. Mellouk, "Survey on machine learning-based QoE-QoS correlation models," in *International Conference on Computing, Management and Telecommunications (ComManTel)*, 2014, pp. 200-204.

[11] C. Jiang et al, "Machine Learning Paradigms for Next-Generation Wireless Networks," *IEEE Wireless Communications,* vol. 24, pp. 98-105, 2017.

[12] ITU-T, "Draft new Recommendation Y.IMT2020-qos-fr: QoS support framework architecture for IMT-2020 networks", 2018.

[13] Recommendation ITU-T, E.802: "Framework and methodologies for the determination and application of QoS parameters," Geneva, 2007.

[14] E. Ibarrola, E. Saiz, L. Zabala, L. Cristobo, and J. Xiao, "A new global quality of service model: QoXphere," *IEEE Communications Magazine,* vol. 52, pp. 193-199, 2014.

[15] Recommendation ITU-T E.419: "Business oriented Key Performance Indicators for management of networks and services," Geneva, 2006.

[16] M. Davis, "A wireless traffic probe for radio resource management and QoS provisioning in IEEE 802.11 WLANs," in *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, Venice, Italy, 2004, pp. 234-243.

[17] M. Davis and T. Raimondi, "A novel framework for radio resource management in IEEE 802.11 wireless LANs," in *Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt'05)*, 2005, pp. 139-147.

UNSUPERVISED LEARNING FOR DETECTION OF LEAKAGE FROM THE HFC NETWORK

Emilia Gibellini[1]; Claudio E. Righetti[1]

[1]Telecom Argentina, Argentina

ABSTRACT

In the context of proactive maintenance of the HFC networks, cable operators count on Full-Band Capture (FBC) to analyze the downstream spectrum and look for impairments. There exists one particular type of impairment, which is ingress, likely to happen along with leakage. Therefore, the detection of the former leads to the identification of the latter. We collect data from FBC tool, and use unsupervised machine learning to group cable modems such that the signal they receive show common patterns. This allows a characterization of all cable modems in a service group. Then, we use the modems' locations to determine whether the root cause of the flaw is inside the homes or not.

Keywords - Machine learning, unsupervised learning, pattern clustering, spectral analysis, content distribution networks, signal processing algorithms.

1. INTRODUCTION

Hybrid Fiber/Coax (HFC) is the term that describes the service delivery architecture used by cable operators and Multi System Operators (MSO). The architecture includes a combination of fiber optic cabling and coaxial cabling to distribute video, data and voice content from the headend to the subscribers, and vice versa. Folds, breaks, corrosion of connectors, among others, cause noise and interference, and distort the transmission on the coaxial. This means that the spectrum inside the HFC shows impairments.

Many home devices emit signals on the radioelectric spectrum at frequencies that match the HFC's upstream band (5 to 42 MHz) and downstream bands (50 MHz to 1 GHz). These signals could enter the cable system through poorly shielded cables or through the communication devices attached to the cable network within the home, causing a particular type of impairment, which we simply call ingress.

The type of ingress may vary according to the kind of damage in the physical network. For instance, a broken coaxial cable may act as a radio antenna, bringing into the HFC spectrum some trace of FM radio signals.

We know that ingress and leakage occur simultaneously. This is quite intuitive because whenever there is ingress, as signals get into the HFC, there is also a possibility that part of the signals that should be contained in the cable are egressing to the air, bringing noise into the radioelectric spectrum. Consequently, the identification of ingress necessarily leads to a proactive detection of leakage.

The identification and fix of the flaws that cause impairments have always been an issue for the field service. CableLabs refers to the full set of impairment identification capabilities as DOCSIS Proactive Network Maintenance (PNM) [1]. CableLabs' InGeNeOS (Intelligent Generation-Next Operational Systems) working group has been working on - and continues to work on- a variety of techniques based on DOCSIS (Data-Over-Cable Service Interface Specification) [2] to deal with impairments to simplify these tasks and improve efficiency.

Modern cable modems, more specifically DOCSIS 3.0 and DOCSIS 3.1, have the capability to measure the spectrum of a downstream signal using a high-speed A-D converter (e.g. 2.5 Gsamples/sec). The chipmaker Broadcom announced in 2011 [3] the first fully digital "Full-Band Capture" tuner chip - able to tune anywhere in the 50 MHz to 1 GHz downstream spectrum.

Full-Band Capture (FBC) allows cable operators to analyze the spectrum of cable modems. Technicians and engineers would look at the data collected by this tool, in real time, and look for signs of spectral impairment. Cable operators are looking for alternatives to the visual analysis; efforts go mainly towards machine learning as it provides an automatic and hence more precise and time-efficient analysis of the spectrum [4].

It is part of our role as scientists to evangelize about machine learning technology within our company. In order to do so, we look for applications that draw on the most intuitive algorithms. We have found that the use of intuitive algorithms allows us to transfer knowledge to other areas in an effective way.

In order to develop this tool, we apply a well-known unsupervised machine learning technique, which is the k-means clustering algorithm to create an easily replicable analysis. The advantage of using k-means is that we can find this algorithm in almost any software. The ultimate goal is to group signals in such way that through the identification of impairments in a few groups (the clusters) we can characterize a larger number of cases. This aims to help the operations team that would usually spend lots of effort analyzing each cable modem individually.

It is essential that the identification of damage in the physical be more rapid. In addition to the characterization of impairments, field service technicians need a geographical reference to determine whether the damage could be inside a client's home (if the same pattern is located at relatively distant and random points) or not (if the same pattern occurs in nearby locations).

2. MEASUREMENT

Telecom Argentina's FBC tool takes 24,000 measurements of each cable modem, in real time. This measures the spectrum existing between 45MHz and 1,005 MHz. For analysis purposes, the tool is configured to collect and record the data on a daily basis.

In order to perform the proof of concept (PoC), we use the data from February 5, 2018. For the purpose of reducing the computational effort, we executed the cluster analysis using the data of frequencies bands where we know that ingress is likely to take place. This reduces the number of data points from 24,000 to 4,458 per cable modem. Table 1 shows the frequency bands in which we focused for this PoC.

Table 1 – Frequency bands [5] analyzed in this paper

Frequencies (MHz)	Service
88 - 108	FM radio
518 - 541	Digital public TV (Argentina's TDA)
703 - 743	LTE uplink
758 - 803	LTE downlink
824 - 849	3G uplink
869 - 894	3G downlink

We analyze the spectrum of all cable modems in a service group. In the HFC plant topology, a service group is the complete set of downstream and upstream channels within a single CMTS (Cable Modem Termination System), that a single cable modem could potentially receive or transmit on [6]. At the time of data retrieval, there were 421 cable modems in the selected service group.

We made all of the data processing in R software [7]. For the cluster analysis, we used the MASS package [8]. In addition, we used Google Earth to obtain location data.

3. METHODOLOGY

Cluster analysis is a term that encompasses a variety of algorithms, aimed to group elements in a way that differences among observations in the same group are minimum, and the groups are as different from one another as it is possible. This kind of algorithms are particularly useful when there is a notion that the observations in a dataset come from K different populations. It reveals the similarities and differences among them.

One of the challenges when applying cluster analysis to a dataset involves defining meaningful dimensions of analysis. In this case, we considered each one of the 4,458 measurements on each cable modem as a new dimension of analysis. Following this line, it is possible to interpret the spectrum as a point in a highly dimensional space.

3.1 The k-means algorithm

The strategy to obtain the clusters that receives the name of *k-means* consists on executing this algorithm [9]:

1. Set K points on the p-dimensional space as cluster centers, based on previous experience or in a random fashion.
2. Calculate distances from all of the observations to the centers.
3. Assign each observation to the nearest center.
4. Use some criteria to evaluate the clusters.
5. Recalculate the clusters' centers.
6. Repeat steps two to five until there is no improvement in the evaluation made in step four.

The result may vary according to the centers selected in the initial step. One way to overcome this limitation is to initiate the routine in different centers and then evaluate if the result varies or not.

It is necessary to define a measurement of distance between observations. For a set of observations $\{\boldsymbol{X}_1, \boldsymbol{X}_2, \ldots, \boldsymbol{X}_n\}$ we use the Euclidean distance:

$$d(\boldsymbol{X}_i, \boldsymbol{X}_{i'}) = [(\boldsymbol{X}_i - \boldsymbol{X}_{i'})' \cdot (\boldsymbol{X}_i - \boldsymbol{X}_{i'})]^{1/2}$$

Where each $\boldsymbol{X}_i$ is a vector in a p-dimensional space. This definition of distance is sensitive to scale variations. A best practice is to scale measurements when the variables involved in the clustering process have different measurement units. It is better to use the original data when all the values have the same measurement unit. This will serve to identify natural patterns throughout the analysis.

3.2 Clusters evaluation

To evaluate the clusters, as stated in the step 4, we use the *Within Cluster Sum of Squares (WCSS)*, which is the sum of the Euclidean distances from all observations in the cluster to its center:

$$\mathrm{WCSS} = \sum_{k=1}^{K} \sum_{i=1}^{n} d^2(\boldsymbol{X}_{ik}, \overline{\boldsymbol{X}}_k)$$

Where the subscript k means that the observation $\boldsymbol{X}_i$ belongs to cluster k. This is also equivalent to a weighted sum of all within-cluster variances:

$$\text{WCSS} = \sum_{k=1}^{K}\sum_{j=1}^{p} n_k \cdot s_{jk}^2$$

Where n_k is the size of the cluster k, and s_{jk}^2 is the estimated variance of the variable j, in the same cluster.

3.3 Estimation of *K*

At the beginning of this section, we assumed that we already knew the value of *K*. It is possible -as it happens in this work- that the value of *K* is unknown. The WCSS is minimum when there are as many clusters as observations; therefore, to look for its absolute minimum is not an appropriate criterion when determining the value of *K*. Nevertheless, there is an empirical approach, the *elbow rule* [10], which uses this statistic to determine *K*. It consists in plotting the values of WCSS against the values of K from which we obtained them. The decision is based on where the curve shows an elbow or inflection point.

There is another exploratory method, called *stable classes* [11], that consists in executing the k-means algorithm to the same dataset, starting at different random centers every time, to identify stable groupings. It has the advantage that leads to identifying high-density areas in the p-dimensional space. On the other hand, it may lead to a high number of classes. Therefore, the number of groups we should keep are those of greater stable classes.

If the variables follow a Normal distribution, we could also obtain an approximate F test to assess the decreasing in the within-cluster variance when *K* increases one unit:

$$F = \frac{WCSS(K) - WCSS(K+1)}{WCSS(K+1)/(n-K-1)}$$

Where n refers to the total sample size. To know if the variance decreases significantly, we could compare the statistic to an *F* distribution with $\mathrm{p};\ \mathrm{p(n-K-1)}$ degrees of freedom. There is also an empirical rule that says that we should keep $\mathrm{K+1}$ clusters if the *F* value is greater than 10 [12].

4. CHARACTERIZING SIGNAL INGRESS

In this section, we present the results obtained in the search for *K*, as well as the clusters that we found, and how we interpreted the groups. Despite the fact that there are guidelines to estimate this parameter, the methods are exploratory and the decision finally depends on the analyst's expertise. Here we show the best results that we could get to the moment.

We already stated that we have 4,458 measurements on each cable modem, and we interpret every one of them as a new dimension of analysis. Therefore, the p-dimensional vector $\boldsymbol{X}_i$ contains all of the measurements made on the *i-th* cable modem, so $\boldsymbol{X}_i = \{X_{1i}; X_{2i}; \dots; X_{4,458i}\}$ and $p = 4{,}458$.

After a few attempts to work with the original data, we decided to standardize each cable modem's values –that means that we take each signal strength value, minus the cable modem mean, divided by its standard deviation-. We found that without standardization, the algorithm would catch that some cable modems receive stronger signals, which may be useful to solve other kinds of problems but not to report on signal impairment.

4.1 The search for the value of *K*

In order to apply the elbow rule, Figure 1 shows the values of the WCSS at different *K* values. It seems that there is an elbow at *K*=5. After that, there is a marginal decreasing of WCSS and a second elbow at *K*=10.

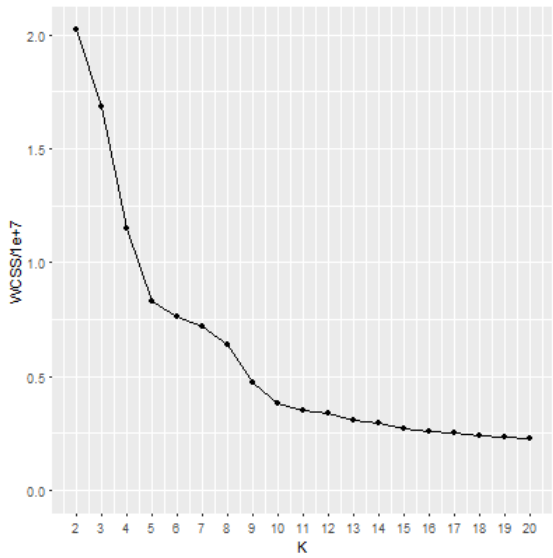


Figure 1 - Plot of K vs. WCSS

With the purpose of applying the stable classes method, the k-means algorithm was executed with two different random starts and *K*=10.

Table 2 - Distribution among *K*=10 clusters after two executions, as percentage of total modem count.

	C1	**C2**	**C3**	**C4**	**C5**
C1	**5,94**	**7,13**	0	**6,89**	0
C2	**15,44**	0	0,48	1,43	0
C3	1,66	0	**9,03**	0	0
C4	0	**11,88**	0	0	0
C5	**5,70**	2,61	0	0,24	0
C6	0	0	0	0	**5,70**
C7	0	0	0,48	0	0
C8	0	0	0	0	2,38
C9	0	0	0,24	0	0
C10	0	0,71	0	0	0

	C6	C7	C8	C9	C10
C1	0	1,19	0	0	0
C2	0	0,24	0,71	0	0
C3	1,66	2,14	2,38	0	0
C4	0	0	0	0	0
C5	0,48	0	0,24	0	2,14
C6	0	0	0	0	0
C7	1,66	1,90	0	0,24	0
C8	0	0	0,48	0	0,95
C9	0	0	0	3,33	0
C10	2,38	0	0	0	0

Table 2 shows the distribution of observations among clusters, and compares the first versus the second execution. There are five cells with frequencies above 6%, and eight cells above 5%. Depending on the cutoff, there may be five or eight stable classes, and this is similar to what we have interpreted from Figure 1.

Table 3 - Observed F values for *K* groups.

K	F value
2	84,31
3	194,52
4	162,58
5	38,78
6	25,46
7	52,52
8	145,45
9	103,23
10	32,79

Even though the variables in this study do not follow an exact Gaussian distribution, we estimated the values of the F statistic. Notice in Table 3 that in all cases the value is superior to 10. The statistic is below the empirical cutoff when K=19. We continue the analysis based on the number of clusters determined by the empirical methods.

4.2 Interpretation of the clusters

We performed this analysis with four to seven clusters and decided that six would be enough. When K varied, we saw on the 3G-downlink band that when there were fewer classes, at least one of them grouped mixed patterns. Setting $K = 7$, the patterns that we identified were the same as the ones seen with $K = 6$. The extra cluster did not add any new information to the analysis.

Next, we present the results obtained after executing the k-means algorithm with K=6.

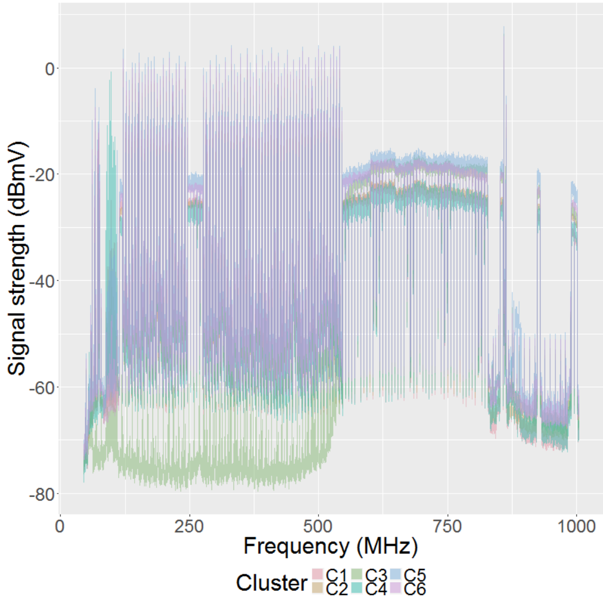


Figure 2 - Clusters' centroids

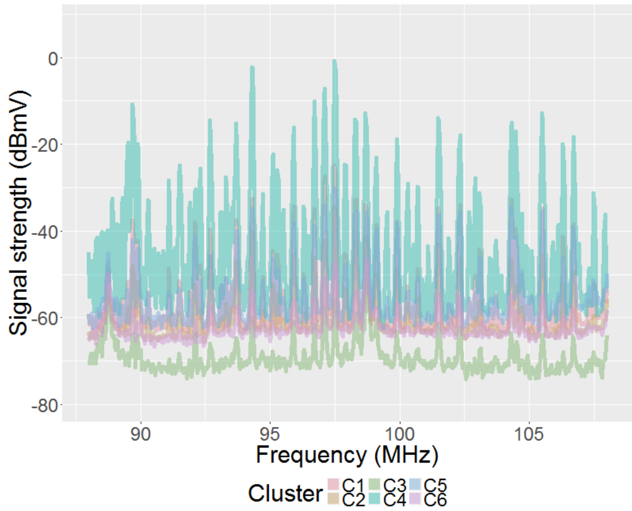


Figure 3 - Clusters' centroids between 88 MHz and 108 MHz

In Figure 2, we have noted at first sight that one of the clusters, C3, groups the cases of all subscribers who hired the Internet service only (usually our subscribers hire both broadband access and video services). We continue to plot the frequency bands that are of main interest for ingress detection.

According to Figure 3, the cluster C4 centroid is consistently above all the rest, and C3 is consistently below. In this frequency range, we could assume there was radio signal ingress.

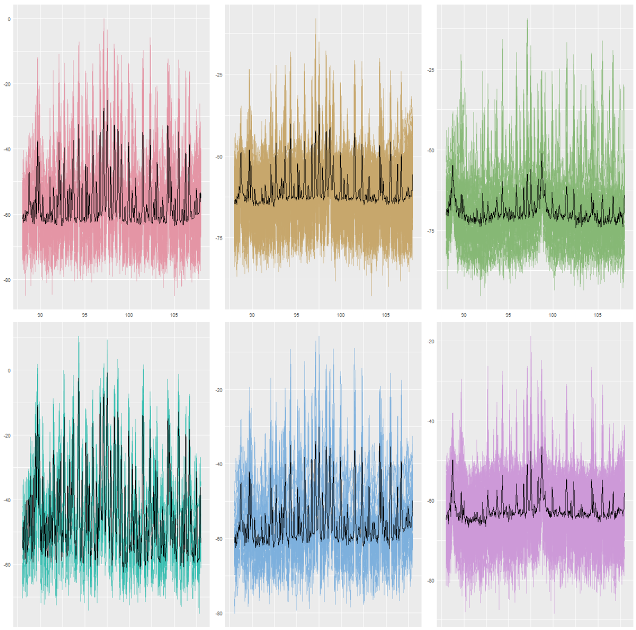


Figure 4 - View of clusters between 88 MHz and 108 MHz

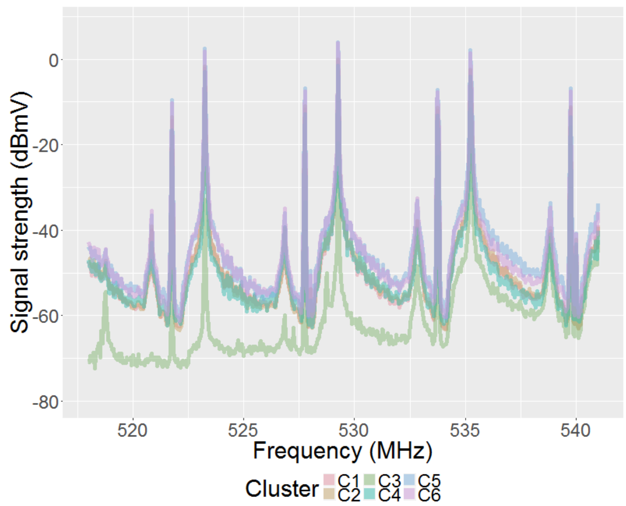


Figure 5 - Cluster centroids between 518 MHz and 541 MHz

To get more information about potential radio signal ingress, we look at the complete view of cluster centroids and the variation of cable modems' signals around them. In Figure 4, it seems like the signals in the fourth and fifth clusters are noisier. This could be due to FM radio signal ingress.

Figure 5 shows the cluster centroids in the frequencies between 518 MHz and 541 MHz. There is an increasing trend among the cases grouped by the third cluster. This is due to a filter that technicians put to the cable modems when subscribers hire the broadband access. Part of the signals transcend and form this pattern.

To gather more information about the patterns between 518MHz and 541MHz and assess the ingress of digital TV signal, we look at all the signals in each cluster in this band.

According to Figure 6, there could be ingress in clusters C1 and C6.

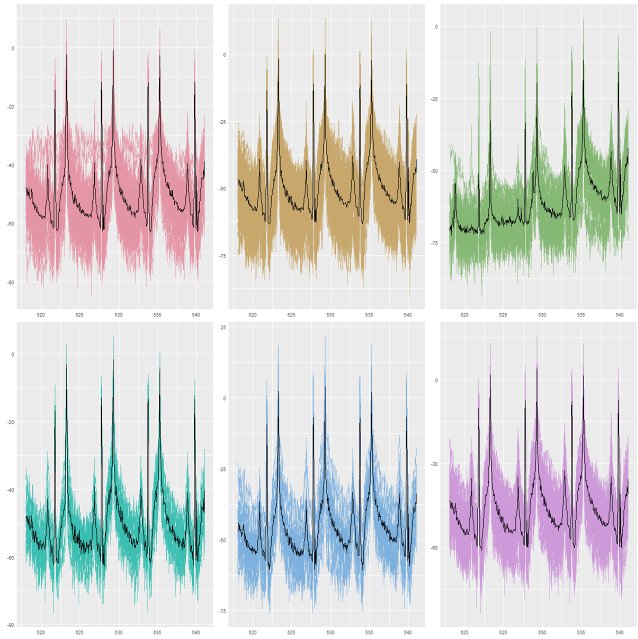


Figure 6 - View of clusters between 518 MHz and 541 MHz

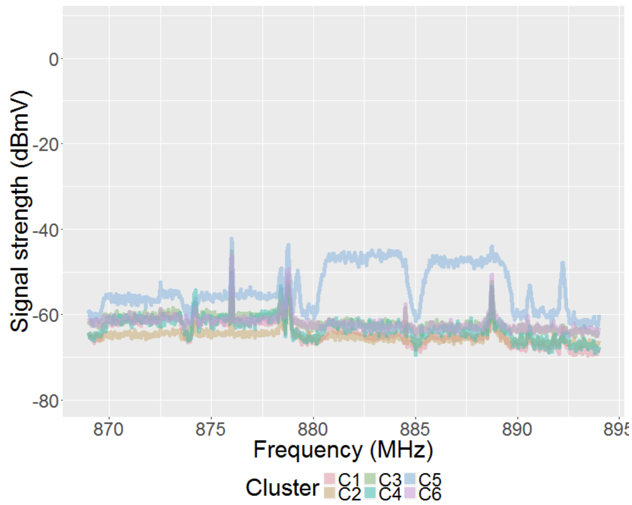


Figure 7 - Cluster centroids between 869 MHz and 894 MHz

We analyzed the cluster centroids, as well as the variation of the signals grouped around them, in the frequencies used for the LTE uplink and downlink, and 3G uplink. We concluded that there was no clear evidence of ingress in these bands.

It is quite clear from Figure 7 that there is ingress of the 3G-downlink signal in C5. In Figure 8, we see the form of four downlink channels, located approximately between 870 MHz and 875 MHz, from 875 MHz to 880 MHz, from 880 MHz to 885 MHz and from 885 MHz to 890 MHz, in clusters C1, C4 and C5. In the first and the fourth case, the original spectrum is not as affected as in the fifth. In C4, there is also more variability around the cluster centroid.

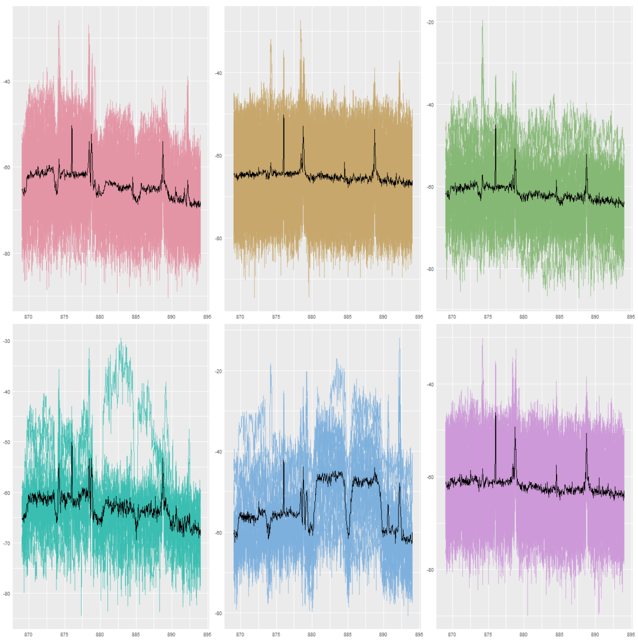


Figure 8 - View of clusters between 869MHz and 894MHz.

In addition, in Figure 8, there is a decrease in cluster C4. This is another type of impairment, called *tilt*, which consists in a loss of the signal strength throughout the spectrum. The analysis of its causes and implications is beyond the scope of this paper.

In clusters C2, C3 and C6, there is no clear evidence of ingress, though the signals in C3 seem noisier than the other two.

4.3 Geographical localization of the clusters

For the purpose of inferring the possible location of the damage, which provokes the presence of ingress -among other possible impairments, such as tilt-, we proceeded to locate the cable modems in a map, as shown in Figure 9.

In Figure 9, it does not look like the patterns group geographically. After discarding the clusters where we do not suspect that there is a presence of ingress, we can see that different types of ingress are all over the service group, and not in one particular block.

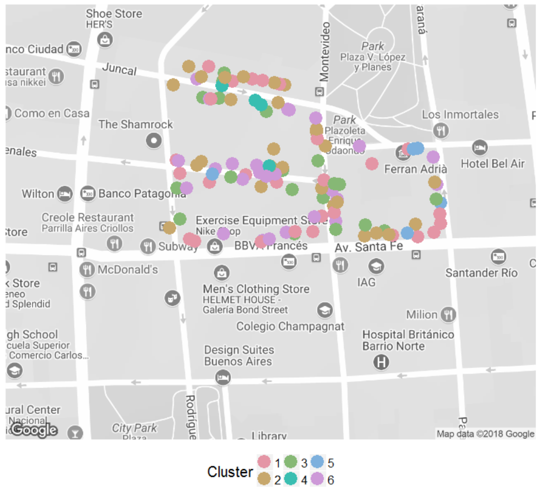


Figure 9 - Geographical disposal of all clusters.

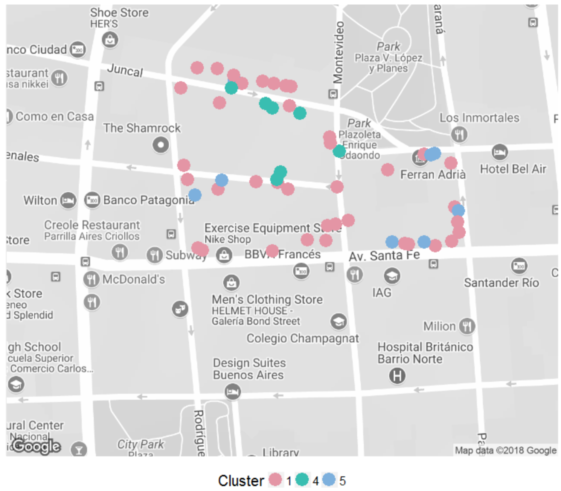


Figure 10 - Localization of cable modems grouped in cluster with ingress.

5. SUMMARY

We obtained six clusters (Table 4), in which we characterized ingress: in the first group, C1, there are traces of the signals from the public digital TV, the FM radio and the 3G downlink channels. It is similar to what we see on cluster C5, except for the fact that in the latter, there are two 3G-downlink channels that have a greater impact.

Table 4 - Characterization of ingress in the clusters.

Cluster	FM	Public digital TV	LTE downlink	3G downlink
C1	✓	✓		✓
C2				
C3				
C4	✓			✓
C5	✓	✓		✓
C6				

In C4, there is radio, as well as 3G-downlink signal ingress. These cases show tilt, which is another type of spectral impairment. The cable modems in clusters C2, C3 and C6 do not show clear evidence of impairment; the group C2 contains noisier or more variable signals, but no evident pattern. C3 contains the cases of Internet service only.

We end our analysis with a look at the spatial location of the cable modems in the C1, C4 and C5 groups. The points are sparse and occupy the total area of the service group, so we conclude that there might be some damage outside the clients' homes.

6. CONCLUSIONS

Cable operators are looking to transmit signals beyond 1 GHz on the HFC network, which may lead to leakage to some 5G bands. Consequently, it becomes necessary to open the discussion on ingress/leakage detection in 5G.

We used the k-means clustering algorithm and the data retrieved by the FBC tool to improve efficiency in spectral analysis. We carried out data processing as well as clusters calculation using open software.

In order to inform about potential sources of leakage, the focus is on the frequency bands where we know that it is possible that ingress takes place. This eliminates any unnecessary computational effort. The scaling of data points was key to get an algorithm that groups signals according to patterns, and not according to signal strength levels.

In the context of PNM framework, our new tool helped us achieve a rapid identification of six common patterns, three of which involve ingress of FM radios, digital TV and 3-G downlink signals. We do not find evidence of LTE ingress in this service group. Considering the location of the clusters in the city map, we have concluded that the cause of ingress was not inside the subscribers' homes.

This tool works as a successful example of machine learning application among the teams of field service, and we hope that this easily replicable PoC may also work as a recommended proceeding for cable operators to detect leakage on their networks.

On the other hand, we want to remark that it is an early stage development, and the analysis is not finished.

We will re-use the identified patterns to train a supervised algorithm that detects the impairments on another set of modems. We will also continue to investigate the impact of the number of samples per modem, as well as the variation of signal patterns in time, in order to determine the minimum conditions that need to be met to apply the method. We expect that in time this could lead to a standardization of the measurement process.

7. AKNOWLEDGMENTS

We thank Gabriel Davila Revelo and José Machao, who took time to induce us into some fundamental PNM concepts, as well as provided feedback on our interpretation of results.

8. REFERENCES

[1] CableLabs. "PNM Best Practices: HFC Networks (DOCSIS 3.0)", July 2016. [ONLINE] Available at: https://apps.cablelabs.com/specification/proactive-network-maintenance-using-pre-equalization [Latest retrieved June 20, 2018].

[2] CableLabs. "DOCSIS 3.0 Operations Support System Interface Specification", July 2017. [ONLINE] Available at: https://apps.cablelabs.com/specification/CM-SP-OSSIv3.0 [Latest retrieved June 20, 2018].

[3] Telecompaper. "Broadcom launches digital Full-Band Capture technology", June 2011. [ONLINE] Available at: https://www.telecompaper.com/news/broadcom-launches-digital-full-band-capture-technology--809318 [Latest retrieved June 20, 2018].

[4] Dorairaj, S.; Burg, B.; Pinckernell, N., Comcast Corporation; Bastian, C., SCTE. "Simplifying Field Operations Using Machine Learning", U.S., 2017.

[5] ENACOM. "Cuadro de Atribución de Bandas de Frecuencias de la República Argentina (CABFRA)". Argentina, pp. 101-185. April 2018.

[6] Society of Cable and Telecommunications Engineers (SCTE). "DOCSIS 3.0 Part 2: MAC and Upper Layer Protocols", Exton, Pennsylvania, U.S., pp. 30. 2013.

[7] R Core Team. "R: A Language and Environment for Statistical Computing", R Foundation for Statistical Computing, Vienna, Austria, 2017.

[8] Venables, W. N.; Ripley, B. D., "Modern Applied Statistics with S", Springer, New York, U. S., 2002.

[9] Peña, D. "Análisis de datos multivariantes", McGraw-Hill/Interamericana de España, Spain, pp. 228-231. 2002

[10] Gove, R. "Using the elbow method to determine the optimal number of clusters for k-means clustering" [ONLINE] Available at: https://bl.ocks.org/rpgove/0060ff3b656618e9136b [Latest retrieved June 20, 2018]

[11] Lebart, L.; Morineau, A.; Piron, M. "Statistique Exploratoire Multidimensionnelle", Dunod, Paris, France, pp. 152-154. 1995.

[12] Hartigan, J. A. "Clustering Algorithms", John Wiley & Sons, [New Heaven, U.S.], pp. 91. 1975.

DOUBLE SARSA BASED MACHINE LEARNING TO IMPROVE QUALITY OF VIDEO STREAMING OVER HTTP THROUGH WIRELESS NETWORKS

Dhananjay Kumar[1]; Narmathaa Logganathan[1]; Ved P. Kafle[2]

[1]Department of Information Technology, Anna University, MIT Campus, Chennai
[2]National Institute of Information and Communications Technology, Tokyo

ABSTRACT

The adaptive streaming over HTTP is widely advocated to enhance the Quality of Experience (QoE) in a bitrate constrained IP network. However, most previous approaches based on estimation of available link bandwidth or fullness of media buffer tend to become ineffective due to the variability of IP traffic patterns. In this paper, we propose a Double State-Action-Reward-State-Action (Sarsa) based machine learning method to improve user QoE in IP network. The Pv video quality estimation model specified in ITU-T P.1203.1 recommendation is embedded in the learning process for the estimation of QoE. We have implemented the proposed Double Sarsa based adaptation method on the top of HTTP in a 4G wireless network and assessed the resulting quality improvement by using full reference video quality metrics. The results show that the proposed method outperforms an existing approach and can be recommended in standardization of future audio-visual streaming services over wireless IP network. We observed the average improvement of 7% in PSNR and 25% in VQM during the live streaming of video.

Keywords – Video streaming, QoE, Machine learning, Sarsa, Video quality measurements

1. INTRODUCTION

The video streaming applications are dominating IP networks over last few years and it is continuously expanding. As per the Cisco Visual Network Index, globally 82% of the consumer internet traffic will be video by 2021, an increase of 73% from 2016 [1]. Further, the mobile data traffic is expected to increase seven times between 2016 and 2021. The Ericsson mobility report (November 2017) forecasts that there would be one billion subscribers for 5G mobile broadband in 2023 [2]. It is recommended that the future IP networks should not only be strong and resilient, but also support interoperability based on open standards with global reach [3]. In order to handle the surging video streaming traffic, the 3GPP and MPEG have proposed Dynamic Adaptive Streaming over HTTP (DASH) [4]. In DASH a video is split into a number of chunks of equal duration and each segment is encoded with multiple version of quality and hence bitrate [5]. The end goal is to provide smooth video streaming services even in networks with constrained available bandwidth.

The underlying principle of DASH i.e., the HTTP Adaptive Streaming (HAS), allows the video chunks to be served to clients utilizing standard HTTP servers in either live or on-demand form. Upon change in network conditions, a client can progressively switch video versions for the chunks to be downloaded to keep up persistent video playback. The dynamic adaptation leads to better Quality of Experience (QoE). However, HAS does not specifically control the transmission rate of video data and it is completely controlled by the TCP [6]. It also takes advantage of the HTTP/TCP universal usages, for example, HTTP-based delivery tackles NAT and firewall issues. Furthermore, it allows utilizing standard HTTP servers and caches for streaming the content; and a reliable transmission provide by the TCP [7].

In maximizing the end user QoE, the process of adaptation needs to consider a dynamic management of streaming media which dictates the perceived quality of the displayed contents. However, developing a robust prediction model for QoE considering reliability, accuracy, scalability, etc. remains a challenge [8]. There is a tradeoff between available network resources and perceived QoE. The dynamic adaptation of coding rate of the requested video by transmission resources could mitigate this problem since even reduction of coding rate is less critical to degradation of QoE than the other parameters such as packet loss and delay [9]. The solution also needs to consider the requirement of standard process in supporting streaming of audio-visual services over IP networks globally.

In a challenging situation where prediction modeling faces several limitations, Reinforcement Learning (RL) provides a promising technique to be incorporated in the system as an elegant and practical solution. However, the large state space of Markov decision process in these techniques becomes a major design challenge [10]. Under RL, the policy in Q-learning is governed by the selection of state-action pair, associated reward, and updating rule. But for convergence, all pairs need to be updated [11]. Further, in some stochastic environment, the overestimation in Q-learning slows down the learning process [12].The complexity of the advanced algorithms like Deep Q-learning [13] and Double Q-learning [12-14] could inflict the system performance particularly in handling the real-time applications like video streaming. The on-policy algorithms such as Sarsa and Double Sarsa [15] prove to be a better fit here because they learn the action-values at each step, depending solely on the states visited and action taken. When rewards are stochastic, Double Sarsa adds significant amount of stability in the learning process at minor increase in computational cost, while providing a higher return in an on-policy algorithm.

In assessing the quality of adaptive audio-visual streaming over reliable transport, the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T) has recommended a video quality estimation model and tool in ITU-T P.1203.1 [16], which is a parametric bitstream-based quality assessment method. This model is intended for client-side monitoring of encrypted/non-encrypted HTTP/TCP based video on demand VoD / live streaming services. Mode-2 of operation defined in P.1203.1 is intended for non-encrypted media and requires an input of meta-data and up-to 2% of the media stream with a medium complexity.

In this work, we propose a new algorithm based on RL approach, Double Sarsa to improve the quality of a live streaming video. In Double Sarsa, two estimates of the action-value Q(s, a) are decoupled and updated against each other in request to enhance the rate of learning in a domain with a stochastic reward system. The system is characterized by a set of states and actions where the best possible action is taken from the current state through a gradual learning process. It then calculates the reward in terms of Mean Opinion Score (MOS) using the ITU-T P.1203.1 framework and determines the resulting state of the system. Two exploration policies: softmax and ε-greedy are used separately to find the future action to be taken which is sent as feedback to the server and finally the Q-matrix is updated. In this approach the adaptation problem is expressed as an optimization process with their proposed internal QoE goal function.

In analyzing the performance of the proposed system, the Double Sarsa based quality adaptation algorithm is implemented independently with softmax policy and ε-greedy, and the performance is compared with an existing QoE driven strategy with future information [17]. The algorithms are implemented on the top (OTT) of HTTP while 4G wireless network are used to establish connectivity between client and server. The video encoding/decoding were carried out dynamically in accordance with test parameters defined in ITU-T J.247 [18] and ITU-T P.1203.1 [16] as listed in Table 1.

The decoded video sequences at the receiver were compared with the original video transmitted by the server for quality evaluation during experimentation. Full Reference (FR) video quality metrics namely Peak Signal to Noise Ratio (PSNR), Structural Similarity (SSIM), Multi-Scale SSIM (MS-SSIM), and Video Quality Metrics (VQM) are used to evaluate the quality of streaming video at client. The server adjusts video resolution based on the client feedback dynamically, the degradation of video quality at receiver is observed due to scaling down of the original content at the server. The proposed solution could be standardized considering its practical use in supporting adaptive streaming of video in IP network over wireless systems.

2. PROPOSED SYSTEM

2.1 System Architecture

The proposed framework design imitates the client server model where the server's activity gets simplified on the cost of client's expanded observation and analysis process. It is implemented on top of HTTP where the live (or stored) video is streamed from the server to the client connected through a 4G wireless network. The media content is encoded progressively utilizing ITU-T H.264 video codec [19] and then streamed to the client. Once the streaming starts, at the client side the proposed algorithm analyses the quality of the streamed media along with the network conditions in order to calculate the decision parameters to be sent as feedback to the server. The server analyses the feedback and adjusts the video quality to deliver the maximum achievable QoE that can be supported by the currently available network bandwidth.

Table 1– Test parameters as per ITU recommendations

Standards	Parameters	Metrics
ITU-T J.247	Transmission	Errors with packet loss
	Frame rate	5fps to 30fps
	Video codec	H.264/AVC (MPEG-4 part10),VC-1,Windows Media9, Real Video (RV10), MPEG-4 Part 2
	Temporal errors	Maximum of 2 seconds
ITU-T P.1203.1	Input video length	20 seconds
	Video resolution / bitrate	240p: 75-150 kbps 360p: 220-450 kbps 480p: 375-750 kbps 720p: 1050-2100 kbps 1080p: 1875-12500 kbps

2.2 Server Side Functions

The server at first obtains the live media content or the location of the stored video in memory and sets the media URL. It then uses the Java framework for the VLC media player (VLCJ) to set the appropriate encoding parameters to ensure continuous streaming of the video. The media player object is initialised and the streaming begins through the specified HTTP port. It then waits for the client's feedback analysis it adapts the video quality parameters (resolution, frame rate).

2.3 Client Side Functions

The client initialises the media player component with the media URL with the appropriate HTTP port and the decoding parameters needed to receive the streaming data. It also establishes a TCP/IP connection with the server. The video track information is examined to obtain the parameters of the video that is being streamed, which in turn is used to identify the current action of the system. The client captures the packets and estimates the throughput. The reward is calculated as described in Mode 2 of the P_v module in ITU-T P.1203.1 video quality estimation model. The estimated throughput is used to identify the current state. With the obtained state, action and the reward, the proposed algorithm decides the future action to be taken by the server and then sends this action as feedback to the server. The feedback is given at a regular interval.

3. COMPONENTS OF THE PROPOSED WORK

3.1 State-Action-Reward-State-Action (Sarsa)

State is the current situation returned by the environment and it contains data regarding the environment at a given time instance. Here the state is characterised as $s_{cur} = \{t_{h1}, t_{h2}, \ldots..t_{hn}\}$ where t_{hn} is n^{th} estimated throughput, thus the throughput values are mapped to the different discrete states. An action represents all the moves the agent can take and hence here the actions represent the different quality adaptation process, thus the various possible quality objectives are mapped to the actions. A reward is immediate return sent back from the environment to evaluate the last action. The input for the reward calculation is the output from the NR video quality assessment metrics.

The Sarsa is basically an on-policy learning method, where the system interacts with the environment in order to updates its policy based on actions taken. In the Q-table, the rows and columns of the matrix are the states of the system and the possible actions respectively. For any given pair *(s,a)*, the Q-value represents the learned value that the system will acquire by taking the action a in state s formulated as

$$Q(s,a) \leftarrow Q(s,a) + \alpha[r + \gamma Q(s',a') - Q(s,a)] \tag{1}$$

where α represents learning rate and γ the discount factor, $Q(s', a')$ the Q-value resulting from new action a' in state s'.

3.2 Double Sarsa

In Double Sarsa method [15], two action-value estimates $Q^A(s,a)$ and $Q^B(s,a)$ are defined in improving the performance of Sarsa in stochastic scenarios. Thus the update rule for Double Sarsa is given as follows.

$$Q^A(s,a) \leftarrow Q^A(s,a) + \alpha[r + \gamma Q^B(s',a') - Q^A(s,a)] \tag{2}$$

The learning rate *(α)* shows how much the acquired knowledge will influence the old value while updating. It is set between 0 and 1, setting it to 0 means that the Q-value will never be updated while setting a high value means the learning can occur quickly. The discount factor *(γ)* which is also set between 0 and 1, models the fact that future rewards are worth less than immediate rewards.

The Double Sarsa works similar to double Q-learning, but since it an on policy, the exploration policies like Softmax, ε – greedy etc. need to be modified.

3.3 Exploration policy

Two exploration policies are taken into consideration here namely, Softmax and ε – greedy. Softmax utilizes action-selection probabilities which are determined by ranking the value-function estimates using a Boltzmann distribution given by

$$\pi(a/s) = \frac{e^{\frac{Q^A(s,a)+Q^B(s,a)}{\tau}}}{\sum_b e^{\frac{Q^A(s,b)+Q^B(s,b)}{\tau}}} \tag{3}$$

where τ is a positive parameter called temperature, and b represents all possible actions. High temperatures cause all actions to be nearly equiprobable, whereas low temperatures cause greedy action selections.

In Epsilon greedy policy a random actions with uniform distribution in given a set of actions is chosen. This policy allows to select random action with ε probability (0 <ε< 1) or an action with 1-ε probability while maximizing reward in a defined state. The ε-greedy policy that uses the average of the two tables to determine the greedy action is as follows

$$\pi(a/s) =$$

$$\begin{cases} 1 - \varepsilon, if \text{ a} = argmax_{a' \varepsilon A(s)} Q^A(s,a') + Q^B(s,a') \\ \frac{\varepsilon}{N_{a'} - 1},\ otherwise \end{cases} \tag{4}$$

where $\pi(a/s)$ is the probability of taking action a from state s, and N_a is the number of actions that can be taken from state s. Double Sarsa based adaptation algorithm is thus used with two exploration policies.

3.4 Video Quality Estimation using No-Reference Metrics

ITU-T P.1203.1 defines a set of objective parametric quality assessment modules [16]. Although P.1203.1 recommendation describes four different quality modes (0, 1, 2 and 3), mode 2 is used here as it deals with no encryption with medium complexity. The following parameters are used in the description of the model:

Quant (*quant*∈ [0, 1]): It is a parameter to represent the degradation due to quantization.

Scale Factor (*scaleFactor*∈ [0, 1]): This parameter is used to capture the upscaling degradation.

FrameRate *(framerate)*: It is the video rate in frames per second.

Display Resolution ***(disRes)***: It represents the video display resolution in number of pixels.
Coding Resolution ***(codRes)***: It is the video encoding resolution in pixels.

3.4.1 Quantization degradation

The Quantization Degradation D_q is defined as follows:

$$D_q = 100 - RfromMOS\ (\widehat{MOSq}) \quad (5)$$

where $RfromMOS$ is described as in [ITU-T G.107], and

$$D_q = \max(\min(D_q, 100), 0) \quad (6)$$

and where $\widehat{MOSq} = q_1 + q_2 . \exp(q_3 . quant) \quad (7)$

and $\widehat{MOSq} = \max(\min(\widehat{MOSq}, 5), 1) \quad (8)$

with $q_1 = 4.66$, $q_2 = -0.07$ and $q_3 = 0.06$

3.4.2 Upscaling degradation

The Upscaling Degradation D_u is defined as follows:

$$D_u = u_1 . \log10\ (u_2 . (\text{scaleFactor} - 1) + 1) \quad (9)$$

with $D_u = \max(\min(D_u, 100), 0) \quad (10)$

$$\text{scaleFactor} = \max\left(\frac{\text{disRes}}{\text{codRes}}, 1\right) \quad (11)$$

where $u_1 = 72.61$ and $u_2 = 0.32$.

3.4.3 Temporal degradation

The Temporal Degradation D_t is defined as follows:

$$D_t = \begin{cases} D_{t1} - D_{t2} - D_{t3}, & \text{framerate} < 24 \\ 0, & \text{framerate} \geq 24 \end{cases} \quad (12)$$

The pure temporal degradation is given by

$$D_{t1} = \frac{100 \cdot (t1 - t2 \cdot \text{framerate})}{t3 + \text{framerate}} \quad (13)$$

Compensation variable1, relative to coding impact is defined as

$$D_{t2} = \frac{Dq \cdot (t1 - t2 \cdot \text{framerate})}{t3 + \text{framerate}} \quad (14)$$

Compensation variable2, relative to spatial scaling impact is given by

$$D_{t3} = \frac{Du \cdot (t1 - t2 \cdot \text{framerate})}{t3 + \text{framerate}} \quad (15)$$

with

$$D_t = \max(\min(D_t, 100), 0) \quad (16)$$

where $t_1 = 30.98$, $t_2 = 1.29$ and $t_3 = 64.65$.

3.4.4 Integration

The Degradation (D) due to the quantization (D_q), upscaling (D_u) and temporal (D_t) factors are computed as:

$$D = \max(\min(D_q) + D_u + D_t, 100), 0) \quad (17)$$

The maximum quality in relation to the pure upscaling and temporal degradations is defined as follows:

$$\widehat{Qmax} = \begin{cases} 100 - D_u - D_{t1}, & \text{framerate} < 24 \\ 100 - D_u, & \text{framerate} \geq 24 \end{cases} \quad (18)$$

The quality (Q) is formulated as:

$\widehat{Q} = 100 - D =$

$$\begin{cases} 100 - \max\left(\min\left((100 - \widehat{Qmax}) + Dq - Dt2 - Dt3, 100\right), 0\right), & \text{framerate} < 24 \\ 100 - \max\left(\min\left((100 - \widehat{Qmax}) + Dq, 100\right), 0\right), & \text{framerate} \geq 24 \end{cases} \quad (19)$$

The estimated mean opinion score is calculated as:

$$\widehat{MOS} = \begin{cases} \widehat{MOSq}, & \text{if } Du = 0 \text{ and } Dt = 0 \\ \text{MOSfromR}(\widehat{Q}), & \text{otherwise} \end{cases} \quad (20)$$

where $\widehat{MOS}$ and $\widehat{Q}$ are the estimated video encoding qualities on two different scales: $\widehat{MOS} \in [1,5]$ and $\widehat{Q} \in [0,100]$.

The P_v module that estimates the video quality with ITU-T P.1203 model is shown in Figure 1. It combines quantization, frame rate, display and coding resolution to estimate the MOS.

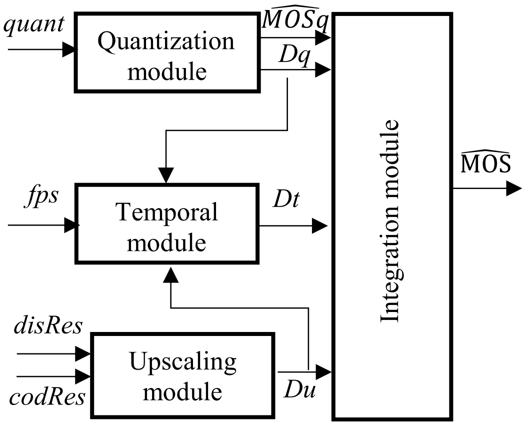


Figure 1 - P_v module in the ITU-T P.1203 model

4. PROPOSED ALGORITHM

4.1 DOUBLE SARSA BASED ADAPTATION ALGORITHM

The algorithm used at the client side for quality adaptation is described as follows:

1. Initialize the number of packets *N*, learning rate *α*, discount factor *γ*, Q-matrices Q^A and Q^B.
2. Identify the current state *s* based on throughput *Th* value using the mapping between throughput and states.
3. Read the resolution *codRes*, frames per second *framerate* at which the video is encoded from the codec header and determine the current action a using the mapping between throughput and states.
4. Perform calculations to obtain the quant parameter *(using Mode 2 calculation of ITU-T P.1203).*
5. Calculate the quantization degradation D_q, temporal degradation $\boldsymbol{D_t}$, upscaling degradation D_u, degradation *D* and the quality *Q*.
6. Assign the final Mean Opinion Score *MOS* obtained as the reward *r* gained for the current state *s* and current action *a*.

7. Compute new throughput *Th* and identify new state *s*' by the mapping between throughput and states.
8. Identify new action *a'* = *softmax(Q,s)* //Exploration policy function.
9. Update $Q^A(s,a) \leftarrow Q^A(s,a) + \alpha[r + \gamma Q^B(s',a') - Q^A(s,a)]$ // Double Sarsa
10. Set $s \leftarrow s'$ //Update new state as the current state
11. $a \leftarrow a'$ //Update new action as the current action
12. Send feedback (*a*) to server.
13. Repeat steps 2-12 until streaming continues.
14. End

4.2 EXPLORATION POLICY ALGORITHMS

Softmax(Q,s)

1. Initialize $\tau = 1$, *limit* = 0, *tot* = 0, *check* = 0 and an array *prb.*
2. For *i* = 1 to *prb.length*
3. *prb[i]* = $e^{\frac{Q^A[s,i]+Q^B[s,i]}{\tau}}$
4. *tot* = *tot* + *prb[i]*
5. For *i* = 1 to *prb.length*
6. *prb[i]* = *prb[i]* / *tot*
7. Generate a random value *rand*.
8. For *i* = 1 to *prb.length*
9. If *rand*>*limit* and *rand*<*limit* + *prb[i]*
10. *actionSelected* = *i*
11. *check* = 1
12. *limit* = *limit* + *prb[i]*
13. If *check = 0*
14. Repeat from step 7
15. Else
16. Return *actionSelected*
17. End.

ε-greedy(Q,s)

1. Initialize fixed probability *ε*, *max* (to store maximum value in s^{th} row of Q-matrix), *max_action*, *limit* = 0, *check* = 0 and an array *prb*.
2. For *j* = 1 to *no_of_actions*
3. If $Q^A[s,j] + Q^B[s,j]$ >= *max*
4. *max* = $Q^A[s,j] + Q^B[s,j]$
5. *max_action* = *j*
6. For *i*= 1 to *no_of_actions*
7. If *i* equals *max_action*
8. *prob[i]* = *1 – ε*
9. Else
10. *prob[i]* = *ε* / (*no_of_actions*– 1)
11. Generate a random value *rand*.
12. For *i* = 1 to *prb.length*
13. If *rand*>*limit* and *rand*<*limit* + *prb[i]*
14. *actionSelected* = *i*
15. *check* = 1
16. *limit* = *limit* + *prb[i]*
17. If *check* = 0
18. Repeat from step 11
19. Else
20. Return *actionSelected*
21. End

4.2 QoE DRIVEN VIDEO STREAMING STRATEGY WITH FUTURE INFORMATION

A probabilistic bandwidth prediction model along with QoE optimization [17] can be used in bitrate adaptation for future media segment in streaming. In starting phase, the first segment with the most minimal quality is asked by the receiver to decrease the startup delay. For all the accompanying portions, the adaptation technique would choose the quality level on the outcome of sub-optimization problem. The sub-optimization process chooses the quality level which maximizes the expected score for the internal QoE. The maximization of QoE score is based on a greedy search approach considering all possible quality patterns requested by the client.

The internal QoE score clubbed with the probability of bandwidth pattern is used to generate the expected QoE. A normalized buffer change factor is defined to be incorporated into the internal QoE. After making, the demand is communicated to the server. If there is starvation at client buffer, the most minimal quality level is asked for to lessen delay. The algorithm is as follows:

1. Initialize the number of segments *N*, total number of available quality level *M*, total number of available bandwidth state *L*, the transition matrix *A*, and the number of future segments involved in the decision for current segment *l*.
2. Select the lowest quality level for $q_i = Q_1$, bandwidth level $b_i = r_{i1}$ i.e., the bitrate of the segment where *i*=1.
3. If starvation occurs, goto step 2.
4. Select quality level which results in maximum expected internal QoE score:
   $max\text{QoE}^{\text{inter}}(\Psi_j)$ s.t. $j \in \{1,2,\ldots M^{l+1}\}$ (21)
5. For all the requested quality patterns $\{\Psi_1, \Psi_2, \Psi_3, \ldots. \Psi_{M^{l+1}}\}$ calculate the expected internal QoE score.
   $\text{QoE}(\Psi_j) = \sum_{i=1}^{3^{l+1}} QoE^{inter}(\Theta_i, \Psi_j) * P(\Theta_i)$ (22)
   where,
   $\text{QoE}^{\text{inter}}(\Theta_i, \Psi_j) = \text{E}(\Psi_j) - w_1\text{V}(\Psi_j) - w_2\text{P}^s(\Theta_i, \Psi_j) + \lambda\Delta\text{T}_i(\Theta, \Psi)$ (23)
   and $\text{P}(\Theta_i) = P_{b_{i-1}, b_i'} \times \prod_{j=0}^{l-1} P_{b_{i+j}', b_{i+j+1}'}$ (24)
6. Request the quality pattern Ψ_j with the maximum expected internal QoE score.
7. Feed the requested quality level and the actual network bandwidth state into the next round of decision.
8. Calculate the average requested media quality *E*(Ψ) using
   $\text{E}(\Psi) = \frac{1}{N}\sum_{i=1}^{N} q_i$ (25)
9. Calculate the quality switching frequency *V*(Ψ) as
   $\text{V}(\Psi) = \frac{1}{N-1}\sum_{i=1}^{N-1} |q_{i+1} - q_i|$ (26)

10. Calculate the starvation ratio $P^s(\Theta,\Psi)$ as the ratio between the total starvation time and the total display time defined as
$$P^s(\Theta,\Psi) = \frac{Ts(\Theta,\Psi)}{Tt(\Theta,\Psi)} \quad (27)$$
11. Calculate the overall QoE formulated as
$$QoE(\Theta,\Psi) = E(\Psi) - w_1V(\Psi) - w_2P^s(\Theta,\Psi) \quad (28)$$
12. Communicate the overall QoE to the server.
13. Continue through steps 3 – 12 till streaming occurs.

5. IMPLEMENTATION ENVIRONMENT

Eclipse IDE was used as the code development platform in Java programming environment based on 64 bit JDK Version 8, as it is platform independent and supports VLCJ framework. Dshow API [20] was used to capture the live video and processing it for streaming. The Java network packet capture library jNetPcap [21] was used to capture packets at the client. The server and client were connected using Reliance 4G Jiofi 3 LTE Hotspot [22] as a means of wireless network. At the server, during encoding, the frame rate was varied between 20 to 30fps with the default rate as 24fps, while adapted video resolutions were 240p, 360p, 480p, 720p and 1080p, confirming to ITU-T P.1203. The server was implemented in Acer laptop with an Intel Core i3 processor, 8GB RAM and Windows 8 64 bit operating system. The client was implemented in Lenovo ThinkPad laptop with an Intel Core i5 processor, 4GB RAM and Windows 7 Professional 64 bit operating system. The network speed of the 4G Jiofi 3 LTE Hotspot dongle was analyzed using the online tool Speedof.Me. One snapshot of download and upload speed observed during experimentation process is shown in Figure 2.

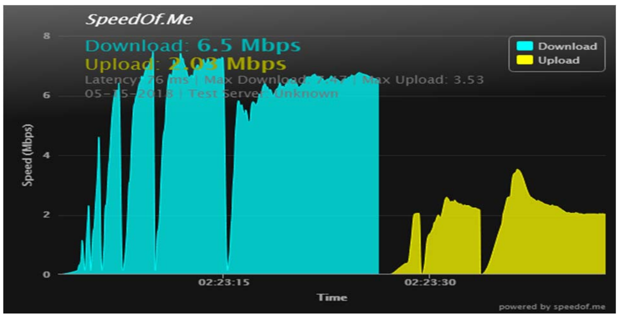


Figure 2 – A snapshot of observed bitrate

5. RESULTS AND DISCUSSION

Since the original video sequences were available during the experiment, the Full Reference (FR) metrics: PSNR, SSIM, MS-SSIM, and VQM were utilized to assess the system performance offline. The FR measurements give the most exact outcome as it is calculated with reference to the original video frames. The proposed Double Sarsa with two approaches was compared with the existing QoE driven strategy with future information. Although the experiments were run for several minutes during different trials, a random sample of 20 consecutive frames during live streaming have been captured and used for all different quality measurements discussed here.

6.1 Peak Signal to Noise Ratio (PSNR)

The calculation of PSNR depends on mean square error with respect to the maximum pixel value in a frame. Even if there is no loss of data in the channel, still PSNR could not be very high because server dynamically trims the original video as per the client feedback in order to improve QoE. The observed PSNR during the experimental process for three algorithms have been depicted in Figure 3. The Double Sarsa – Softmax (DS-S) approach shows an average PSNR of 7% higher than QoE Driven Strategy (QD-S), and 12.7% higher than Double Sarsa – Greedy (DS-G) approach. The DS-S approach performs better compared to the other two as it is able to adapt well in delivering higher quality with varying network bandwidth conditions.

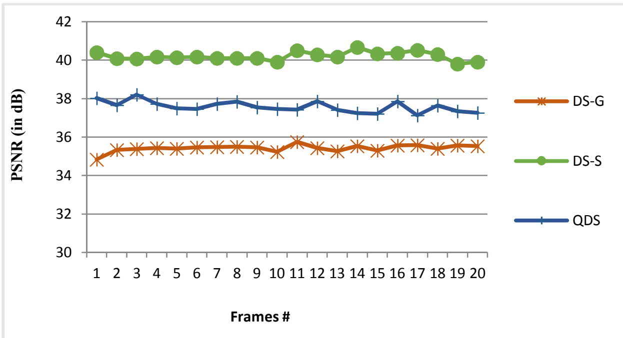


Figure 3 – The PSNR measurement

6.2 Structural Similarity Measurement (SSIM)

Although measurement of SSIM is more complex than PSNR, it provides a human perception based model considering luminance, contrast, and structure of the frame. Since pixels have high inter dependencies in the spatial neighborhood, it carries significant structural information of an object. The SSIM index was computed for the three algorithms (DS-S, DS-G, QD-S) and the results are plotted in the Figure 4. The proposed DS-S demonstrates average higher SSIM index value with 0.6% higher than the DS-G approach and 0.4% higher than QD-S. The higher SSIM index for the proposed algorithm is a reward for the perceived video quality.

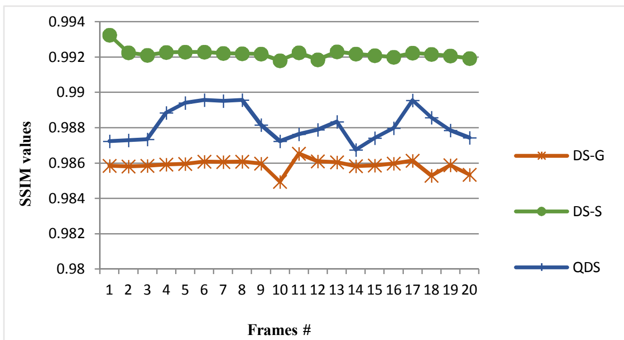


Figure 4 – The SSIM index values

6.3 Multi Scale Structural Similarity (MS-SSIM)

The MS-SSIM is computed over multiple scales through a process of multiple stages of sub-sampling, which is a reminiscent of multi scale processing in a vision system. It provides a suitable method to include details in a frame at different resolutions. The MS-SSIM score is computed as multiplication of weighted components at different resolutions. As shown in Figure 5, on an average DS-S algorithm provides 0.06% higher values than QDS and 0.15 % higher than DS-G algorithm.

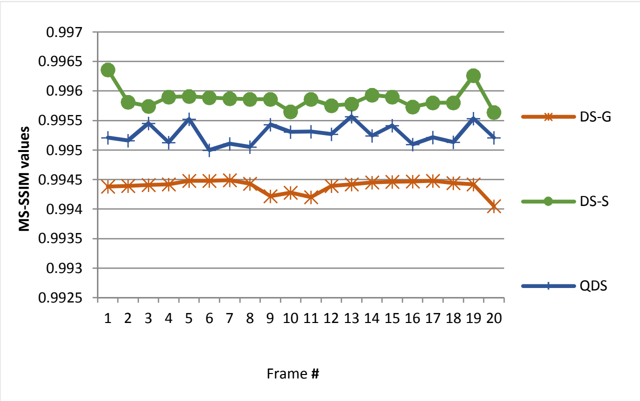


Figure 5 – The MS-SSIM index

6.4 Video Quality Metric

The perception effects of video impairments including blurring, jerky or unnatural motion, global noise, block distortion and color distortion can be measured by VQM. These impairment values can be combined into a single metric. The subjective quality assessment of the streamed video at receiver can be employed the VQM metric. Since the VQM score is the sum of many weighted parameters and its high value represents the maximum loss of quality in the video. As shown in Figure 6, the DS-S algorithm shows 25% VQM score values than QD-S and 41.5% lesser values than DS-G approach.

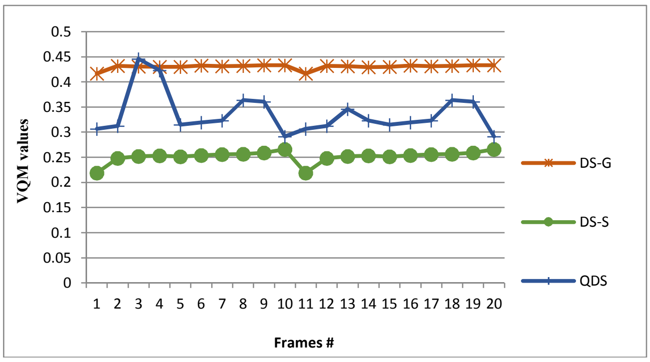


Figure 6 – The VQM Observation

6.5 Inter packet delay

Figure 7 shows the observed packet inter arrival delay on JioFi4G LTE-TD network during live video streaming. An average delay of 7.125 milliseconds was observed during the experimentation process.

6.6 Mean Opinion Score

The parametric bitstream-based quality assessment of adaptive audiovisual streaming services over reliable transport using video quality estimation module defined in ITU-T P.1203.1 provides output values on the 5-point ACR scale (MOS) per output sampling interval. It is a No Reference video quality estimation method that is utilized in the proposed approach as the reward function. The MOS values obtained are plotted in the Figure 8. An average value of 3.08 is observed in a network with fluctuating bandwidth conditions.

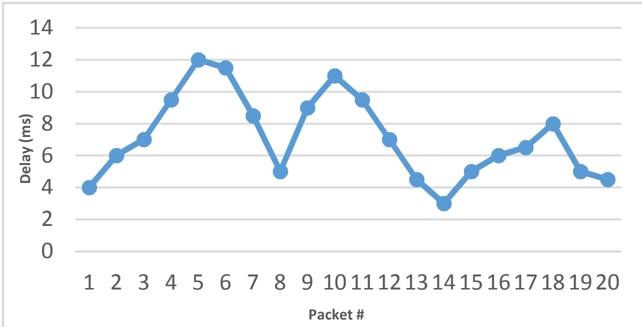


Figure 7 – Inter packet delay

6.7 Some Selected Original and Decoded Frames

Figure 9 shows the few original and decoded video frames captured during live streaming at the server and the client, respectively. The display resolution in this selected frame is 640*360 with the frame rate of 24. Because of high obtained PSNR noticeable changes absent in the decoded sequences. The live video streaming was carried out in a laboratory environment. The codec used for encoding and decoding process is H.264 for live as well as stored video.

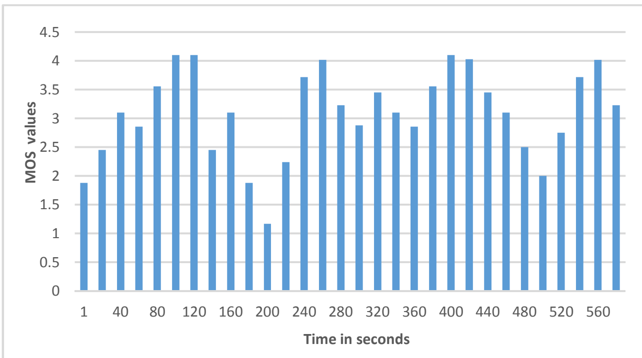


Figure 8 – MOS values

(a) Live video sequesces (original)

(b) Received video sequence (decoded)

Figure 9 – Some original and decoded frames during live streaming.

6. CONCLUSION AND FUTURE WORK

A HTTP adaptive streaming through 4G wireless network was implemented using Double Sarsa approach of reinforcement learning. To achieve the better QoE, the choices that are made to adjust video quality in a real time video streaming depend on the present condition of the system and the action to be selected in that state providing maximum reward. The proposed Double Sarsa based learning algorithm utilizing Softmax and e-greedy policy was developed and implemented utilizing ITU-T P.1203.1 model. The results were validated using FR video quality metrics and proposed method could be recommended in standardization of future audio-visual streaming services over wireless IP network. The system was implemented and tested in one way communication; however, it can undoubtedly be employed to facilitate two-way video communication.

7. REFERENCES

[1] Cisco Visual Networking Index: Forecast and Methodology, 2016–2021, Updated on June 6, 2017

[2] Ericsson Mobility Report, Interim Update, Nov. 2017. www.ericsson.com/mobility-report

[3] Global Internet Report, "Paths to Our Digital Future," Internet Society, 2017.

[4] ISO/IEC JTC 1/SC 29/WG 11, "Coding of Moving Pictures and Audio" ISO/IEC JTC 1/SC 29/WG 11 N12258, Dec. 2011.

[5] W. Huang, Y. Zhou, X. Xie, Di Wu, M. Chen, and E. Ngai, "Buffer State is Enough: Simplifying the Design of QoE-Aware HTTP Adaptive Video Streaming," IEEE Trans. on Broadcasting, vol. 64, no. 2, pp. 590 – 601, June 2018.

[6] G. Tian and Y.Liu, "Towards Agile and Smooth Video Adaptation in HTTP Adaptive Streaming," IEEE/ACM Trans. on Networking, vol. 24, no. 4, pp. 2386–2399, Aug. 2016.

[7] V.Martín, J. Cabrera, and N.García, "Design, optimization and evaluation of a Q-Learning HTTP Adaptive Streaming Client," IEEE Trans. on Consumer Electronics, vol. 62, no. 4, pp. 380 – 388, Nov. 2016.

[8] J.Nightingale, P. Salva-Garcia, Jose M. Alcaraz Calero, and Q.Wang, "5G-QoE: QoE Modelling for Ultra-HD Video Streaming in 5G Networks", IEEE Trans. on Broadcasting, vol. 62, no. 4, pp. 621 – 634, April 2018.

[9] M. De Filippo De Grazia, D. Zucchetto , A. Testolin, A. Zanella , M. Zorzi, and M.Zorzi, "QoE Multi-Stage Machine Learning for Dynamic Video Streaming," IEEE Trans. on Cognitive Comm. and Networks, vol. 4, no. 1, pp. 146–161, March 2018.

[10] M. Gadaleta, F. Chiariotti, M. Rossi, and A. Zanella, "D-DASH: A Deep Q-learning Framework for DASH Video Streaming," IEEE Trans. on Cognitive Comm. and Networking, vol. 3, no. 4, pp. 703-718 Dec. 2017.

[11] R. S. Sutton and A. G. Barto, "Reinforcement Learning: An Introduction," MIT Press Cambridge, Massachusetts, 2012.

[12] H.V. Hasselt, "Double Q-learning," Advances in Neural Information Processing Systems Conference on Neural Information Processing Systems (NIPS 2010), Dec. 2010.

[13] H. V. Hasselt, A. Guez and D. Silver, "Deep Reinforcement Learning with Double Q-learning", DOI: arXiv:1509.06461, Dec. 2015.

[14] M. Dumke, "Double Q(σ) and Q(σ,γ)Unifying Reinforcement Learning Control Algorithms", DOI: arXiv:1711.01569v1 5, Nov. 2017.

[15] M.Ganger, E. Duryea, and W.Hu, "Double Sarsa and Double Expected Sarsa with Shallow and Deep Learning", Journal of Data Analysis and Information Processing, vol. 4, no.4, pp. 159-176, Oct. 2016.

[16] ITU-T Recommendation P.1203, "Parametric bitstream-based quality assessment of progressive download and adaptive audiovisual streaming services over reliable transport", 2016.

[17] L.Yu, T.Tillo, J. Xiao, "QoE-Drien Dynamic Adaptive video Streaming Strategy with Future Information," IEEE Trans. on Broadcasting Society, vol. 63, no. 3, pp. 523 – 534, Sep. 2017.

[18] ITU-T Recommendation J.247, "Objective Perceptual Multimedia Video Quality Measurement in the Presence of a Full Reference," Aug. 2008.

[19] ISO/IEC JTC1/SC29/WG11 and ITU-T SG16 Q.6 JVT-AB031, "New Video Quality Metrics in the H.264 Reference Software," July 2008.

[20] "DirectShow (Windows)". https://docs.microsoft.com/en-gb/windows/desktop/DirectShow/directshow

[21] http://jnetpcap.sourceforge.net/docs/jnetpcap-1.0-javadoc/

[22] https://www.jio.com/shop/en-in/jiofi/p/491193576

SESSION 2

ARTIFICIAL INTELLIGENCE AND 5G

SELF-HEALING AND RESILIENCE IN FUTURE 5G COGNITIVE AUTONOMOUS NETWORKS

Janne Ali-Tolppa[1]; Szilard Kocsis[2]; Benedek Schultz[2]; Levente Bodrog[2]; Marton Kajo[3]

[1]Nokia Bell Labs, Munich, Germany
[2]Nokia Bell Labs, Budapest, Hungary
[3]Technische Universität München, Munich, Germany

ABSTRACT

In the Self-Organizing Networks (SON) concept, self-healing functions are used to detect, diagnose and correct degraded states in the managed network functions or other resources. Such methods are increasingly important in future network deployments, since ultra-high reliability is one of the key requirements for the future 5G mobile networks, e.g. in critical machine-type communication. In this paper, we discuss the considerations for improving the resiliency of future cognitive autonomous mobile networks. In particular, we present an automated anomaly detection and diagnosis function for SON self-healing based on multi-dimensional statistical methods, case-based reasoning and active learning techniques. Insights from both the human expert and sophisticated machine learning methods are combined in an iterative way. Additionally, we present how a more holistic view on mobile network self-healing can improve its performance.

Keywords – SON, cognitive network management, self-healing, anomaly detection, machine learning

1 INTRODUCTION

Mobile networks are becoming ever more complex, while the pressure for reducing the operational expenses and cost per bit is increasing. Network management automation is a key enabler for the increased dynamicity of the future 5G networks. Furthermore, the dynamic and complex future networks require automation that can autonomously adapt to changes in the context and in the environment, which necessitates the use of machine learning, analytics and artificial intelligence. [1]

Traditionally, the Self-Organizing Networks (SON) use cases are divided into three categories: self-configuration, self-optimization and self-healing. Self-configuration refers to automated, "plug and play" deployment of new network functions, which are implemented by SON functions such as the Automatic Neighbor Relationship (ANR) detection and Physical Cell Identifier (PCI) allocation. Self-optimization functions -- for example Mobility Robustness Optimization (MRO), Capacity and Coverage Optimization (CCO) and Mobility Load Balancing (MLB) -- optimize the network function configuration so that specified objectives are fulfilled. [2]

While self-optimization functions optimize a set of configuration parameters to improve the network performance from a given network state, the self-healing functions focus on ensuring that the system can fulfill its purpose and serve its customers even in case of unexpected changes or events that risk a degradation in the network performance. In other words, their objective is to make the network more resilient [3, 4, 5].

In this paper, we discuss the methods for improving resiliency in future 5G mobile networks and present a SON self-healing function applying automatic anomaly detection and diagnosis that enables detection of unexpected changes and events and allows fast reaction to them. Unlike in optimization, the self-healing functions can typically only monitor the symptoms of a fault and the causes are not a priori known. Due to this and the less-constrained problem space, the self-healing process is often more complex than the optimization control loops. This complexity is accentuated by the distributed and heterogenous nature of mobile networks. Finally, diverse fault states often occur only in very rare cases, which makes it impossible to collect statistically meaningful data for each case. The lack of statistical samples makes the reliable root-cause analysis extremely difficult. Therefore, mobile network self-healing functions typically require more sophisticated machine learning and augmented intelligence methods, as well as knowledge-sharing between domains. In our concept we've applied a holistic view on the network to detect the diverse problem states that may occur, as well as considered active and transfer learning methods.

The rest of the paper is structured as follows. In section 2, we present the main principles of resilient systems and how they map to the future cognitive mobile networks. Section 3 focuses on SON self-healing as an enabler for resiliency and gives an overview of the self-healing process. In sections 4 and 5, we look more closely to the most important phases of the self-healing process, namely the anomaly detection and diagnosis, respectively. Section 6 outlines how a more holistic view on the complete network, over several management areas, can improve the resilience of the system. A demonstrator evaluating the presented concepts is introduced in section 7 and in section 8 we present our conclusion and discuss future work.

2 ROBUSTNESS AND RESILIENCY IN MOBILE NETWORKS

Resiliency is the capability of a system to recover to a stable, functioning state after failure or adverse events [3]. It is not the same as robustness. A robust system is strongly designed to withstand any foreseen problems or failures, but may be too rigid and fail to survive and adapt in case of unforeseen circumstances, which are inevitably bound to happen in complex systems. For example, a farmer may prepare his crop against fire and flooding and local pests, but the crop can be destroyed by a foreign plant virus introduced in the environment. Paradoxically, a very robust system can be more susceptible to failure due to its increased rigidness and complexity [3]. Modern telephone networks are often said to be (together with electric power grids) among the largest and most complex human-created systems and their distributed nature makes them even more complex to manage and predict. Therefore, simple robust design principles (redundancy etc.) are not sufficient to ensure the ultra-reliable highly-available network performance required for many critical future use cases, for example remote surgery.

Resilient system, on the other hand, follow principles that allow them to recover even in case of completely unforeseen disastrous events. For example, by diversifying the crop, a farmer can ensure that a new plant virus will not be able to wipe out all the production. Typically, resilient systems follow a number of design principles [3]:

Monitoring and adaptation: Resilient systems must be responsive to change, and for that they need to monitor the system and detect changes early. An automatic anomaly detection system can profile and learn normal behavior at runtime and detect deviations from it, giving an early warning even in case of unforeseen circumstances. If connected to a diagnosis function, it can also trigger automatic corrective or mitigating actions. SON self-healing function based on anomaly detection and diagnosis are discussed in the following chapters.

Redundancy, decoupling and modularity: In addition to duplicating capacity for redundancy, resilient systems often have a decoupled and decentralized structure. In 5G RAN, one such approach is the RAN multi-connectivity. It is often utilized to increase the throughput, but can be also used to exploit the inherent macro-diversity effect of multiple simultaneous connections, such that the probability that at least one connection is sufficiently strong is increased [6].

Focusing: When changes are detected, resilient systems may focus on the problematic area to respond to a problem or a change. In network management, excess resources can be deployed where unexpected events are detected. Especially in telco cloud deployments, more fault management functions can be placed to more problematic areas.

Diverse at the edge, but simple at the core: Resilient systems may be very complex, but share simple common properties. The Internet, for example, consists of a very large number of very diverse services, some of them extremely complex, but they all communicate and interface with a simple set of shared protocols. In future mobile networks, a common data plane can provide such simplicity at the core. The data providers and consumers may operate in vastly different scopes and time durations, but be able to communicate with each other using the Service-Oriented Architecture (SOA) principles in a cloud-native architecture utilizing a common data sharing bus.

3 SELF-HEALING IN MOBILE NETWORKS

The simplest self-healing solutions are rule-based systems, where specified automated corrective workflows are triggered, when given trigger conditions are fulfilled. Such systems, however, can reliably work only on anticipated problems and typically fail to perform well in completely unforeseen circumstances. Furthermore, the creation and maintenance of the rule base is expensive and laborious. It may even make the system more *rigid* and thus less resilient.

The rules, which corrective actions to trigger, could be learned using machine learning, as a classification problem. Each state is classified either as normal or to a degraded state connected to one of the corrective workflows. However, since the anomalous states are, by definition, rare, the detection model is learned on a skewed training dataset. It may also fail to recognize new, unforeseen problematic states. Another problem is the availability of such labelled training datasets.

Therefore, self-healing functions are often implemented as a four-stage process: profiling the normal states of the system, detecting deviations from the normal (anomalies), diagnosis and acting. The advantage of learning the normal behavior is that any deviations from it, even unforeseen ones, can be detected. On the other hand, not all deviations are degradations and so a diagnosis function is required to diagnose the detected anomalies and connect them to possible corrective actions. Additionally, to adapt to trend and seasonal changes in the normal network behavior, for example to the evolution in the network traffic characteristics, the profiles for the normal states need to be continuously updated.

In Radio Access Networks (RANs), resources are typically more scarce and it is often not possible to achieve desired level of resilience simply by means of overprovisioning of resources. The available spectrum, for example, is limited and cannot be extended. Therefore, in addition to methods like multi-connectivity [5], self-healing solutions can be especially important in RAN to enable the required level of reliability.

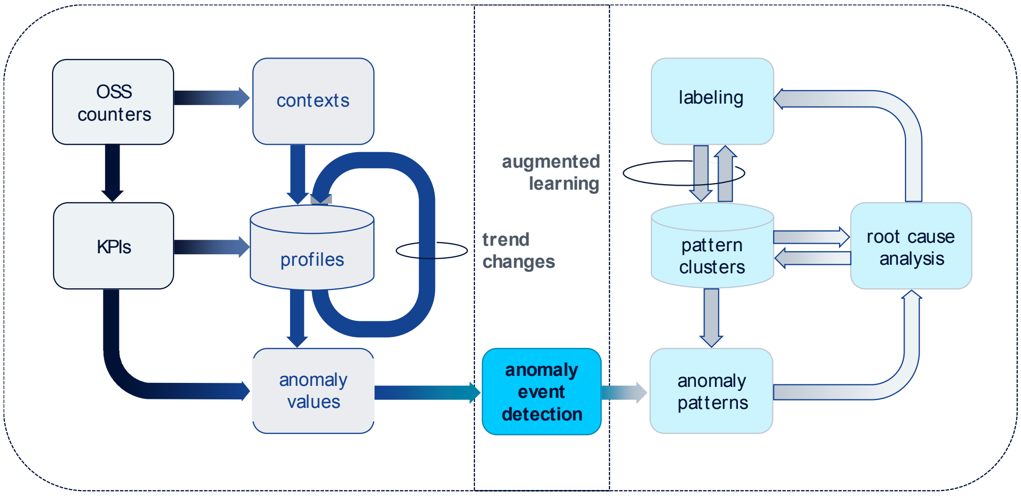


Figure 1 – Anomaly detection and diagnosis

Figure 1 shows an overview of our anomaly detection and diagnosis function for Radio Access Networks (RANs). Profiling, detection and diagnosis are done per selected contexts, for example per cell and distinguishing between workdays and weekends. The intended deployment resides on NM-level and analyzes Performance Management (PM) data collected from a Network Management System (NMS). The collected Key Performance Indicators (KPIs) are typically aggregated with minutely or hourly granularity. Note that the concept allows also other deployment options.

Once the profiles are created, an *anomaly level* is calculated for each KPI in each cell against the profiles for the collected time series samples. Based on the anomaly levels, distinct anomaly events are detected. An anomaly event only indicates that something unusual has occurred, but not necessarily a network performance degradation or other event that would require corrective actions. Therefore, the detected anomaly events are analyzed by a diagnosis function, which connects the detected anomalies to the most like root cause(s). Once the causes of the anomaly are known, they may be connected to corrective workflows. In the next two sections we look closer at the two main steps of this process, the anomaly detection and the diagnosis, for RAN self-healing.

4 ANOMALY DETECTION IN RADIO ACCESS NETWORKS

The basis on which an anomaly detection algorithm marks an event anomalous is subject to learning. The model that captures the learned normal behavior is called a profile. Depending on the anomaly detection algorithm profiles may be of various kinds: in [7] the profiles are statistical models of normal distributions with fitted set of parameters, whereas in [8] the profile consists of cluster centroids in an encoded feature space. The choice of profiling algorithm is dependent on application specific design choices that need to be considered, some of these considerations are:

- The implementation architecture, e.g. distributed or centralized
- Is any labelled data available or is the learning fully unsupervised, i.e. based on the assumption that common or average network states are normal
- The scope of the profiling: e.g. individual network element, subsets of similar network elements or one baseline for all network elements
- The profiled features and their distributions
- Is the whole feature set considered as one high dimensional distribution or only subsets of them?
- Should the profiles be understandable and intuitively interpretable

For the RAN anomaly detection algorithm that is based on [7], we decided that profiling would be on individual cell-level and based on sub-sets of features. These choices made the algorithm applicable for distributed implementation and computationally less demanding. The consideration of sub-sets of features for a profile also made the results and the profiles more interpretable. Additionally, individual profiles were created for work days and weekends. This means that we create two profiles for each cell.

The algorithm uses two kinds of profiles: the diurnal profile considers the daily seasonality of the KPIs, while the cross-correlational profile captures the correlation relationship of KPIs. The underlying algorithm is the same for the two types of profiles, the difference is the input data for the algorithms. The diurnal profiling considers one KPI for one profile and for each hour of the day captures the distribution with statistical models, whereas the cross-correlational profile considers two or more KPIs together and captures the joint distribution of the KPIs.

The **Figure 2** illustrates the two types of profiles for a cell: the diurnal pattern caused by the human life-cycle is

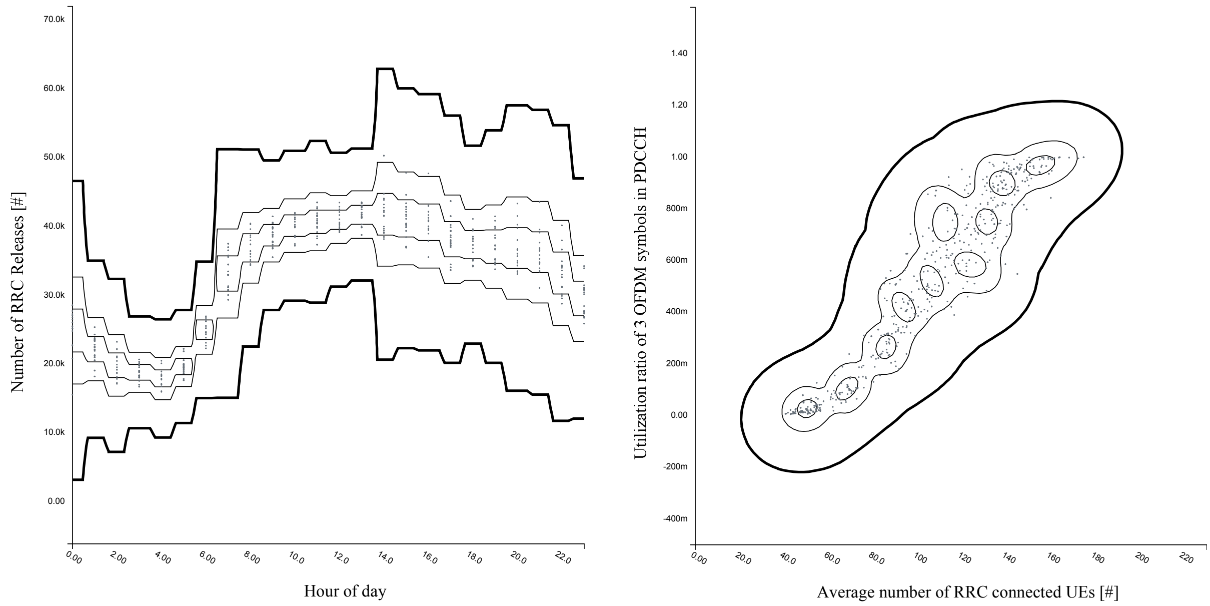


Figure 2 – Diurnal and cross-correlational profiles

observable on the left, while a nonlinear dependency pattern can be observed on the right that resembles the enclosed area of a hysteresis curve. The ellipse curves represent quanta in the profile to which bivariate normal distributions have been fitted respectively. The diurnal profile does not contain ellipse curves: one-dimensional normal distributions were fitted to each hour of day in that case. The continuous curves represent 1, 2.5 standard deviations distance from the profiles, while the thicker curve is the parameterizable boundary for detection. Let's look at the two-dimensional correlation profiles more in detail in the next sub-sections, while the diurnal profiling is described in [7] and [9].

4.1 Fitting profile centroids

For each profile, the number of centroids (N_{cent}) to be fitted needs to be set. The N_{cent} parameter determines the number of bivariate normal distributions to be fitted, hence the granularity of the model, which has a regularizing effect as well. The N_{cent} centroids are divided among the number of larger initial clusters – created in the so-called pre-clustering using the Density-Based Spatial Clustering of Applications with Noise (DBSCAN) algorithm – proportional to the area of each cluster.

If the set of DBSCAN clusters is C^{DB}, then for each $C_i^{\text{DB}}, i \in \{1, 2, \ldots, |C^{\text{DB}}|\}$ cluster, N_i^{DB} bivariate normal distributions are fit. For partitioning the points into N_i^{DB} sets for a C_i^{DB} cluster in the current implementation two choices are available:

- Fitting an $N_i^{\text{DB}} \times 1$ SOM, then the best matching units (BMU) for each node define the partitions.
- Performing k-means clustering with $k = N_i^{\text{DB}}$, the resulting clusters being the partitions

At this point we have the $P_j, j \in \{1, 2, \ldots, N_i^{\text{DB}}\}$ partitions of data points for each C_i^{DB}. For the data points in each P_j we fit a bivariate normal distribution ($N(\boldsymbol{\mu}_j, \boldsymbol{\Sigma}_j)$):

$$\boldsymbol{\mu}_j[1, l] = \text{mean}(\mathbf{P}_j[:, l]), \qquad l \in \{1,2\}$$

$$\boldsymbol{\Sigma}_j = \text{cov}(\mathbf{P}_j)$$

Vectors $\hat{\mathbf{v}}_1$and $\hat{\mathbf{v}}_2$ are the two eigenvectors, λ_1 and λ_2 are the two eigenvalues of $\boldsymbol{\Sigma}_j$ (which are result of spectral decomposition). The profiles are stored as triple of vectors $\boldsymbol{\mu}_j, \mathbf{v}_1 = \sqrt{\lambda_1}\hat{\mathbf{v}}_1$ and $\mathbf{v}_2 = \sqrt{\lambda_2}\hat{\mathbf{v}}_2$ for each centroid.

4.2 Anomaly value calculation

For each profile, bivariate normal distribution, $N(\boldsymbol{\mu}, \boldsymbol{\Sigma})$, is characterized by its vector valued mean and its covariance matrix.

$$N(\boldsymbol{\mu}, \boldsymbol{\Sigma}) = \boldsymbol{\mu} + \mathbf{V}\boldsymbol{\Lambda}^{\frac{1}{2}}N(0, \mathbf{I}) = \boldsymbol{\mu} + \mathbf{T}N(0, \mathbf{I})$$

$\mathbf{V} = (\hat{\mathbf{v}}_1 \quad \hat{\mathbf{v}}_2)$ consists of the eigenvectors of the covariance matrix and

$\boldsymbol{\Lambda} = \begin{pmatrix} \boldsymbol{\lambda_1} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{\lambda_2} \end{pmatrix}$ consists of the corresponding eigenvalues

From now on, let $\mathbf{c}_i = \boldsymbol{\mu}_i$ denote the ith profile centroid identical to the mean of the ith bivariate normal distribution fit to the cluster members.

Observing $\mathbf{p}$, a pair of KPI values, its anomaly value component, with regards to the largest standard deviation of the ith profile centroid, is determined as the number of standard deviations the $\mathbf{p}$ deviates from the centroid

$\mathbf{a}_i = \mathbf{T}_i^{-1}(\mathbf{p} - \mathbf{c}_i) = \mathbf{\Lambda}_i^{-1/2}\mathbf{V}_i^{-1}(\mathbf{p} - \mathbf{c}_i)$.

The anomaly value components, one for each profile centroid, are then aggregated in the following way.

Let us denote n the number of profile centroids and $\mathbf{d}_i = \mathbf{p} - \mathbf{c}_i, i \in \{1, \dots, n\}$, the distance vector of the observed KPI-pair, $\mathbf{p}$, from the ith profile centroid. The Euclidean distance is then calculated as $d_i = |\mathbf{d}_i|, i \in \{1, \dots, n\}$ among which the closest one is determined as $d_{\min} = \min_{i \in \{1,\dots,n\}} d_i$.

Using the lengths $a_i = |\mathbf{a}_i|, i \in \{1, \dots, n\}$ of the anomaly components, the resultant *per KPI anomaly value* is the weighted sum

$$\alpha = \frac{\sum_{i=1}^{n} w_i a_i}{\sum_{i=1}^{n} w_i},$$

$$w_i = \mathrm{e}^{\left(\frac{d_i - d_{\min}}{b\, d_{\min}}\right)^2} \; \forall i \in \{1, \dots, n\}, b = 0.5$$

4.3 Anomaly Event Detection

The goal of the anomaly event detection is to detect, as the name implies, distinct anomalies, which belong to the same underlying event, based on the anomaly level timeseries values of the profiled features. First, for each profiled feature or KPI, anomalous timespans are detected using the DBSCAN algorithm. An observation for feature k at time T is considered anomalous if the *anomaly value density* $A_k(T)$ goes above a given threshold $MinPts, i.e.$:

$$A_k(T) = \int_{T-\varepsilon}^{T+\varepsilon} |\alpha_k(t)| dt > MinPts.$$

, where ε is time window, in which the anomaly density is calculated.

The start time $S_{j,k}$ of the anomaly comes from the above definition, i.e. it is when the anomaly density exceeds the threshold set by the *MinPts*. All subsequent points until end of event $T_{j,k}$, where the density remains above it are considered as part of the same event. The severity value of the anomaly, for quantification purposes, is calculated as

$$v_{j,k} = \sum_{S_{j,k} \le t \le T_{j,k}} A_k(t).$$

5 DIAGNOSIS

There is a vast diversity in the possible fault states that may occur in a complex system like a mobile network. Therefore, many of the fault states can be exceedingly rare. The lack of statistical samples makes the reliable automated analysis of the faults and the finding of the corrective actions extremely difficult. And since we want to prepare also for the unexpected and unprecedented, we need to combine machine learning with insights and the intuition of a human expert. We've developed a diagnosis concept, where we use *augmented intelligence*, *Case-Based Reasoning (CBR)* and *active learning* methods to dynamically build and maintain a diagnosis knowledgebase, which can be utilized for both, autonomous self-healing actions as well as supporting a human expert troubleshooting a network issue.

5.1 Diagnosis with case-based reasoning

First, the detected anomaly events are described for diagnosis with an *anomaly pattern*. The anomaly pattern can consist of the features (KPIs) used in the detection phase, but typically it is an extension of these. As a medical analogy, fever is a good indicator of an illness, but for a diagnosing which illness it is, more information is required. In our implementation, the averaged anomaly levels of an extended set of network KPIs were used. The anomaly pattern should capture as many aspects of the anomaly event as possible.

Next, the observed anomaly pattern is compared against the already analyzed and labelled anomalies stored in the *diagnosis knowledgebase*. The closest matching labelled anomaly pattern or patterns are found, in the sense of similarity, and given as the most likely automated diagnosis. Different distance measures were tested and in the end a combination of Euclidean and cosine distances was used. The distance measure gives the probability of the diagnosis. **Figure 3** depicts two anomaly patterns as a radar chart. Each segment of the chart corresponds to a diagnosis feature. The outer blue area is the observed anomaly event and the inner orange area is the closest matching labelled anomaly in the knowledgebase. The darker innermost circle is the expected value for each feature and the actual observation can of course be either above or below it.

5.2 Active learning in the diagnosis process

Such CBR-based diagnosis function allows the diagnosis knowledgebase to be developed and expanded dynamically

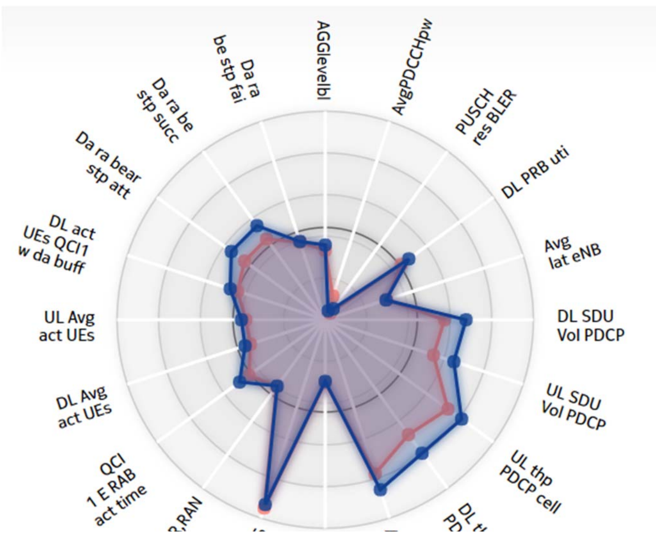


Figure 3 – An anomaly pattern for an observed anomaly event compared against a label in the diagnosis knowledgebase

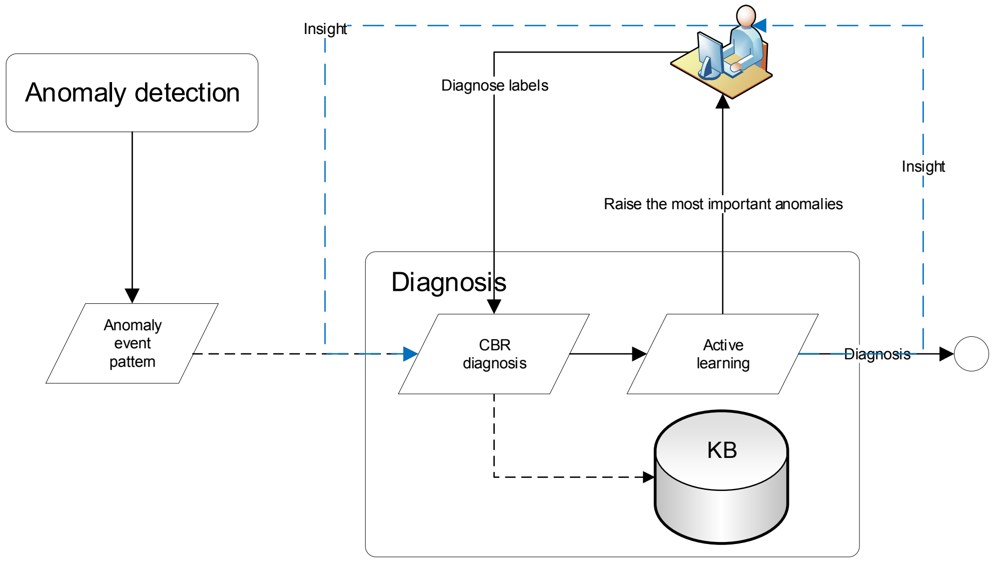


Figure 4 – An overview of active learning in the diagnosis process

during operation. As analyzed anomaly patterns are added, the quality of the automated diagnoses improves. The collection and maintenance of a sufficient knowledgebase can be, however, expensive and time-consuming. To mitigate this process, active learning methods can be used. In active learning, the system raises those cases to be analyzed and labeled by the human expert that are the hardest for the diagnosis function to diagnose or that would improve the quality of the diagnosis knowledgebase the most. This way it can guide the human expert diagnosis process to analyze the anomalies that are the most meaningful for the automated diagnosis.

Figure 4 shows an overview of active learning in the diagnosis process. The black dotted lines depict the flow of data and the continuous blue lines the insights shared between the machine analytics and human expert. The iterative process works as follows:

1. Initially, the detected anomalies are diagnosed by the CBR-based diagnosis.
2. The diagnosis results are fed to the active learning component, which analyzes, which diagnosed anomalies are the most relevant to be raised to the human operator, i.e. the ones where the automatic diagnoses are the most unreliable or the ones which are on the border of different diagnoses.
3. The human expert analyzes the raised cases and provides the analysis results as new labeled and diagnosed anomaly patterns into the diagnosis component.
4. Steps 1-3 are repeated for**:**
   a. **Refining** the labelling of existing anomalies
   b. Incorporation of **newly detected anomalies** in the labelling

5.3 Transfer Learning

Because the fault states can be very rare, even with the augmented diagnosis it can be difficult and time-consuming to create a comprehensive diagnosis knowledgebase. It would also be highly desirable to be able to diagnose and quickly remedy or even prevent problems that have never occurred in the system before. One way to enable this is to use *transfer learning* to share diagnosis knowledge between different networks.

[10] describes a framework for sharing diagnosis knowledge and presents an example using topic modeling and Markov Logic Networks (MLNs). It defines three components for a diagnosis cloud: Central, Gateway and Local Diagnostic Agents (CDA, GDA and LDA). The GDA is an agent mapping models between the CDA's central storage of models and the local models in an LDA. Sharing knowledge between diagnosis knowledgebases enables fast "bootstrapping" of completely new self-healing deployments, or updating an existing one, for example when managed network functions go through major upgrades. It raises also the question, how such diagnosis knowledge can best be shared. Standardized knowledge sharing methods may be required in addition to sharing data.

6 HOLISTIC SELF-HEALING

Another recurring principle in resilient systems is holism. In a complex system, improving the resilience of only one part or level of organization can sometimes (unintentionally) introduce fragility in another. To improve the resilience, it is often necessary to work in more than one domain and scale at a time. [3]

In mobile network management, this means we cannot consider different management domains and levels in isolation. The different management areas, although operating on different time scales and on different managed objects, need to be able to share knowledge and make a holistic picture of the whole system, for example:

- **Quality of Service (QoS) and Quality of Experience (QoE) driven management:** Optimizing the end-to-end customer experience at the application and individual subscriber level
- **Network Management (NM):** Management automation aggregated on a (Virtual) Network Function (V)NF level
- **VNF and Service Orchestration**: Orchestration of cloud resources, CPU cores, memory, storage, links etc.

To give an example, consider the corrective actions done by a QoE-driven self-healing function in a transport network SON system described in [11]. It can re-route traffic past problematic links at a very fast pace. If there are underlying issues necessitating such re-routing, however, which are not corrected, it may eventually happen that the QoE management system is no longer able to fulfill the customer expectation with the available resources. The network will fail and the danger is that because it is failing at a later and potentially more escalated stage of the problem, the failure will be more catastrophic and more difficult to troubleshoot. If you are failing, it is often better to fail fast.

Our solution for a more holistic view, enabling early detection of any issues, is to have the NM-level self-healing function monitoring the corrective actions performed by the QoE-driven, application and user centric backhaul SON system. The actions are modelled and aggregated as additional KPIs that are used as input features for the NM SON self-healing, in addition to the normal NM-level alarms and performance KPIs. Several corrective QoE-driven actions may be an indication of an emerging problem, especially if occurring together with other indicators for a network performance degradation. This may be further extended to cover also VNF orchestration, for example. The different management areas can collaboratively monitor each other's corrective actions or determine the best course of action in a cooperative manner. This also enables coordination of the actions taken by different management agents on different management areas.

Therefore, mechanisms and KPIs to communicate manage decisions and actions between management areas are required. The management functions may be created by different vendors, which may raise a need for standardization.

7 SON EXPERIMENTAL FRAMEWORK

The presented concept was demonstrated in a tool called the SON Experimental Framework (SEF) [12]. It is a framework implemented in the R-language that can be integrated to different data sources. For evaluation, data collected from real operator networks was used, as well as live integrations to networks and testbeds. The system provides a web UI that can be used to visualize the whole profiling, anomaly detection and diagnosis process.

The collaborative self-healing with a QoE-driven backhaul SON system was evaluated in a test network, where a ground truth could be established. Delay of different network segments as well as radio KPIs such as the Channel Quality Indicator (CQI) were monitored in both the anomaly detection and diagnosis. The testbed consisted of two cells.

Test runs consisted of three-day cycles, where the first day the network was in a normal state, the second a radio attenuation condition was present and on a third a Software Defined Network (SDN) misconfiguration was introduced in the radio backhaul network. The three-day cycle was repeated four times, while constantly increasing background traffic (video streaming). When the background traffic volume was low, the self-healing mechanisms of the backhaul SON solution could mitigate the problems caused by the radio attenuation and the SDN misconfiguration so that the end user experience was not affected. However, when the background traffic was increased, on the last three-day cycle the available resources become insufficient for the backhaul SON to correct the degradations. This is shown in **Figure 5**. The horizontal axis shows the aggregated throughput demand of a cell in Mbps and the vertical the actual throughput. The shaded area is normal correlation between the demand and the actual throughput, as profiled by the SEF. As can be expected, normally the actual throughput follows the demand. The points in the scatter plot represent the observations after profiling. We can see that a set of points transgress the profile boundary, indicating an anomaly, where the cell cannot provide the throughput required.

Figure 6 shows the anomaly-level and anomalies detected by SEF during the last four days in the test run. SEF is monitoring both the NM KPIs and KPIs indicating the actions taken by the backhaul SON. The shaded areas are the anomalous timeframes detected by SEF.

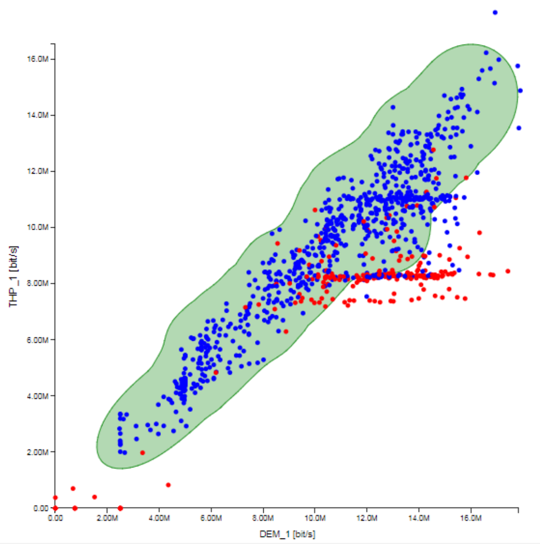


Figure 5 – Service degradation as detected by SEF

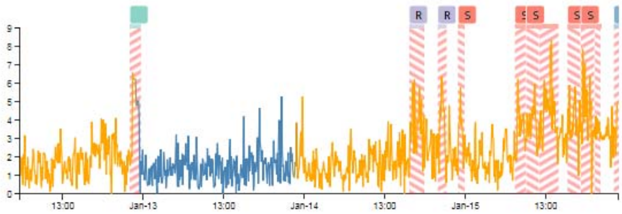


Figure 6 – Anomaly le1vel and anomalies detected by SEF compared to labelled problem states

We can see that it detected the degradations on the last two days, but that in addition an anomaly is raised already during the second-last three-day cycle, giving an early warning on the impeding problem that the QoE-driven backhaul SON is no longer able to resolve. The automated diagnosis of SEF can distinguish between the radio and transport network degradations and appropriate corrective actions can be taken. The deployment of corrective actions will be studied as future work.

8 CONCLUSIONS AND FUTURE WORK

In this paper, we argued that to be able to meet the reliability requirements of future 5G use cases, such as for the ultra-reliable communications, the networks need to be resilient also against unforeseeable problems. We introduced the wider context of resilience in 5G networks and presented our anomaly detection and diagnosis based self-healing concept, which enables early detection of and reaction to problems in a dynamic way. The method is generic and can be applied to other radio technologies as well, e.g. to LTE. We discussed how active and transfer learning methods can be used to mitigate the diagnosis knowledgebase collection effort and to combine the insights from both machine learning based analytics and the human expert. Furthermore, we presented a holistic self-healing method over several management areas as an enabler for a truly over-arching and resilient solution for self-healing. Such over-arching methods require not only the transfer of data, but transfer of knowledge, for example of the anomaly patterns and their diagnosis labels or features indicating the corrective actions executed on different management areas, between organizations and vendors. Lastly, we introduced the SON Experimental Framework (SEF), where the self-healing capabilities have been implemented and demonstrated using data from real network instances as well as in live integrations. In SEF, we also evaluated the cooperative self-healing between QoE-driven backhaul and Radio Access Network Management SON functions. In our future work, the transfer learning methods will be also further studied in the context of self-healing as well as looking into the deployment of corrective actions.

9 REFERENCES

[1] S. Mwanje, G. Decarreau, C. Mannweiler, M. Naseer-ul-Islam, L. C. Schmelz, "Network management automation in 5G: Challenges and opportunities", PIMRC, Valencia, 2016

[2] H. Sanneck, S. Hämäläinen, C. Sartori, "LTE Self-Organizing Networks", Wiley 2012.

[3] A. Zolli, A. M. Healy, "Resilience – Why Things Bounce Back", Headline Publishing Group, 2012.

[4] A. Berns, S. Ghosh, "Dissecting Self-* Properties", Third IEEE International Conference on Self-Adaptive and Self-Organizing Systems, 2009

[5] S. S. Laster, A. O. Olatunji, "Automic Computing: Towards a Self-Healing System", Proceedings of the Spring, 2007

[6] D. Michalopoulos, B. Gajic, B. Crespo, A. Gopalasingham, J. Belschner, "Network Resilience in Virtualized Architectures", 11th International Conference on Interactive Mobile Communication Technologies and Learning (IMCL), 2017

[7] L. Bodrog, M. Kajo, S. Kocsis and B. Schultz, "A robust algorithm for anomaly detection in mobile networks," 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Valencia, 2016, pp. 1-6.

[8] Caglar Aytekin, Xingyang Ni, Francesco Cricri, Emre Aksu, "Clustering and Unsupervised Anomaly Detection with L2 Normalized Deep Auto-Encoder Representations", International Joint Conference on Neural Networks (IJCNN), 2018

[9] G. Ciocarlie, U. Lindqvist, S. Nováczki & H. Sanneck, "Detecting Anomalies in Cellular Networks Using an Ensemble Method", 9th International Conference on Network and Service Management (CNSM 2013), pp. 171–174.

[10] G. Ciocarlie et. al., "Diagnosis cloud: Sharing knowledge across cellular networks", 12th International Conference on Network and Service Management (CNSM), Montreal, 2016

[11] L. Bajzik, C. Deak, T. Karasz, P. Szilagi, Z. Vincze, C. Vulkan, "QoE Driven SON for Mobile Backhaul Demo", 6th International Workshop on Self-Organizing Networks (IWSON), 2016

[12] L. Bodrog, M. Kajo, S. Kocsis, B. Schultz, "Demonstrator of KPI Analytics for Anomaly Detection and Diagnosis in Mobile Networks", The 28th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE PIMRC), Montreal, 2017

AI AS A MICROSERVICE (AIMS) OVER 5G NETWORKS

Gyu Myoung Lee[1], Tai-Won Um[2], Jun Kyun Choi[3]

[1]Liverpool John Moores University (LJMU), g.m.lee@ljmu.ac.uk
[2]Chosun University, Corresponding author, twum@chosun.ac.kr
[3]Korea Advanced Institute of Science & Technology (KAIST), jkchoi59@kaist.edu

ABSTRACT

As data-driven decision-making services are being infused into Internet of Things (IoT) applications, especially at the 5G networks, Artificial Intelligence (AI) algorithms such as deep learning, reinforcement learning, etc. are being deployed as monolithic application services for autonomous decision processes based on data from IoT devices. However, for latency sensitive IoT applications such as health-monitoring or emergency-response applications, it is inefficient to transmit data to the Cloud data centers for storage and AI based processing. In this article, 5G integrated architecture for intelligent IoT based on the concepts of AI as a microservice (AIMS) is presented. The architecture has been conceived to support the design and development of AI microservices, which can be deployed on federated and integrated 5G networks slices to provide autonomous units of intelligence at the Edge of Things, as opposed to the current monolithic IoT-Cloud services. The proposed 5G based AI system is envisioned as a platform for effective deployment of scalable, robust, and intelligent cross-border IoT applications to provide improved quality of experience in scenarios where real-time processing, ultra-low latency and intelligence are key requirements. Finally, we highlight some challenges to give future research directions.

Keywords – AIMS, Microservice, AI, 5G

1. INTRODUCTION

Over the last decade, the number of Internet-enabled devices has run into billions, in fact exceeding the number of people on the planet. The emergence of these devices and the large volume of data they generate have a significant impact on our day-to-day existence in diverse ways. Thus, with this development and the success of Cloud computing, a whole new networking paradigm has emerged known as the fifth generation wireless networks (5G), leading to the development of completely new platform for large scale distributed applications and mobile services in variety of application domains such as the Smart City, Smart Grid, Healthcare Monitoring, intelligent transport, Smart manufacturing, etc., exploiting the humongous data generated by the "smart" objects [1].

A microservice is a software development technique that structures an application as a collection of loosely coupled services. Decomposing an application into different smaller services can improve modularity and make the application easier to develop and deploy [2].

In this article, we propose a new concept of AI as a microservice (AIMS) as an IoT data-driven intelligence-provisioning infrastructure with the 5G capability to provide intelligent connectivity as services closer to the Things by leveraging resources of emerging computing technologies like Real-time Onsite Operations Facilitation (ROOF) [3], Fog [4] and Edge computing. The AI services will be provided as microservices, implementing lightweight functions that have been factored from the AI algorithms or processes. We envision the proposed system to allow AI functionality to be infused into 5G networks as distributed, composable microservices consisting of independent virtual components that can be deployed on the federated ROOF-Fog-Cloud continuum to improve scalability, interoperability and cutting down latency for real-time 5G applications. Thus, the proposed 5G integrated platform allows AI services to be provided seamlessly not only at the centralized data centers but essentially, also at the edge, closer to the IoT devices. The system and its concepts advocate an architectural principle based on the abstraction that provides end-to-end fabrics for composing, provisioning, deploying, managing and monitoring AI services regardless of whether such services are composed from the ROOF, Fog or cloud microservices. The proposed 5G architecture allows hierarchical and horizontal federation of smaller data centers from the Edge to the Cloud data centers continuum so that AI features and functions can be incrementally composed from microservices in such hierarchy as dictated by the required and available networking and computing resources at the ROOF and Fog levels to independently execute such AI functions. In fact, this architectural design would allow cross-border microservices to be composed from different local ROOF and Fog microservices over 5G network slices.

The remainder of this article is organized as follows. Background information on 5G networks and distributed Cloud is provided in Section 2. The proposed AIMS infrastructure is described in Section 3. Section 4 shows AIMS use cases. In Section 5, we highlight some challenges to give future research directions. Finally, we summarize our work in Section 6.

2. BACKGROUND

One major enabler of AIMS is the integration of 5G and Cloud computing, enabling the 5G applications to leverage the abundant compute and storage power of the geo-distributed Cloud data centers.

One of the widely researched challenges relates to how heterogeneous services and their operating platforms can interoperate on the same network. However, various research enthusiasts are aggressively addressing these “5G Vertical” challenges to enable the development of network slicing, multi tenancy, network programmability [5]. One of the main weaknesses of the solutions in this regard is that they still rely on transporting humongous IoT data across the 5G networks to various cloud data centers for storage or processing. We have identified the negative impacts and challenges of this model as follows:

- Latency sensitive nature of the Edge based application services necessitates that real-time decisions based on the acquired data from the Edge devices requires mechanisms for real-time processing of data for real-time intelligence [6]. How do we design, model and expose these intelligent services for decision making at the Edge of Things to address latency related problems of AI services across the 5G networks?

- Intelligent decision making at the Edge of Things introduces new AI dimension to IoT services such as real-time local processing of IoT data for quick intelligent decision making without necessarily transporting the heavy data through the expensive 5G networks. The challenge here is how do we develop data-centric IoT Services in which AI is a first-class design element?

Indeed, to take advantage of interoperable IoT platforms over 5G networks, IoT applications should be driven by AI deployed as autonomous microservices, essentially implementing the DIKW (Data, Information, Knowledge and Wisdom) at the edge of IoT [7]. Additionally, as interoperable IoT based platforms are being deployed through various use cases such as Smart City applications, Smart Manufacturing, etc., transporting huge volume of data from the IoT edge to the geo-distributed centralized Cloud data centers for processing is not only efficient in terms of communication bandwidth and energy consumption but also cannot support ultra-low latency applications [8].

With these ultra-low-delay sensitive applications, the current solutions are obviously not practicable. For example, a security surveillance application requires real-time processing of huge live video data, which is transmitted to the Cloud data centers for processing before intelligent decisions can be made [9]. This approach will not only be impossible to meet the latency requirements as such application may have to identify object in real-time but also such delay could lead to disastrous consequences. Thus, it is necessary to devise alternative solutions to the current store-and-process later systems such that processing and intelligent decision-making based on such data can be done close to the data sources in real-time.

Additionally, various solutions and concepts have recently been proposed to address this problem, from federated clouds, to Edge computing [8]. The federated clouds are a collection of heterogeneous infrastructures that may span the entire globe and requires that data from the IoT devices be transmitted to the cloud data centers. Thus, this architecture still depends on the Internet and public telecommunication infrastructure with very high latency and bandwidths requirements. Fog, on the other hand, aims to provide a system level horizontal architecture that distributes computing, storage, control and networking functions closer to the users in the Thing-Cloud continuum [10]. ROOF computing is closely related to Fog computing in that it provides highly distributed pervasive and virtualized platform data/processing to a central cloud data center. However, ROOF computing has been proposed to provide highly functional, secure and scalable IoT. It promises interoperable connectivity for variety of Things under the ROOF, context information and decisions for taking actions in real-time, information management and efficient connectivity to the Cloud and Service as well as efficient network design [4], [11]. This reduces communication delays and the size of data that needs to be migrated across the 5G to the cloud data centers.

3. AI AS MICROSERVICES (AIMS) AT THE EDGE OF THINGS

To deploy data-driven intelligent capability at the 5G networks, AI in various forms of machine learning algorithms, such as the deep learning, must be infused into the Edge-Cloud platform components. Thus, the 5G capabilities should be equipped with tools that allow intelligent services to be composed as data-driven microservices [12], [13]. The rationale is to address the weaknesses of the current monolithic Cloud based AI services, which cannot meet the requirements of real-time and ultra-low delay sensitive 5G applications. Rather than shipping the data to the cloud data centers where AI algorithms are applied to incorporate intelligent decision-making capabilities into 5G applications, these AI algorithms can be implemented and deployed closer to the sources of the IoT data and users by factoring the AI functionality into smaller functions that can be implemented as distributed microservices [14]. We proposes a hierarchically integrated infrastructure spanning the ROOF, Fog and Cloud computing platforms (Figure 1), to exploit resources at the Edge of Things (ROOF and Fog Computing resources) and Cloud data centers, as well as microservice concepts to incorporate AI capabilities into IoT applications. The microservice concept allows the decomposition or factoring of the current monolithic AI services (which are deployed only on the centralized Cloud data centers) into smaller functions deployed as AI microservices. The microservices can then be deployed closer to the data sources and users allowing seamless composition of AI services across the ROOF-Fog-Cloud layer. The AI features and functions are composed from the distributed microservices AIMS integrated platform, allowing AI functionality as intelligence services to be implemented and deployed close to the data sources and users despite the limited resources available at these layers and the huge computing resources required by AI algorithms.

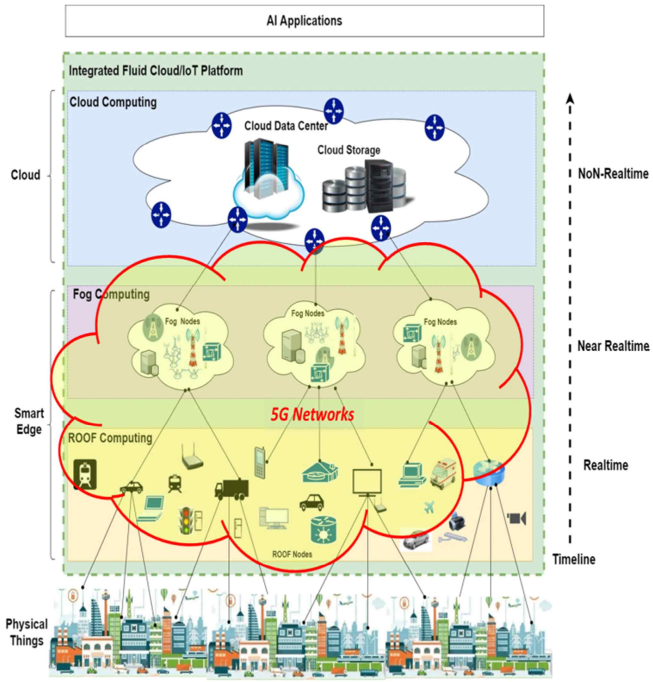


Figure 1 – Edge-Cloud high-level integrated architecture over 5G networks for various AI enabled IoT applications

In software engineering, the concept of service-oriented architecture is not new. This is based on the idea that an application can be designed such that the functionality it provides is divided into smaller functions and implemented as services that can interact via well-defined programming interfaces and thus allowing scalability, robustness and interoperability. Network slicing is recognized as a game changer in the remarkable paradigm shift from 4G to 5G era because it can maximize the sharing of network resources and flexibility for dedicated logical networks [15]. AIMS based application involves composing interoperable microservices from the ecosystem of microservices distributed across the ROOF-Fog-Cloud systems as illustrated in Figure 2, showing how microservice at each 5G network slice can be composed. At ROOF level, for example, an AIMS service could execute a decision process based on the data obtained from the IoT devices after some other microservices at this layer have executed data gathering, and pre-processing tasks on the collected data. In fact, the pre-processed data can be temporarily stored on some of the nodes at this layer. One advantage of service composition at this layer is that some more important decision process with low latency can be executed without offloading such process and data to the upper layer such as the Fog and Cloud layers. Note that these microservices are developed and deployed independently of each other and are composable at runtime. The composition of the microservices can be realized sequentially based on Network Function Virtualization (NFV) [2] management and inter-slice resource brokering process. The dynamic adopting microservice architecture for the deployment of AI services means that we can now engineer data-driven IoT based applications that are composed of multiple hierarchical self-contained, lightweight, portable runtime and modular components deployed across a federation of network slices. This means that AI algorithms can be factored into modular functional entities that can be implemented as data-driven reusable algorithmic primitives. For example, the core functionality of a particular AIMS service could be a service providing regression analysis, classification, clustering, IoT data pre-processing functions such as feature extraction, feature reduction, dealing with missing data values etc. Each microservice is responsible for the execution of a smaller portion of an AI task with its own data, processing and notification points accessible to other microservices.

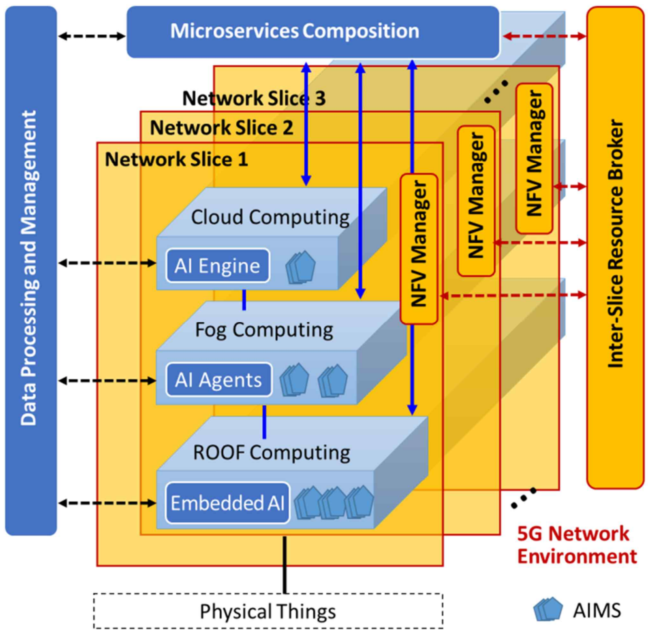


Figure 2 – The ecosystem of microservices distributed across the ROOF-Fog-Cloud systems over 5G networks

In Figure 2, the first layer is the physical layer consisting of the IoT devices and connectivity protocols. The IoT devices can be categorized into 3 types. The first type consists of the edge sensors and actuators. These devices are capable of capturing data with little or no processing capability of operating system. They are equipped with low power 5G radio connectivity with which they can communicate with the edge devices. The second type of IoT devices at the edge are the edge devices. These are devices with the capability to run operating systems such as Android, IOS, Windows, Linux, etc. They possess the capability to not only aggregate data but also to execute pre-processing on the collected data. Some of these devices can also run some embedded AI algorithms as microservices to provide simple intelligent decision and insights on the data they have aggregated.

The ROOF layer consists of devices and nodes such as 5G gNodeBs, home routers, smartphones that provide the resources for always-available services, security, privacy in real-time as the next hop for the Things. It can be implemented on these devices that serve as Things' proxies for connectivity to the network and Cloud. In our proposed architecture, ROOF serves as a proxy for the physical Things for connectivity to the Fog and to the Cloud Computing data centers. At the layer of the architecture, AI agents and other related distributed applications can be deployed as microservices.

The third layer is the Fog layer, which is a virtualized layer providing compute, storage and networking services between the ROOF and the traditional Cloud data centers. This layer can deliver more powerful 5G application services that can be supported by the ROOF layer. This layer consists of Fog nodes, which are facilities and infrastructure that can provide resources for distributed 5G application services. In our architecture, base stations and other core network gateways serve as Fog nodes.

The fourth layer is the Cloud layer, which is located in the core network and support interoperability and wide-usage as AIMS modules independent to the data. In addition, it provides long-term decision making in the smart city services.

4. AIMS: USE CASES

4.1 Smart City Surveillance Application

One of the key areas where the architecture proposed in this article is most useful is in security surveillance in a Smart City platform. In a Smart City, there are numerous smart cameras installed in various parts of the city for different purposes ranging from traffic monitoring, security surveillance at train stations, bus stations, airports, shopping malls, streets, etc. Imagine that there is intelligence about an intending terror attacks and the pictures of possible suspects have been shared among various security monitoring systems in the city. The security monitoring system is linked with the smart cameras. To report the sighting of a suspect, the smart cameras should be empowered to carry our real-time analysis of live streams of video data and decide if an individual with a suspicious bag is one of the wanted terror suspects. To realize that, different analytical AI algorithms, such as anomaly detection using deep learning, can be deployed as microservices to support the surveillance cameras installed in the 5G based virtualized service infrastructure.

AI algorithm analyzes the video data for autonomous local decision-making. The smart camera can then communicate its decision to the appropriate authority for action while the cameras keep on monitoring the suspect and if need be passing control information to nearby cameras should the suspect move away from the current camera. Thus, the system can locally process the streams of live video data among themselves and thus to reducing traffic overhead, latency in 5G networks.

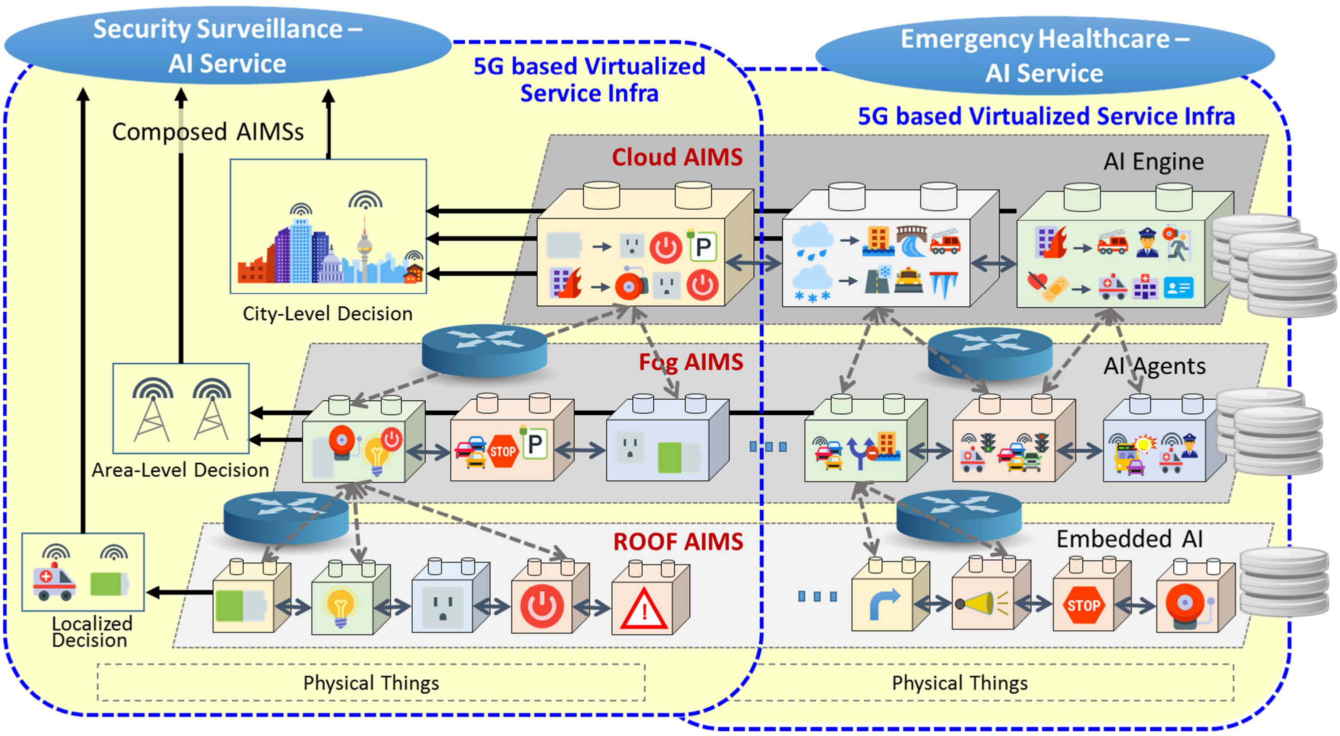


Figure 3 – 5G based Virtualized Service Infrastructure

4.2 Emergency Healthcare System

AI Microservices in the Fog-Clouds could be used to provide smart healthcare services where real-time vital sign and other data must be processed, and an instant decision has to be communicated to healthcare providers such as emergency health services. A microservice, might be responsible for collecting the data, another for processing the data and other for predicting, and another for deciding on action to take based on the prediction. The AI algorithms that these microservices implement are deployed on cross-border Fog-Cloud systems. This kind of system would provide low-latency, privacy, trust and secured mobility and location-aware supports to the individuals in the 5G environment.

To facilitate AI-powered 5G applications such as the security surveillance and emergency healthcare as shown in Figure 3, AIMS infrastructure hierarchically incorporates Cloud and Edge computing with AI and 5G technologies. AIMS provides multi-level AI components located from the Smart Edges (ROOF/Fog) of things to the Cloud centers. Thus, the AIMS enables various levels of intelligence, which are deployed at ROOF/Fog/Cloud layers, to be developed as independently deployable microservices (AIMS components). These AIMS components can then be incorporated based on message driven communications provided by the platform, allowing easier extensibility, interoperability, evolution, integration and composition of high-level, complex AI-powered 5G services.

5. CHALLENGES

The 5G integrated AIMS platform is envisioned to address important challenges of an advanced and efficient federated cloud platform with IoT for AI applications. It will be designed to offer distributed AI services (as a microservice) over 5G networks, leveraging multi-cloud computing, IoT and Big Data technologies.

5.1 Defining an integrated platform architecture for Cloud, AI and 5G

One of the key challenges is how to define an integrated reference architecture for multi-cloud IoT based microservices, enabling intelligent data acquisition and analysis through integrated protocols and standards with uniform access while supporting different interactions between various IoT services deployed on federated cloud systems at the 5G networks. Presently, there are frameworks providing solutions in this direction. A good example is the EdgeXFoundry open source platform developed for the edge of the network [16]. It interacts with the physical everyday working world of devices, sensors, actuators and other IoT objects. It has been designed as a framework for industrial IoT edge computing, enabling rapidly growing community of IoT solution providers to work together in an interoperable ecosystem of components to reduce uncertainty, accelerate time to market and facilitate scale. This platform brings the much-needed interoperability that makes it easier to monitor the physical world, send instructions to them and collect data, move the data across the Fog up to the Cloud where it can be stored, aggregated, analyzed and turned into information that can be acted upon. One important aspect of this platform that relates to AIMS is its capability that allows data to travel northwards and laterally to other edge gateways, or back to devices, sensors and actuators. However, the edge gateways only function as data collectors or aggregators for the IoT devices from which such data is transmitted to the cloud data centers. The EdgeXFoundry platform does not provide integration with other cross-border Cloud-IoT platforms and also does not incorporate intelligence at the edge of the network to allow application of AI algorithms for data processing and analyzing IoT data for intelligent decision making. Another is the MUSA project sponsored by the European Union [17]. MUSA is a distributed multi-cloud application platform over heterogeneous cloud resources. Its components are deployed in different cloud service providers and work in an integrated way and transparently for the end users. BigClouT [18] is another similar ongoing project sponsored by the European Union that leverages the power of Cloud computing, IoT and Big data analytics to provide distributed intelligence in a smart city network. The AIMS aims to define and develop an integrated platform architecture for the incorporation of multi-clouds systems and IoT for AI based services.

5.2 Specifying essential components and interfaces to support data-driven AI services

The AIMS infrastructure consists of broad variety of heterogeneous nodes, devices, protocols, etc. That interacts in diverse operating conditions from ROOF to the Cloud. This heterogeneity raises important question of how microservices deployed across this ecosystem of the federated AIMS platform would be able to communicate to exchange information and data that are in different formats. The popular solution would be to design a unified middleware framework, providing the abstractions of various layers on top of AIMS to hide this complexity from the microservices and allow them to fluidly exchange not only heterogeneous data and information but also intelligence seamlessly. Thus, various components and interfaces for communication across a federation of ROOF, Fog and Cloud platform would be specified. This middleware and its associated interfaces should be designed to guarantee interoperability between the federated ROOF, Fog and Cloud elements, coordinating the life cycle of the whole tasks of various microservices taking part in delivering intelligence as a service. Components for communication, configuration, microservice and resources discoveries, composition via orchestration or choreography and other related service interfaces would be specified and designed.

5.3 Supporting the harmonious management of computing resources

In the proposed AIMS integrated platform, large heterogeneous and distributed IoT devices will produce huge volume of data at rapid velocity. Gleaning meaningful information and insights from this data using distributed AI services will require a shift from the traditional architectural style to a more agile approach that allows more robust scalability, evolvability and maintainability of large-scale distributed multi-cloud IoT systems. Microservice architecture, as one of the recent trends in the design and development of agile distributed systems, defines a new approach to designing and developing a single application as a suite of smaller services, each running in its own process and communicating with lightweight mechanism to execute just one task. Such services are small, highly decoupled, independently deployable, focusing on doing a small specific and interdependent task that can provide some level of intelligence and yet when combined with other tasks provide higher or deeper intelligence depending on available and required resources. In order to achieve a much bigger task, these services can be combined to realize such functionality. One of the key challenges therefore that need to be addressed is that of dynamic allocation and orchestration of resources for the distributed microservices in the AIMS federated platform depending on what compute resources are currently available and how much of resources are required by the current microservices for the task execution. Although, there has been existing resource allocation in 5G networks, however, there is no yet concrete solution for resource allocation for integrated ROOF, Fog and Cloud platform. Even for the more mature Fog, resource and service orchestration remains a challenging research problem. For the AIMS platform, there would be several microservices sharing resources and this might result in resource contention and interference. Thus, new mechanisms and strategies for dynamic and fluid resource allocation and scheduling would be investigated to reduce response time for task execution across the 5G integrated AIMS platform.

5.4 Applying new mechanisms using intelligence in data lifecycle

To provide distributed intelligence at the edge of things, a critical factor for deploying AI services on the ROOF-Fog-Cloud integrated infrastructure is more related to application partitioning or factoring, real-time service composition, data mobility and aggregation. To address these issues, there is need for new mechanisms for factoring or decomposing AI services into functions that can be delivered as re-usable microservices for executing specific smaller tasks. These new mechanisms for service composition must be developed to achieve a fluid decision making process exploiting raw data from the physical devices, extracting meaning and insights in order to achieve the DIKW at the ROOF, Fog and Cloud layers of the infrastructure's hierarchy. Such mechanisms should support the dynamic discovery, composition and relocation of AIMS according to the required and available resources across the integrated nodes on the AIMS platform. How to determine based on the available resources, what level of intelligence should be provided by a microservice, what tasks or functions should be executed and at what layer of the infrastructure are important technical challenges.

5.5 Supporting trusted AI services

The AIMS based applications will process large volume of data using distributed microservices from ROOF to Cloud continuum of the platform. Thus, as distributed and interoperating microservices execute intelligence based on data from the physical devices, such data can be compromised as they may be exposed to malicious third parties. In fact, malicious microservices can be injected into the system to wreak havoc or to provide false or misleading decisions. This is a crosscutting challenge since it does not only affect a layer but all layers and aspects of the AIMS ecosystem, from radio communications to the microservices across the 5G networks. Additionally, the interfaces between Cloud, Fog and ROOF computing are potential sources of vulnerability and consequently may lead to corruption of IoT data and services. To ensure trust, privacy and security, capabilities for end-to-end encryptions, intrusion detection and prevention of unauthorized microservices or services will be required. Trust management should be investigated as a useful technology for providing such required security services. How can trust management be used to provide security, dependability and reliability for AIMS and associated data at various layers of the ROOF, Fog and Cloud integrated platform? For users' needs and rights to be enforced as autonomous microservices exploit IoT data to infuse intelligence into IoT applications, there is need to investigate integrated and federated ROOF, Fog and Cloud platform to propose the best and unique trust and security mechanisms for enforcing integrity, dependability and reliability of the platform and its services.

6. CONCLUSION

This article proposes an IoT data-driven intelligence-provisioning infrastructure with the 5G capabilities to provide intelligent connectivity as services closer to the Things by leveraging the compute resources of a hierarchically integrated computing environment (ROOF-Fog-Cloud). The proposed AIMS aims to provide a lightweight platform for effective deployment of scalable, robust, and intelligent cross-border 5G applications. We have envisioned the proposed architectural approaches in terms of system perspectives to allow AI functionality to be infused into 5G networks as distributed, composable microservices consisting of independent virtual components that can be deployed on the federated Roof-Fog-Cloud continuum to improve scalability, interoperability and cutting down latency for real-time 5G applications. In this article, we have also highlighted some challenges to give future research directions.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2018R1A2B2003774).

REFERENCES

[1] A. Krylovskiy, M. Jahn and E. Patti, "Designing a Smart City Internet of Things Platform with Microservice Architecture," 2015 3rd International Conference on Future Internet of Things and Cloud, pp. 25-30, Aug. 2015.

[2] "Microservices," https://en.wikipedia.org/wiki/ Microservices.

[3] P1931.1, "Standard for an Architectural Framework for Real-time Onsite Operations Facilitation (ROOF) for the Internet of Things," https://standards.ieee. org/project/1931_1.html.

[4] N. Mohan and J. Kangasharju, "Edge-Fog cloud: A distributed cloud for Internet of Things computations," 2016 Cloudification of the Internet of Things (CIoT), pp.1-6. 2016.

[5] Marco Gramaglia, Albert Banchs, "Definition and specification of connectivity and QoE/QoS management mechanisms," 5G NORMA Deliverable D5.2, Jul. 2017.

[6] P. Patel, M. Intizar Ali and A. Sheth, "On Using the Intelligent Edge for IoT Analytics," in IEEE Intelligent Systems, vol. 32, no. 5, pp. 64-69, Sep. 2017.

[7] M. Fazio, A. Celesti, R. Ranjan, C. Liu, L. Chen and M. Villari, "Open Issues in Scheduling Microservices in the Cloud," in IEEE Cloud Computing, vol. 3, no. 5, pp. 81-88, Sep. 2016.

[8] H. Liu, F. Eldarrat, H. Alqahtani, A. Reznik, X. de Foy and Y. Zhang, "Mobile Edge Cloud System: Architectures, Challenges, and Approaches," IEEE Systems Journal, vol. 12, no. 99, pp. 1-14, Feb. 2017.

[9] A. Celesti, M. Fazio, M. Giacobbe, A. Puliafito and M. Villari, "Characterizing Cloud Federation in IoT," 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 93-98, Mar. 2016.

[10] C. Long, Y. Cao, T. Jiang and Q. Zhang, "Edge Computing Framework for Cooperative Video Processing in Multimedia IoT Systems," in IEEE Transactions on Multimedia, vol. 20, no. 99, pp. 1126-1139, May 2018.

[11] Y. Ai, M. Peng, and K. Zhang, "Edge cloud computing technologies for internet of things: A primer," Digital Communications Networks, vol. 4, iss. 2, pp. 77-86, Apr. 2017.

[12] A. Taherkordi and F. Eliassen, "Poster Abstract: Data-centric IoT Services Provisioning in Fog-Cloud Computing Systems," 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 317-318. 2017.

[13] James Kobiolus, "Building AI Microservices for Cloud-Native Deployment," https://wikibon.com /building-ai-microservices-for-cloud-native-deployments/.

[14] M. Villari, M. Fazio, S. Dustdar, O. Rana, and R. Ranjan. "Osmotic Computing: A New Paradigm for Edge/Cloud Integration," IEEE Cloud Computing, pp. 76–83, 2016.

[15] Qi Wang, et. al., "SliceNet: End-to-End Cognitive Network Slicing and Slice Management Framework in Virtualised Multi-Domain, Multi-Tenant 5G Networks," 2018 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), pp. 1-5, 2018.

[16] "Edge X Foundry," https://wiki.edgexfoundry.org/ display/FA/EdgeX+Foundry+Project+Wiki.

[17] A. Sill, "The Design and Architecture of Microservices," IEEE Cloud Computing, vol. 3, no. 5, pp. 76-80, Sept. 2016.

[18] "BigClouT: Big data meeting Cloud and IoT for empowering the citizen clout in smart cities," http://bigclout.eu/.

MULTIFRACTAL MODELING OF THE RADIO ELECTRIC SPECTRUM APPLIED IN COGNITIVE RADIO NETWORKS

Luis Tuberquia-David[1]; Cesar Hernandez[1]

[1]Universidad Distrital Francisco Jose de Caldas, Colombia

ABSTRACT

The work discussed in this article is framed within the context of cognitive networks in America, showcasing the scenario of the radioelectric spectrum of the city of Bogotá, Colombia. The objective is to model the traffic of the wireless network, since it is underused in this region of Latin America. Hence, some tools are studied to allow the structuring of the type of traffic seen in the network. Based on stochastic tools such as the log-scale diagram, the linear multiscale diagram, and the multifractal spectrum, this research aims to verify the multifractality of traffic series collected on the electric radio spectrum of Bogotá, Colombia in 2012. In fact, the study reveals that all the channels of the network have a multifractal behavior with 90% of them presenting a Hurst parameter in the 0.5 to 1 range. The evidence suggests that the traffic in this region could be modeled as multifractal time series. Therefore, the analysis carried out intends to provide a new modeling method for the Colombian radioelectric spectrum in the form of a multifractal-based analysis.

Keywords – Multifractal, cognitive radio, radio electric spectrum, Bogotá, Hurst Parameter

1. INTRODUCTION

Historically, spectrum allocation in Colombia is regulated by the Ministry of Information and Communications Technologies (by its acronym in Spanish, TIC), with the help of the National Agency of the Spectrum (by its acronym in Spanish, ANE). This branch is in charge of granting users the best quality in service, although studies such as [1], [2] have revealed that the radio spectrum in Colombia is underused. Many research projects have been carried out around the globe, stating that the radioelectric spectrum is underused in terms of frequency, time and geographic domains [3],[4]. The results of the investigations show that this is a global phenomenon that not only occurs in Colombia. As a solution to the problem of underuse, several solutions have been proposed from where cognitive radio (CR) networks [5] stand out. CR presents a dynamic spectrum management technique, known as Dynamic Spectrum Access (DSA) [6] which is designed to prevent interference, adapt to the immediate availability of the local spectrum and create times and locations for Secondary Users (SU) to share with Primary Users (PU) [7].

Communication networks have been a subject of study for over two decades, showing that the times between the arrival of user demands and the demand placed on the network have a correlation that persists across different time scales [8]. Since the 1980's, studies have been developed on data traffic, in order to predict, control and improve the overall service. Furthermore, the research carried out at Bellcore [9] on Ethernet traffic revealed that the nature of Ethernet traffic is multifractal [10]. Additionally, it has been pointed out that the time series of incoming packets related to user demand behave with stochastic self-similarity which is the main characteristic of multifractal signals [11], [12]. Moreover, multifractal traffic has been validated in different network structures as evidenced in [13], [14].

The use and demand of wireless data have increased recently, which is expected to continue due to the nonstop development of wireless applications. This means that the monthly use of mobile data will be multiplied by eight before 2020 in comparison to 2015 [15]. The research detailed in this article is based on the three mentioned premises: the underuse of the radioelectric spectrum in Colombia, the multifractal nature of network traffic and the growing trend of wireless systems. Therefore, the main goal of the authors is to confirm the nature of the traffic data captured in the city of Bogotá within the requested Wi-Fi band. Furthermore, probabilistic tools are used such as the Log-scale Diagram (LD) to calculate the Hurst parameter, The Multiscale-linear Diagram (MD) to estimate said parameter in two different statistical moments, and the Multifractal Spectrum (MS) analysis to determine the width of the spectrum. Hence, the research wishes to prove that the network traffic in Bogotá has a multifractal behavior.

To reach the proposed objective, spectral occupancy data corresponding to the Wi-Fi band was used since it is freely available and has a more chaotic behavior which makes it harder to model compared to the GSM band.

In Section 2, the article starts by explaining the data collection process and how the time series was built. In Section 3, the steps required to compute the MS are detailed. Section 4 presents the results of the statistical analysis of the data gathered from the radioelectric spectrum of Bogotá. The conclusions of this investigation are stated in Section 5.

2. FROM MEASUREMENTS TO TIME SERIES

2.1 Collecting data

In March 2012, a collection of data from the radioelectric spectrum was conducted in the city of Bogotá, Colombia. A spectrum analyzer was used to detect the traffic based on the power of the signals. Consequently, the gathered information indicates whether the signals are present or absent during the defined sampling time. The captured data is located within the GSM, Wi-Fi and 1850 MHz to 2000 MHz bands [16].

The equipment used to capture the measurements of the spectrum were a Discone antenna set in the 25 MHz – 6 GHz frequency range, a low noise amplifier (LNA) running in the 20 MHz - 8 GHz frequency range and a spectrum analyzer operating in the 9 kHz – 7.1 GHz range [17]. The map of the spectrum measurement campaign in the city of Bogotá is shown in Figure 1, indicating the data collection spots in yellow.

Figure 1 – Map of the measurement campaign in Bogotá. Adapted from [16]

Measurements were carried out in six buildings scattered across the city and located in strategic points. Their coordinates (latitude and longitude) are listed in Table 1.

Table 1 – Geographic location of the measurement spots

Location	Latitude	Longitude
1	4°73’0” north	74°0’5’’ west
2	4°68’2” north	74°0’5’’ west
3	4°65’5” north	74°1’0’’ west
4	4°62’8” north	74°0’6’’ west
5	4°58’8” north	74°1’0’’ west
6	4°57’9” north	74°1’5’’ west

The main technical parameters for the captured data in the spectrum were the bandwidth resolution which was set at 100 kHz, the span set at 50 MHz and the scanning time at 333 milliseconds [16].

2.2 Spectrum Availability Matrix

The Wi-Fi data includes the information of 461 frequency channels, with a time resolution equal to one third of a second. In total, the Wi-Fi database has 4.978.800 data and a Wi-Fi assessment of 829,800 [17].

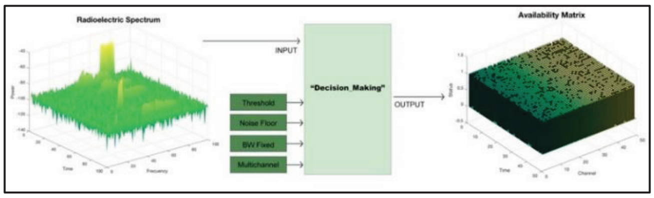


Figure 2 – Building the availability matrix from the power matrix

Figure 2 shows the block diagram that represents the construction process of the availability matrix. The availability matrix indicates when a channel is being occupied by a primary user (with a value of 1) or available for use (with a value of 0). The power values of the 461 channels are assessed for one element at a time by comparing them with a threshold value. The tool proposed in [17] transforms the data between -40 dBm and -147 dBm into binary values according to the restriction set by a specific threshold.

2.3 Time series of Wi-Fi traffic in Bogotá

Based on the Wi-Fi Availability Matrix, it is proposed to create a time series that collects the download packages of users in time units, as well as the availability of consecutive time instants within the channel. The idea is to form a time series with the ongoing tendency of a channel and measure the fluctuations between occupied and idle states.

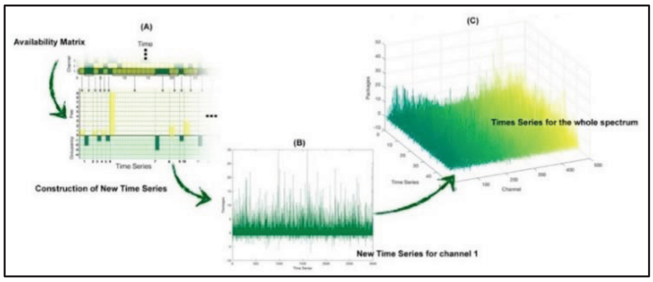


Figure 3 – Fluctuations between *busy* and *idle* states of channels in Bogotá’s radioelectric spectrum in Wi-Fi band

In order to generate the time series, the first step involves assigning a positive weight in the instant in which the channel is free and a negative weight when the channel is busy. Then, positive and negative time units are counted in sequence to create a new time series. They are stored in an intercalary free packet, followed by the packages currently occupied by users. Figure 3a displays the construction process of the time series, described above. Hence, the new time series includes positive values representing available time units and negative values representing occupied time units. Figure 3b illustrates the complete construction of the time series for Channel 1 with a length of more than 3500 packages. Finally, the same process is repeated for all channels, leading to the chart in Figure 3c which shows the behavior of the entire radioelectric spectrum.

3. MULTIFRACTAL SPECTRUM CALCULATION

3.1 Log-scale diagram and Hurst parameter calculation

The newly obtained time series is analyzed with the help of probabilistic tools. Firstly, the Log-scale Diagram (LD) is used to analyze the time series at different scales. Therefore, the series is split into logarithmic scales and a detail coefficient is estimated for each scale. A correlation between the detail coefficients ensures that the temporal estimators have minimum variance. Additionally, it is estimated that the variance of the detail coefficients $dx(j,\cdot)$ is given by Equation (1) [18], [19].

$$\mu_j = \frac{1}{n_j}\sum_{k=1}^{n_j} |d_X(j,k)|^2 \qquad (1)$$

where n_j is the number of detail coefficients in the octave j, and μ_j is the estimator of $E[|d_x(j,\cdot)|^2]$. Once the detail coefficients have been determined, it is noteworthy to mention that the second statistical moment follows the power law with an exponent of $2H-1$ where H is the Hurst parameter representing the self-similarity of the second stochastic moment. Thus, the estimation of the Hurst parameter can be described by Equation (2).

$$\log_2 \mu_j = (2H-1)j + \log_2 C \qquad (2)$$

The LD is the result of plotting the $\log_2 \mu_j$ as a function of octave j. Figure 4 shows the calculation of H for the time series corresponding to Channel 1 as illustrated in Figure 3. Furthermore, it performs a linear regression on the estimators computed for each scale. Then, the slope of said regression is calculated. A gradual estimate of H is obtained with confidence intervals determined by the standard deviation of H.

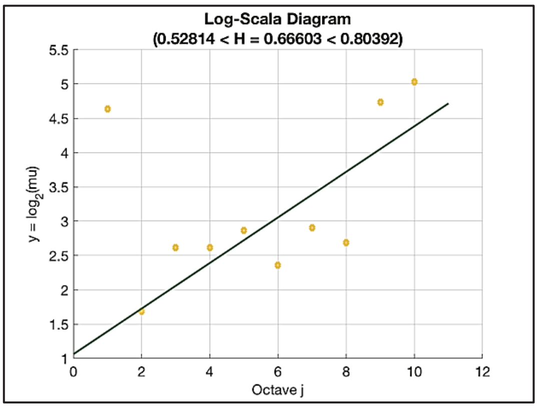


Figure 4 – Hurst parameter estimation with LD

3.2 Extension of the variance estimator and statistical moments

By extending the estimator in Eq. (1) for statistical moments to $q \neq 2$ and considering positive and negative values of q in a set of real numbers, the analysis of the stochastic tool discussed in the preview section can be broadened. By denoting q as the order of the estimator, Equation (3) can be derived as:

$$\mu_j{}^q = \frac{1}{n_j}\sum_{k=1}^{n_j} |d_X(j,k)|^q \qquad (3)$$

In a self-similar processes with $0.5 < H < 1$, the estimator follows the power law and can be extended to Equation (4) according to [20]

$$E[|d_X(j,k)|^q] = C_q 2^{j(\zeta(q)-q/2)} \qquad (4)$$

where C_q is a function of q and $\zeta(q)$ is a function that allows the differentiation between monofractal and multifractal processes. Therefore, the scaling exponent of order q is estimated by [20] in the same method described with Eq. (2). To create a representation of the behavior of such exponents according to an order q, the Multi-scale linear Diagram (MD) is used where H is projected according to the order q for negative and positive values of it.

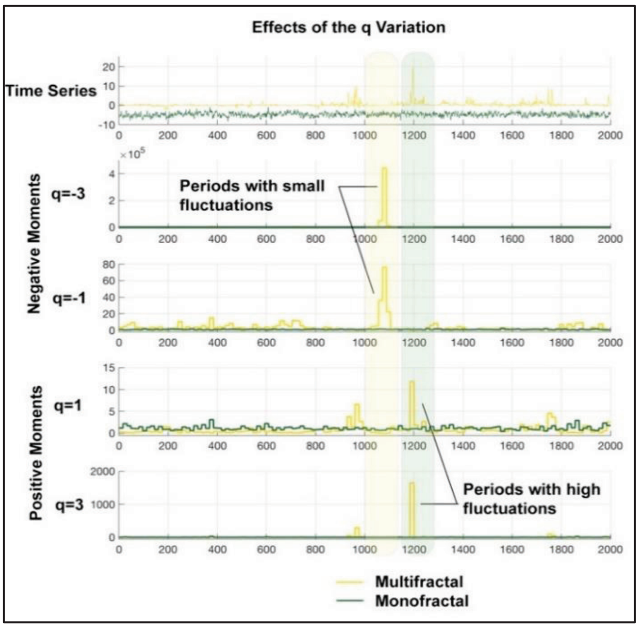


Figure 5 – Dissection of fluctuation traces for small changes in negative moments and significant changes in positive moments. Adapted from [21]

Figure 5 illustrates how the analysis is affected by the changes in q as it goes from negative to positive values. On the one hand, the analysis of negative values of q pertains to the study of small fluctuations in multifractal traces. As q decreases, the analysis of small fluctuations is more noticeable in contrast with monofractal traces where fluctuations are scarce, and the trend is the same for all q. On the other hand, for positive values of q, the analysis requires studying large fluctuations related to the average fluctuations of the traces. As the value of q increases, the analysis of larger variations is more noticeable, and the trend of monofractal traces remains the same as in negative values of q.

3.3 Legendre transformation and multifractal spectrum calculation

It is then proceeded to calculate the multifractal spectrum using the Legendre transformation. This method measures the singularity dimension of order q denoted as $D(q)$ and the resolution function is named $H(q)$ [22]. $D(q)$ is a linear transformation that converts scales into statistical moments since the mapping function of sampling scales into individual statistical moments is non-linear [23]. Hence, the Legendre transformation is computationally more efficient than other methods used to calculate the multifractal spectrum [8]. This version of the multifractal spectrum calculation was implemented hereby.

To calculate the singularity dimension, $\tau(q)$ serves as an intermediate variable in the form of Equation (5).

$$\tau(q) = qH(q) - 1 \qquad (5)$$

The calculation of the singularity dimension D of order q in Equation (6) [24] can be determined once $\tau(q)$ has been estimated.

$$D(q) \equiv \frac{\tau(q)}{q-1} = \frac{qH(q)-1}{q-1} \qquad (6)$$

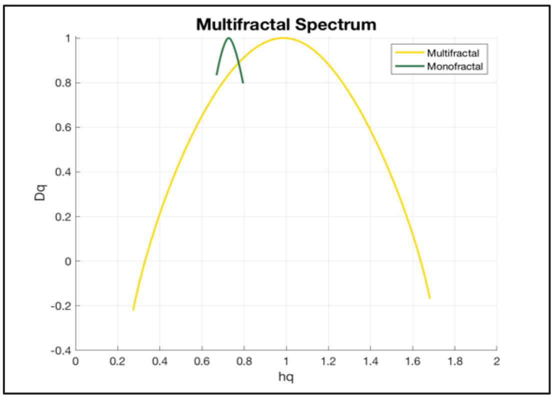


Figure 6 – Multifractal spectrum for a monofractal and multifractal time series

Plotting $D(q)$ as a function of $H(q)$ results in the Multifractal Spectrum shown in Figure 6 where the shape of the spectrum for monofractal and multifractal time series can be appreciated. As expected, the shape of the monofractal spectrum is not as broad as for the multifractal spectrum. Furthermore, the monofractal behavior is not as prolific during fluctuations of q, which is the opposite case for the multifractal scenario where the activity surrounding q is quite intense. The result of this transformation is a long arc where the difference between the maximum and the minimum values of $H(q)$ corresponds to the width of the multifractal spectrum [21]. The MS form can be approximated to a second order polynomial function and its width can be measured with the zero-crossing operation $D(q)=0$.

4. BEHAVIOR OF THE RADIOELECTRIC SPECTRUM IN BOGOTÁ

4.1 Calculation of the Hurst exponent for the radioelectric spectrum in Bogotá

The next step involves calculating the Hurst parameters for each channel based on the time series seen in Figure 3. Using the detail coefficients, the variance of the estimator is calculated, and the slope is derived from the estimation around the octaves for each channel Eq (1). Figure 7 corresponds to a plot of the variable H for all channels of the radioelectric spectrum. The channels with a value of $H > 0.5$ are denoted in light green, stating a persistent behavior in the trend and short-range dependence. The channels with $H > 1$ are denoted in dark green, indicating persistence against the trend-related behavior and long-range dependence. Out of the 461 channels, 25 channels showed a value of $H < 0.5$, two channels had a value of $H > 1$ and the remaining 434 channels were in the range $0.5 < H < 1$.

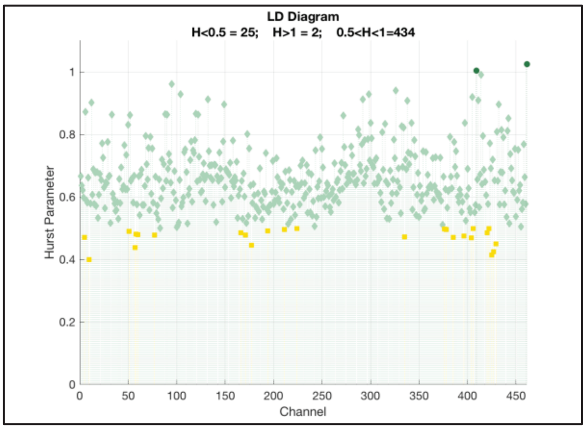


Figure 7 – Hurst parameter estimation for all channels

4.2 Sampling correction in the extensor of the variance estimator

Moving on, the Multi-scale linear Diagram (MD) is computed for all channels of the spectrum. When calculating the MD, the channels presented irregularities in the shape and distribution of $H(q)$. In Figure 8a, the green curve highlights the example of a channel with irregularities in the sampling process of the diagram. The appropriate selection of $H(q)$ is carried out by a hierarchical decision tree that chooses the maximum value of the function in the vicinity of q=0 [25] that can be compared based on a curve similar to a sigmoidal function. To correctly deermine the width of the multifractal spectrum, as shown in Figure 8b, the green curve represents the multifractal spectrum with a lousy sampling procedure, leading to an unmanageable calculation of the multifractal spectrum's width.

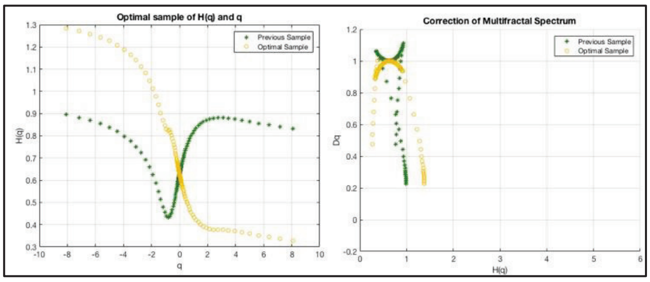


Figure 8 – Before and after optimal sampling
a. MD b. MS

By correcting the MD sampling, the yellow curve in Figure 8a is obtained. It decreases when q goes from the negative to the positive domain. Plus, the calculation of the MS width becomes more precise as shown in Figure 8b.

4.3 Multifractal spectrum calculation for the radioelectric spectrum of Bogotá

Once the MDs are corrected, all the spectral widths are computed in order to verify the multifractality of the time series generated from the traffic in Bogotá. Figure 9 shows the spectral amplitudes for the channels of the city's spectrum. The spectral widths reach an average of 1.2072, a standard deviation of 0.3647, a minimum value of 0.7285 and a maximum value of 4.7910.

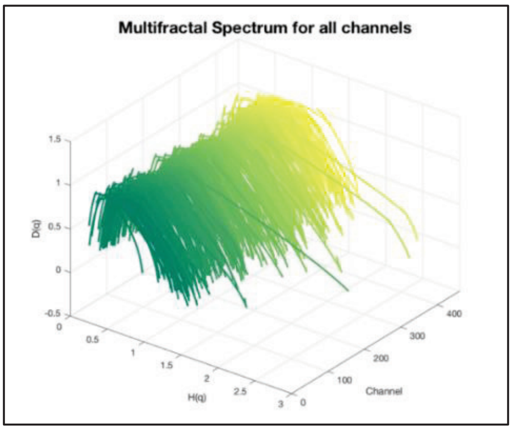


Figure 9 – Multifractal spectrum for the time series generated from the traffic in Bogotá

5. CONCLUSIONS

The results of this research evidence the multifractal behavior of data traffic in wireless networks such as Wi-Fi. This can be extended to other wireless applications such as mobile networks and television bands, where cognitive radio technology could prove to be useful.

Multifractal modelling of spectral occupancy data in mobile networks can become an excellent prediction tool of the primary user's behavior. Hence, spectral resources can be used more efficiently and improve the design of CR networks. Although Wi-Fi is freely accessed, it can be considered as an alternative for spectral resource allocation.

ACKNOWLEDGMENTS

The authors wish to thank Center for Research and Scientific Development of Universidad Distrital Francisco José de Caldas for the supporting and funding during the course of this research project.

REFERENCES

[1] L. F. Pedraza, C. Hernández, K. Galeano, E. Rodríguez-Colina, and I. P. Páez, *Ocupación espectral y modelo de radio cognitiva para Bogotá*, Primera. Bogotá: Editorial UD, 2016.

[2] L. Pedraza, C. Hernandez, and E. Rodriguez, "Modeling of GSM Spectrum Based on Seasonal ARIMA model," in *The 6th IEEE Latin-American Conference on Communications*, 2014.

[3] T. M. Roberson, R. B. Taher, K. J. Bacchus, and D. A. Zdunek, "Long-term spectral occupancy findings in Chicago," in *New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, 2011, pp. 100–107.

[4] K. Patil, K. Skouby, A. Chandra, and R. Prasad, "Spectrum occupancy statistics in the context of cognitive radio," in *2011 14th International Symposium on Wireless Personal Multimedia Communications (WPMC),* 2011, p. 1_5.

[5] S. Haykin, "Cognitive Radio : Brain-Empowered," *IEEE J. Sel. AREAS Commun.*, vol. 23, no. 2, pp. 201–220, 2005.

[6] S. E. Safavi and K. P. Subbalakshmi, "Effective bandwidth for delay tolerant secondary user traffic in multi-PU, multi-SU dynamic spectrum access networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 1, no. 2, June., pp. 175 – 184, 2015.

[7] X. Xing, T. Jing, W. Cheng, Y. Huo, and X. Cheng, "Spectrum prediction in cognitive radio networks," *IEEE Wirel. Commun.*, vol. 20, no. 2, April, pp. 90–96, 2013.

[8] R. H. Riedi and J. L. Vehel, "Multifractal Properties of TCP traffic: a numerical study," *IEEE/ACM Trans. Netw. 1997*, 1997.

[9] W. E. Leland and D. V. Wilson, "High time-resolution measurement and analysis of LAN traffic:Implications for LAN interconnection," *IEEE INFCOM '91. Conf. Comput. Commun. Tenth Annu.*

Jt. Comference IEEE Comput. Commun. Soc. Proc., pp. 1–7, 1991.

[10] M. Tuberquia-David, F. Vela-Vargas, H. López-Chávez, and C. Hernández, "A multifractal wavelet model for the generation of long-range dependency traffic traces with adjustable parameters," *Expert Syst. Appl.*, vol. 62, pp. 373–384, 2016.

[11] W. E. Leland, M. S. Taqqu, W. Willinger, and D. V. Wilson, "On the self-similar nature of Ethernet traffic (extended version)," *IEEE/ACM Trans. Netw.*, vol. 2, no. 1, pp. 1–15, 1994.

[12] S. Contreras, G. Ospina, and M. Alzate, "Cascadas Conservadoras Aplicadas a la Predicción de Tráfico Multifractal," *Rev. Ing.*, vol. 11, pp. 62–67, 2006.

[13] Y. Yu, M. Song, Y. Fu, and J. Song, "Traffic prediction in 3G mobile networks based on multifractal exploration," *Tsinghua Sci. Technol.*, vol. 18, no. 4, p. -, 2013.

[14] S. Wang and Z. Qiu, "A novel multifractal model of MPEG-4 video traffic," *IEEE Int. Symp. Commun. Inf. Technol. 2005. Isc. 2005.*, vol. 1, pp. 97–100, 2005.

[15] A. Al-Tahmeesschi, M. López-Benítez, J. Lehtomäki, and K. Umebayashi, "Investigating the Estimation of Primary Occupancy Patterns under Imperfect Spectrum Sensing," *2017 IEEE Wirel. Commun. Netw. Conf. Work. WCNCW 2017*, 2017.

[16] L. Pedraza, F. Forero, and I. Paez, "Metropolitan Spectrum Survey in Bogota Colombia," in *The IEEE International Conference on Advanced Information Networking and Applications Workshops*, 2013.

[17] C. Hernández and D. A. Giral, "Spectrum Mobility Analytical Tool for Cognitive Wireless Networks," *Int. J. Appl. Eng. Res. ISSN*, vol. 10, no. 21, pp. 42265–42274, 2015.

[18] O. I. Sheluhin, S. M. Smolskiy, and A. V Osin, "Principal Concepts of Fractal Theory and Self-Similar Processes," in *Self-similar Processes in Telecomunications*, Chichester, UK: John Wiley & Sons Ltd, 2007, pp. 1–47.

[19] P. Flandrin, P. Gonçalves, and P. Abry, *Scale Invariance and Wavelets Scaling*. London, UK, 2009.

[20] P. Abry, P. Flandrin, M. S. Taqqu, and D. Veitch, "Wavelets for the Analysis, Estimation, and Synthesis of Scaling Data," in *Self-similar Network Traffic and Performance Evaluation*, 2000, pp. 39–88.

[21] E. a F. Ihlen, "Introduction to multifractal detrended fluctuation analysis in Matlab," *Front. Physiol.*, vol. 3 JUN, no. June, pp. 1–18, 2012.

[22] P. Meakin, "Appendix B: Multifractals," in *Fractals, Scaling and Growth Far From Equilibrium*, Cambridge University Press, 1998, pp. 585–607.

[23] R. H. Riedi, M. S. Crouse, V. J. Ribeiro, and R. G. Baraniuk, "A multifractal wavelet model with application to network traffic," *IEEE Trans. Inf. Theory*, vol. 45, no. 3, pp. 992–1018, 1999.

[24] J. W. Kantelhardt, S. a. Zschiegner, E. Koscielny-Bunde, S. Havlin, A. Bunde, and H. E. Stanley, "Multifractal detrended fluctuation analysis of nonstationary time series," *Phys. A Stat. Mech. its Appl.*, vol. 316, no. 1–4, pp. 87–114, 2002.

[25] C. A. Schneider, W. S. Rasband, and K. . Eliceiri, "NIH Image to ImageJ: 25 years of image analysis," *Nat. Methods 9*, pp. 671–675, 2012.

TOWARDS COGNITIVE AUTONOMOUS NETWORKS IN 5G

Stephen S. Mwanje and Christian Mannweiler

Nokia Bell Labs, Germany

ABSTRACT

Cell densification and addition of new Radio Access Technologies have been the solutions of choice for improving area-spectral efficiency to serve the ever-growing traffic demand. Both solutions, however, increase the cost and complexity of network operations for which the agreed solution is increased automation. Cognitive Autonomous Networks (CAN) will therefore use Artificial Intelligence and Machine Learning (ML) to maximize the value of automation. This paper develops the models for cognitive automation and proposes a CAN design that addresses the requirements for 5G and future networks. We then illustrate the benefit of this approach by evaluating ML models that learn a network's response to different mobility states and configurations.

Keywords – Cognitive Autonomous Network, Network Management Automation, 5G

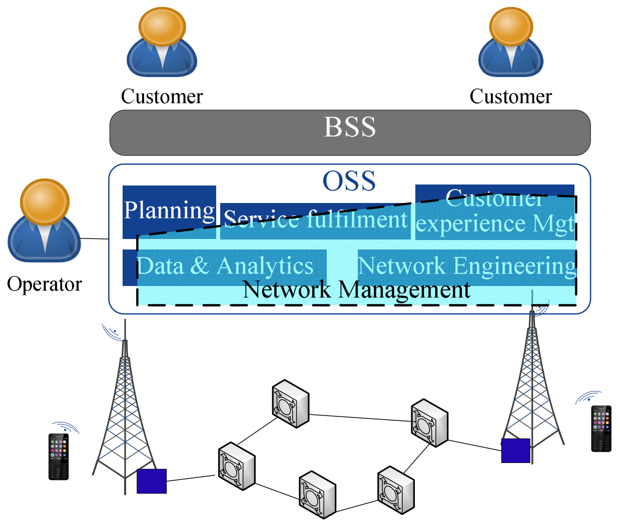


Figure 1: BSS and OSS deliver value from the network, but Network Management maximizes automation value.

1. INTRODUCTION

Demand for mobile communication services has grown unabatedly for at least two decades, recently driven by mobile Internet connectivity and the related broadband services, especially video. The solutions hereto have been twofold: (1) to deploy new Radio Access Technologies (RATs) intended to improve area-spectral efficiency (in bits/Hz/m^2) amidst ever higher spectrum demand; and (2) densification in each RAT, by deploying ever more cells to meet users' Quality of Service (QoS) needs at all locations and times. So mobile networks are characterized by heterogeneity and high Base Station densities, which directly translate into high Capital Expenditures (CapEx) and Operational Expenditures (OpEx) as well as high complexity of network design and operation. 5G, which at the least adds another radio layer, will further complicate these networks. Yet, although networks can be very complicated, the individual devices need to be rather simple and cost-efficient to be scalable to global-scale networks. Thus, the complexity is transferred to the network operability layers which must, at all times, retain the broader view across the network (see Figure 1).

The major solution to these challenges is automation, especially automation of network management. For a given network, Business Support Systems (BSS) and Operations Support Systems (OSS) ensure to deliver value from the network, both to the customer through BSS applications and to the Communication Services Provider (CSP) operating the network through the OSS. Network Management (NM) as a part of the OSS (see Figure 1) is responsible for the knowledge about, control of, and (re-)configuration of the network's devices to match operational objectives. It carries the biggest burden of network complexity as it defines which network devices, at what locations and for which customers should be used in which way and to which degree. Prioritizing the automation of NM processes will as such maximize the impact of the CSP's overall automation efforts. This includes processes in network configuration and operation optimization and healing as described in the Fault, Configuration, Accounting, Performance & Security Management (FCAPS) framework of the International Telecommunication Union's Telecommunication Standardization Sector recommendation M.3400 [1].

Today, a degree of automation has been achieved through Self-Organizing Networks (SON) [2]. SON is the first generation of NM automation, where SON Functions (SFs), realized as closed-loop control systems, address specific NM problems like balancing load among cells [2]. The SFs exhibit static, rule-based behavior that maps observed network states, e.g., changes in Key Performance Indicators (KPIs), to (re-)configurations of individual Network Configuration Parameters (NCPs) or entire network configurations. Since the multitude of SFs need to be coordinated, their management and coordination is performed in a hierarchical manner according to rather fixed rules, or through policies that are created based on fixed rules and input from Mobile Network Operator (MNO) and SON vendor.

SON is however limited since the control loops are inflexible to match the infinitely many contexts in networks. Thus, SFs are unable to adapt to major environmental or operational changes, from say technical upgrades, network architecture modifications, or new operator business and service models. Such changes will occur even more often in 5G networks, so a more flexible and adaptive NM system is required. Cognitive capabilities derived from Artificial Intelligence (AI) and Machine Learning (ML) promise better automation in networks, but the path thereto needs to be drawn out. This paper proposes such a framework and related models.

The rest of the paper is organized as follows: Section 2 reviews the notion of cognitive autonomy and describes a cognition model for the optimal design of Cognitive Autonomous Networks (CAN) and functions thereof as well as the extent to which AI and ML techniques achieve the desired functionality. Using the intuition from Section 2, Section 3 presents an AI/ML CAN implementation framework that is applicable to cellular network environments. Section 4 then presents the usage of such a framework towards learning the network's response to different mobility states and configurations before Section 5 makes some concluding remarks.

2. COGNITIVE AUTONOMOUS SYSTEMS

2.1. Automation, self-organization, and cognition

Automation has historically been equated with self-organization, typically as derived from biologically inspired autonomy. A common example of self-organizing systems in biology is the formation and management of colonies in social insects, e.g. haplometrosis in ant populations [3]. Many collective (social) activities performed by insects result in the formation of complex spatial-temporal patterns. Without centralized control, workers are able to work together and collectively tackle tasks far beyond the abilities of any one individual. The resulting patterns produced by a colony are not explicitly coded at the individual level, but rather emerge from non-linear interactions between individuals or between individuals and their environment [4]. A good example here is the foraging for food by ant colonies through which ants are able to establish efficient routes to and from the nest to the food sources [5].

New studies, however, show that the behavior of colony animals (especially ants) is more than random or deterministic self-organization, i.e. "each foraging process of an animal is also a learning process. With foraging repetition, long-term memory accumulates, an animal's knowledge about the environment of its nest gets richer, and the region that the animal is familiar with continues to enlarge" [6]. The observed emergent behavior is due to some internal cognitive process in which the ants process information to make decisions. Internally, within each insect, there are sub-processes that the insect uses to compute its decision that eventually leads to the observed outcome, i.e., "the animals use their intelligence and experience to guide them" [6].

2.2. Copying from human cognitive autonomy

According to various dictionaries, cognition relates to the collection of mental sub-processes that support the process of acquiring knowledge and understanding through sensory stimuli, experience, and thought. The human brain, which is the best example of a cognitive entity, continuously executes the cognitive processes to process all the information received from the environment and adequately analyze a situation to flexibly adapt to its reality, demands, and changes. The mental processes and subsequent skills can be grouped into [7]: basic, mutually independent processes that are independently fundamental to the functioning of the brain and higher or complex processes that are built up from combinations of basic and other complex processes.

The four basic processes are sensation, perception, attention, and memory. Sensation is the awareness of the various stimuli in our environment while perception enables us to process the received impulses and make out meaning from the stimuli. Attention enables us to voluntarily and/or involuntarily chose what we focus on amongst all the infinitely many concurrent stimuli from the environment. Finally, memory allows us to encode the data that we either receive from the environment or mentally create, so that we can consolidate and retrieve it at later points in time.

Higher processes presuppose the availability of knowledge which they put to use. Among these are thought, language, intelligence as well as combinations of these leading to problem solving and learning. Through thought, the brain creates concepts and processes them to derive new knowledge. Language enables us to produce and comprehend different sounds and words and to combine letters and phrases to express with precision whatever we want to communicate. Intelligence, in all its different forms as intrapersonal, linguistic, logical-mathematical, musical, and the recently popular emotional intelligence, takes complex combinations of basic and other higher processes to manifest. Core to all these higher processes is the concept of reasoning through which the brain combines different pieces of information and knowledge to create new knowledge.

2.3. Cognition: A perception-reasoning pipeline model

From our analysis of above biological processes, we postulate in the context of this work that cognition is a perception-reasoning engine which takes a piece of data, hereinafter called a Data Element (DE), and processes it to generate understanding and action(s). As shown in Figure 2**,** there are four quasi-orthogonal processes of this engine that lead to the realization of the two broad outcomes – perception and reasoning. Perception prescribes the ability to make sense of an incoming DE both on its own and in relation to data elements about its context. On the other hand, reasoning implies understanding the DE and its implications which then leads to the selection of the most appropriate actions for the data element and its context. We describe below the four processes and the related translation of the data elements into memory and actions.

2.3.1. Conceptualization

Given a DE captured through the sensory system, the first step in perceiving information related to the DE is conceptualization of the DE. Thereby, the entity with these cognitive skills (hereafter called the cognitive agent) makes a hypothesis about what the DE is or may be. Through such a conceptualization, the agent will for example decide if an animal it sees could be a fat cat, a small lioness or a lion cab. However, since such an initial conception of the DE may be inaccurate, the DE must be further processed for accuracy. The agent draws on its memory to crystalize the created concept. For example, it matches what it has seen with its in-memory pictures to confirm that what it sees is actually a cat and not a small lioness or its cab.

2.3.2. Contextualization

The conceptualization identifies the isolated information that the DE delivers, but to choose the right course of action, the DE must be put in the right context. The contextualization evaluates the situational, environmental, and other information related with the DE to concretize the knowledge on that DE. Besides being used for further processing, the context may also partly help to confirm the accuracy of the conceptualization or to at least increase the confidence level thereof. E.g., if the observed big cat or small lioness is found in the African wild, this context increases the possibility that it is a lioness. And where the conceptualization was accurate, contextualization guides the decision making to select the most appropriate actions for the DE and its context. In the lioness case, different decisions will be made if the lioness is encountered in the wild African Savannah or in a zoo.

2.3.3. Organization

Given accurate perception of DEs, the organization step defines relations among DEs - making connections with descriptive words like "is", "is not", "can", "cannot", "may", etc. In the cat vs. lioness case, this step creates statements like: "the African savannah has lions roaming around"; "A lioness is dangerous"; "A cat can be dangerous"; etc. These are partly previously inferred conclusions that have been stored in memory although the organization step can also create new connections among DEs. E.g., when one decides two items are related without necessarily knowing how they are related, such a realization is part of the DE organization step. It is logical to consider that the outcome of the organization step is information organized in such a way that each connection is an Information Element (IE).

2.3.4. Inference

The inference step logically and arithmetically combines multiple DEs and IEs to create new IEs and relations. It undertakes the logical analysis of DEs and their relations

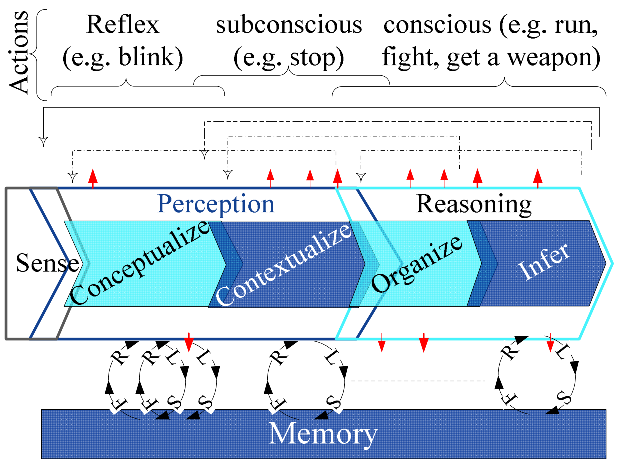


Figure 2: Cognition - a perception-reasoning pipeline

through the logical operations (*AND, OR, NOT*) as well as the linguistic information conjunctions (*BUT, WHILE, NOTWITHSTANDING*, etc.). In the lioness example, consider three IEs that could be evaluated alongside the "concept of a lioness" and the "African savannah context" – A: "I am watching TV" or B: "I am out hunting" or C: "I am seated inside a vehicle on a tour excursion". The inference step evaluates the truthfulness of the different combinations of the lioness DE and these IEs to derive the decision. Correspondingly, different decisions will be made if watching TV as opposed to when one is out hunting.

2.3.5. Memory operations and actioning

Each stage of the data processing cycle has access to the memory operations cycle. This cycle involves the four steps of Fetch(F), Read(R), Label(L) and Store(S). At the conceptualization state, it is mainly the label and store functions that are executed. The correctly conceptualized DE is appropriately labeled (e.g. it is a cat or a lioness) and stored then in memory if necessary, e.g., if it is a new DE that is being encountered for the first time. Fetching and reading is mainly done after the conceptualization step. Thereby the agent needs to check what it has in memory either to confirm its perception of the object; or to create new and/or edit existing relationships for the DE; or to even derive actions among the many possible actions known to the agent. In respect of this, a previously stored DE may also have to be updated, in which case the agent fetches and reads the DE before it relabels it and stores it again.

At each process, actions are triggered in response to the respective stimuli, knowledge and/or understanding. Mostly, actions are triggered after contextualization, which explains the case of actions appropriate in one context being wrong if taken in another context. E.g., one does not run on seeing a lion in zoo because we contextualize that this is a zoo where the animal is caged. So, the zoo context does not allow for the reflex action to be triggered. It may however be triggered in cases where the contextualization is faulty or inappropriately developed e.g. in young kids.

Actions may be distinguished between automatic and conscious actions, respectively related to automatic and controlled processes [8]. "Automatic processes are inevitably engaged by the presentation of specific stimuli inputs, regardless of the agent's intention". Correspondingly, "... an automatic process is modelled after the reflexes, taxes, and instincts from physiology…" [8]. Note that the automation is not always innate but can also be achieved through extensive practice. Meanwhile automatic actions can also "consume attentional resources once invoked by appropriate stimuli conditions" [8]. This explains the presence of subconscious processes and actions as distinct from reflex processes and actions. Action automation also exists in organization and inference, albeit to a lesser degree especially in inference. Here, the agent instead uses its cognitive functions to process the available information and generate the optimal action.

2.4. Cognitive capabilities of AI/ML tools

AI and ML provide many techniques that process input data to generate solutions as knowledge, decisions, or even actions. For their use towards cognitive autonomy in networks however, it is necessary to define the extent to which these techniques achieve the processes in the perception-reasoning pipeline model. For brevity, this section describes these capabilities without detailing the design or even operation of the respective AI/ML techniques. The tools can be grouped into three major categories: (1) Classical AI systems which are concerned with figuring out a way to act in an environment; (2) Learning from data where the system attempts to capture insights from a large data set; and (3) Online learning where the system learns while acting in an environment that trains the system through feedback. The recently famous fields of Neural Networks and Deep Learning (or simply shallow and deep Neural Networks, respectively) are computation models that allow for the efficient realization of learning solutions.

2.4.1. Classical artificial intelligence

Classical AI techniques mainly refer to Expert, Closed-loop control, Case-based Reasoning, Fuzzy Inference, and other similar systems. Such systems are made up of two basic parts: a knowledge base and an inference mechanism. The knowledge base holds semantic knowledge of objects including names of the objects and the known concepts, theories, and relationships thereof. The inference mechanism includes procedures which examine the knowledge base in an orderly manner and those used to reason and subsequently answer questions, solve problems or make decisions within the domain. It is evident therefore that they mostly achieve inference based on the relationships prescribed by the knowledge base, although they may, to a limited extent, afford some organization by learning new relations among the data in the knowledge base.

2.4.2. Learning from data

Learning from data includes the ML techniques in which a system is trained from a trove of data – specifically the three areas of supervised, unsupervised, or semi-supervised learning. Therein, the respective algorithm is given raw data from which it captures insight about the perceptions (concepts and contexts) of the data and the relationships thereof. Correspondingly, these ML techniques offer an aggregated combination of perception and data organization. Their perceptive capabilities are however limited, since they typically need a preprocessing (transduction) step that translates the observed natural data into a format over which the algorithms are able to reason. Note also, that their ability to predict (e.g. through regression) may be interpreted as an inference capability. This, however, is also limited by the need for a post processing step required to interpret such predictions into the desired knowledge, decisions, or actions.

2.4.3. Reinforcement Learning (RL)

RL is the modern form of optimal control focusing on learning how to optimally act in a given environment. It assumes abstractions of the states in the respective environment to which it learns the optimal actions. Evidently, RL offers mainly data organization and inference based on predefined abstract states.

The capabilities of the three categories of AI/ML techniques show that to realize full cognitive autonomy, a system must combine multiple techniques each of which only achieves subparts of the data processing pipeline. This understanding is used in designing the framework for cognitive autonomy in network management as described in the next section.

3. COGNITIVE AUTONOMY IN NETWORKS

3.1. Taxonomy - levels of automation in networks

Based on the forgoing discussion, the two dimensions for describing an entity are its degree of independence in acting and its level of intelligence in decision making. In the context of CAN, we describe entities as automated, self-organizing, cognitive, or autonomic as follows:

- An automated entity is said to have a fixed way of behaving – responding to a certain stimulus - with the behavior defined a priori by the entity's creator
- A Self-Organized (SO) entity is one capable of selecting actions as triggered by a given signal without external control. This differs from an automated entity in that the internal mechanisms of such an SO entity are of no interest to its owner or user.
- An autonomous or autonomic entity has the freedom to act as it wishes without influence from external entities
- A cognitive entity is one capable of making perceptions and interpretations of its sensory inputs to derive decisions through reasoning.

In effect a self-organized entity may be cognitive but if otherwise, such self-organization is achieved through a hard-wired decision logic within the entity. Subsequently, all cognitive entities are self-organized but not all self-organized entities are cognitive. Correspondingly for networks, the following definitions hold with the relative differences illustrated by Figure 3:

- A scripted or script-controlled network allows scenario specific execution of automation scripts. By and large, the network is still human controlled, but allows the scripts to be run autonomously for those specific and very routine activities.
- A Self-Organizing Network (SON) does not only automate the selection and execution of actions but also interprets events under different context to determine the cause-effect relations of these events under different contexts.
- An autonomous network is one able to act on its own i.e. it does not take dictation or rules from anyone but may however not be able to reason its environment or even be smart enough to make the best static decisions (e.g. incorrectly interpret its internal rules).
- A cognitive network is able to reason and formulate recommendations for subsequent behavior, even where the recommendations must be approved by a human operator before their execution.

Based on these definitions, a cognitive autonomous network has both cognition and autonomy, i.e., it uses reasoning to formulate recommendations for action and subsequently independently executes the derived actions. The degree to which the network is cognitive or not is represented by the 7 capabilities or levels of autonomy illustrated by Figure 3.

3.2. The vision: outlook to eventual CANs

The characterization of the different levels of automation hint at the stages through which network management automation is expected to transit. This path, illustrated by Figure 5 starts with manual control through automated and cognitive automated control to eventually a cognitive autonomous network. The manually controlled network may undertake some automation e.g. using scripts to automate routine actions for operator convenience. The automated network, exemplified by SON, has human-designed control loops that undertake simple control through monitoring and (re-)configuration of network parameters, but the functions are configured by the operator to optimize their performance.

The cognitive automated network adds cognitive capabilities over and above the automation functions while cognitive autonomous networks take full control by not only learning the actions but also the possible applicable contexts in the network. The current network deployments are mainly at the second level since they have deployed several automation functions in the network which are still largely being controlled by the operators. There are, however, publications that push the boundary towards level 3 by proposing learning functions that take the responsibility of configuring the automation functions away from the operator. This has mainly been referred to as Cognitive Network Management (CNM), but the eventual step requires an end-to-end design of the CAN in a way that embeds the learning capabilities of AI/ML techniques into each part of the cognitive functions.

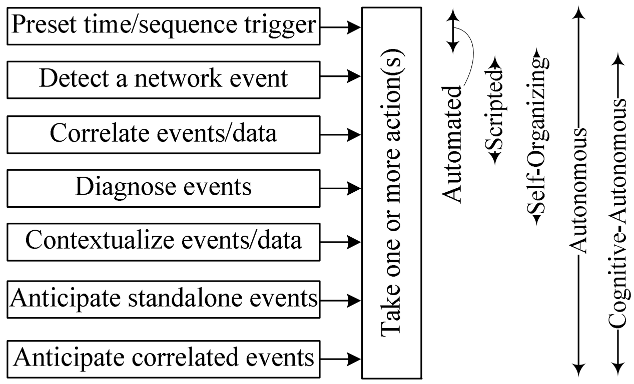


Figure 3: The abstract levels of autonomy in networks

3.3. The CAN framework

To achieve the levels of automation described above, we have proposed the CAN framework of Figure 5 as the system through which NM applications may be designed and integrated into a single cognitive autonomous system for network automation. The framework has five modules to be integrated, specifically the Network Objective Manager (NOM), Environment Modelling and Abstraction Engine (EMA), Decision Applications (DApps), Coordination Engine (CE), and the Configuration Management Engine (CME). The framework applies both to fully-centralized and to quasi-centralized environments (e.g. respectively the traditional 3GPP network management [9] and controllers expected in the new (edge) cloud RAN [10]). All the modules are learning entities, albeit learning from different data and towards different objectives.

The NOM learns how to translate the operator's goals and intents into technical objectives to be fulfilled by the entire network management system. The NOM aggregates the concepts of intent-based, policy-based, and objective-based optimization to derive the technical objectives communicated over interface *a*. The EMA learns to abstract observed network events and contexts (from interface *b*) into consistent network states that are communicated to all the other modules over interface *c*.

The DApps, the core of the Cognitive Functions (CFs), are the specialized applications responsible for specific network configurations and optimizations. Example DApps will target minimization of interference, optimization of mobility, reduction of energy consumption, or coverage and capacity optimization. Each such DApp learns to select the most optimal action for a specific state as detected by the EMA. Note that a CF may exclusively be only the DApp or may also include other functionality besides the DApp.

The CE learns to detect and resolve any possibly conflicting network configurations recommended by the DApps. Such coordination must be natively multi-vendor since the DApps will be expected to be supplied by different vendors.

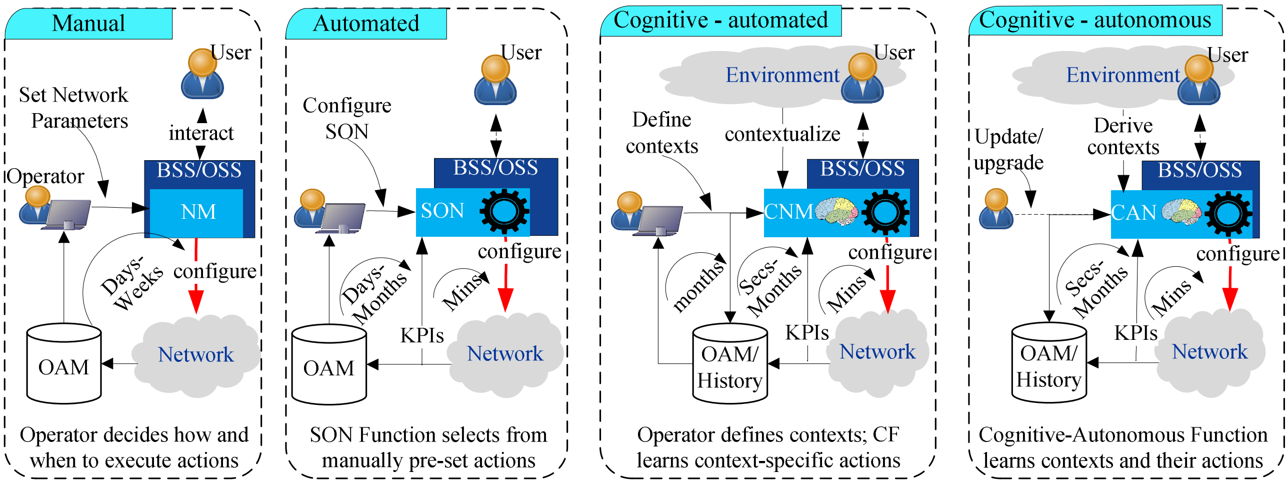


Figure 5: From a manually controlled network to a cognitive autonomous network

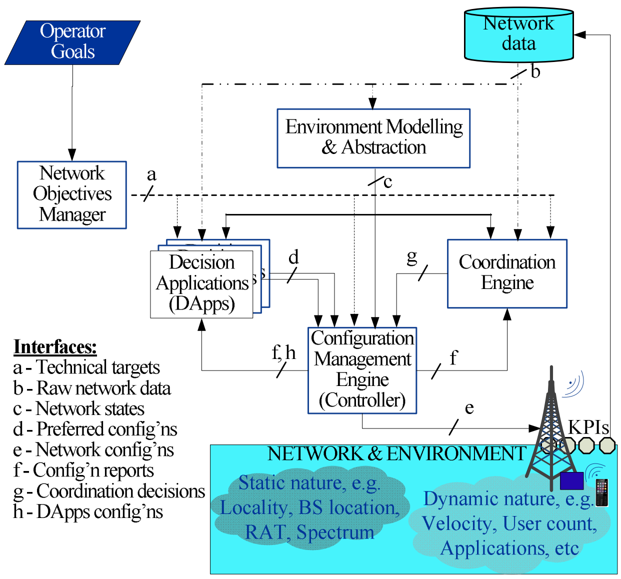


Figure 4: CAN framework – Functions of CAN system and related Cognitive Functions

The CME is the controller for the entire cognitive system instance. First it decides if a DApp configuration recommendation should be enforced on the network. In so doing it is responsible for concurrency control which is different from logical coordination that is undertaken by the CE. The CME communicates the selected network configurations to the DAPPs and the CE (for their learning and coordination purposes) through interface f. Secondly, it also defines and refines the legal/acceptable candidate network configurations for the different contexts of the different DApps based on the meta learning from the CE. In the simplest form, the CME masks a subset of the possible network configurations as being unnecessary (or unreachable) within a specific abstract state. So, the set of possible network configurations is fixed and the CF/DApp only selects from within this fixed set when in the specific abstract state. A more cognitive CME may, however, also be able to add, remove or modify (e.g., split or combine) the network configurations based on the learning of how or if the network configurations are useful.

It is obvious that without the specialized DApps, the CE is the default automation engine. The critical aspect of the design is that the system does not have to observe all states in order to know how to behave. Full knowledge of all states can be achieved by extrapolation from known data, i.e., the observations made in some states can be used to predict how to behave in other network states.

4. LEARNING NETWORK BEHAVIOR – A CAN EXAMPLE FOR MOBILITY MANAGEMENT

Let us assume a CAN and the use case of managing terminal mobility. Using a RL DApp (e.g. like that in [10][12]), the CAN is able to learn the optimal behavior for a mobility state (the average velocity observed in the cell) as the best Hysteresis (Hys) and Time-to-Trigger (TTT) values for the state. For the network, the state-action space is very large and not all states are frequently observable (some states are very rare) yet the CAN needs to know how to behave in all states. We show here that CANs can effectively learn the network response in the unknown states based on their observations in the known states. The CAN is particularized as supervised learning algorithms which, using multiple examples, learn to perceive a data element as instance of the earlier-on learned network's response to mobility management parameters. Then, by reasoning over the DE's relationship with the earlier examples, the algorithms can predict the likely network's response to that instance.

4.1. Simulation set up

For this study, we obtained data from simulations for 6 velocity states [3,10,30,60,90,120 in kmph] and different mobility configurations (Hys and TTT) in an LTE network of 21 states using a simulator described in [10][12]. For each configuration, we simulate 200 minutes of network operation and note the rates of handover (HO) successes, Ping-Pongs,

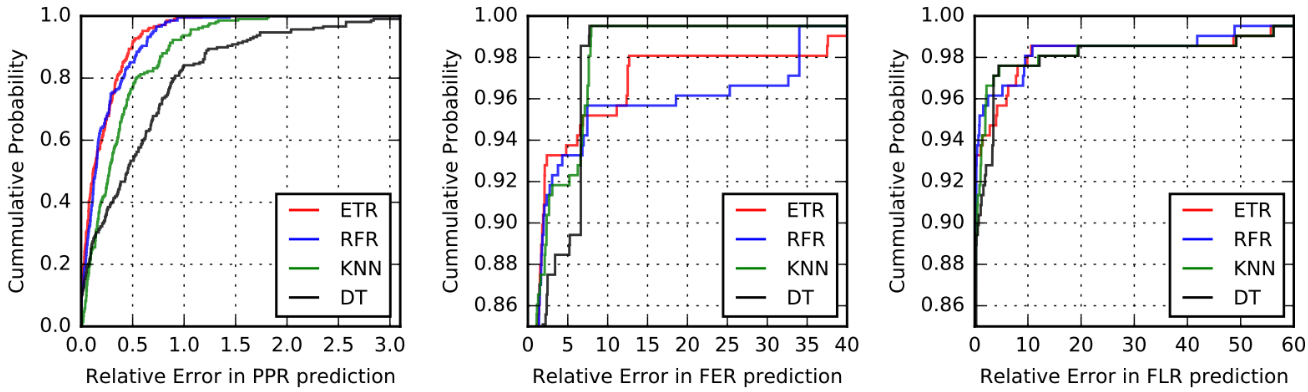


Figure 6: Learning network response – ML algorithms predict behavior in unknown states using response in known states

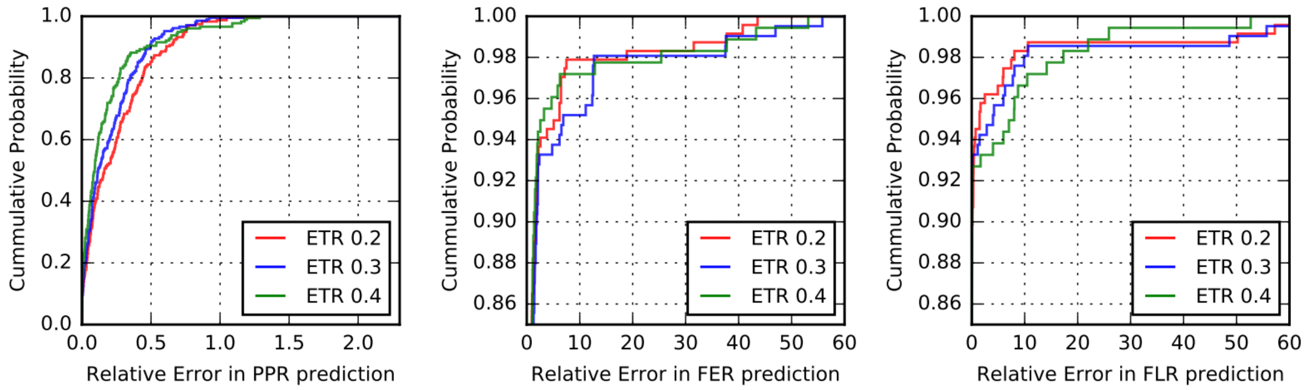


Figure 7: The effect of number of known states – knowing more states may not significantly improve prediction accuracy

and Radio Link Failures due to early and late handovers (HOS, PPR, FER, FLR respectively) as defined in [11]. We divide the data into training and test sets, the training set indicating the subspace which the CAN will have learned. The intention is to use machine learning regression (an expected capability of the DApps, CE, or CME) to determine how well we can predict network performance at unknown combinations of velocity and Hys-TTT configurations.

We compare four models for prediction, which are regressors based on k-Nearest Neighbors Regression (KNN) [13]; Decision Trees (DT)[14][15], Random Forests (RFR) [15], and Extremely Randomized Trees (ETR) [15]. Each model is trained to predict the three rates (PPR, FER, FLR) with accuracy evaluated in terms of Relative Error (RE) of the respective rate. For each point i of rate y, RE is the absolute error relative to expectation of the rate E{y} as in (1)

$$RE = \frac{|y_i - \hat{y}_i|}{E\{y\}} \tag{1}$$

4.2. Performance results

The relative accuracy of the models is shown in the CDFs of Figures 6,7, and 8. First we see in Figure 6 that all three regressors learn fairly good network response functions for PPR and FER and even better functions for FLR, i.e., the error made in predicting the rate is very small in the majority of unknown states. For a small set of examples, however as expected, the models make extremely poor predictions – explaining the cases with RE>>1. As such the models will in most of the cases select the right parameter values. In Figure 7, we use the best model (ETR) and compare the proportion of the state-space that needs to be known to guarantee accuracy. Taking 10%, 20% and 40% of the data as training data, we observe that although the accuracy increases with the amount of training data, the respective increase is insignificant especially for the link failure rates. This indicates that the units do not need to be trained on excessively large amount of data for them to be able to derive structure.

However, it may be possible to achieve better outcomes through smart combinations of algorithms. With knowledge that FER is zero for low to medium HO delay, a two-step learning process that first separates the zero-FER region can, e.g., improve the prediction. Here, a classification step learns the zero-FER boundary so that the regression only learns the non-zero response function. Applying this with 10% training data on the random forests and extremely randomized trees models (hereafter respectively named RFC and ETC) improves the performance as showed in Figure 8. In both cases (RFR vs. RFC and ETR vs. ETC), the performance improves for all prediction states. This demonstrates the benefit of combining multiple models to achieve the perception-reasoning model. In this case, by first identifying if a given sample is within or outside the zero-FER region,

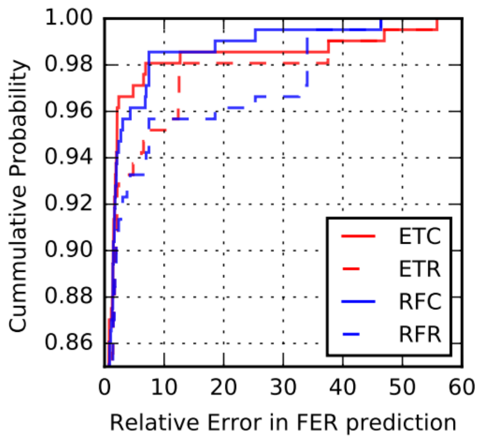


Figure 8: Smart combination of different algorithms

classification improves the perception before the reasoning is applied to predict the actual non-zero FER value.

These results show that learning methods can be used to automate network management functions not only to learn the best configurations for specific states but to also learn the underlying network response which can then be used to predict response in unknown states.

5. CONCLUSION AND OUTLOOK

This paper has outlined a framework for Cognitive Autonomous Networks (CAN). A cognitive entity is one capable of perceiving stimuli, transforming them into data elements over which it reasons to select actions. It conceptualizes and contextualizes a data element and logically or arithmetically relates it with other data elements to make inferences about the elements and their relations and, subsequently, to select the appropriate action. Networks with this capability and the ability to independently act become CANs. We have proposed a cognition model based on this perception-reasoning flow and used it to describe the path towards CAN and a functional design of a typical CAN system for which AI/ML techniques form a part of each function. We then showed how this kind of learning can be beneficial in network operations using a use case of learning a network's response to different mobility states and handover configurations. Our future work is to build and test a complete CAN based on the proposed framework.

REFERENCES

[1] ITU T. Recommendation, "M. 3400: TMN management functions." (2000).

[2] S. Hämäläinen, H. Sanneck, C. Sartori (Eds.), "LTE Self-Organising Networks (SON)," John Wiley & Sons, 2012

[3] Diehl-Fleig, E., and A. M. De Araujo. "Haplometrosis and pleometrosis in the antAcromyrmex striatus (Hymenoptera: Formicidae)." Insectes sociaux 43, no. 1 (1996): 47-51- Springer

[4] Theraulaz, Guy, Jacques Gautrais, Scott Camazine, & Jean-Louis Deneubourg. "The formation of spatial patterns in social insects: from simple behaviours to complex structures." A Philosophical Transactions of the Royal Society of London: Mathematical, Physical and Engineering Sciences 361, no. 1807 (2003): 1263-1282.

[5] Marco Dorigo, Gianni Di Caro and Luca M. Gambardella, "Ant Algorithms for Discrete Optimization", Artificial Life, MIT Press, 1999

[6] Lixiang Li, Haipeng Peng, Jürgen Kurths, Yixian Yang, and Hans Joachim Schellnhuber, "Chaos–order transition in foraging behavior of ants", Proc National Academy Sciences U.S.A. 2014 Jun 10; 111(23): 8392–8397.

[7] Stephen K. Reed, "Cognition: Theory and Application", 9th, Cengage Learning, 2012

[8] Kihlstrom, John F. "The psychological unconscious." Handbook of personality. Theory and research (1990): 424-442.

[9] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; "Telecommunication management; Principles and high-level requirements (Release 15)," 3GPP, Tech. Spec. 32.101 V15.0.0, September 2017. [Online]. Available: http://www.3gpp.org

[10] Huaning Niu, Clara (Qian) Li, Apostolos Papathanassiou, Geng Wu, "RAN Architecture Options and Performance for 5G Network Evolution", IEEE WCNC 2014 - Workshop on Wireless Evolution Beyond 2020

[11] Mwanje, Stephen S., and Andreas Mitschele-Thiel, "Distributed cooperative Q-learning for mobility-sensitive handover optimization in LTE SON." Computers and Communication (ISCC), 2014 IEEE Symposium on. IEEE, 2014.

[12] S. Mwanje, L.C. Schmelz, and A. Mitschele-Thiel, "Cognitive Cellular Networks: A Q-Learning Framework for Self-Organizing Networks," IEEE Transactions on Network and Service Management, vol 13, no. 1, pp. 85 – 98, January 2016.

[13] Altman, N. S. "An introduction to kernel and nearest-neighbor nonparametric regression". The American Statistician. 46 (3) *(1992)*: *175–185*. doi*:*10.1080/00031305.1992.10475879.

[14] T. Hastie, R. Tibshirani & J. Friedman, "Elements of Statistical Learning", Springer, 2009. And L. Breinan

[15] Random Forests regressor - L. Breiman, "Random Forests", Machine Learning, 45(1), 5-32, 2001.

[16] P. Geurts, D. Ernst., and L. Wehenkel, "Extremely randomized trees", Machine Learning, 63(1), 3-42, 2006.

SESSION 3

MACHINE LEARNING IN TELECOMMUNICATION NETWORKS - II

MACHINE LEARNING OPPORTUNITIES IN CLOUD COMPUTING DATA CENTER MANAGEMENT FOR 5G SERVICES

Fabio López-Pires[1] and *Benjamín Barán*[2]

[1]Itaipu Technological Park, Hernandarias, Paraguay
[2]National University of the East, Ciudad del Este, Paraguay

ABSTRACT

Emerging paradigms associated with cloud computing operations are considered to serve as a basis for integrating 5G components and protocols. In the context of resource management for cloud computing data centers, several research challenges could be addressed through state-of-the-art machine learning techniques. This paper presents identified opportunities on improving critical resource management decisions, analyzing the potential of applying machine learning to solve these relevant problems, mainly in two-phase optimization schemes for virtual machine placement (VMP). Potencial directions for future research are also presented.

Keywords - 5G service operations, cloud data centers, machine learning, virtual machine placement.

1. INTRODUCTION

According to Rost et al. [17], 5G networks and services will increase exponentially in data traffic, storage and processing, considering smartphones as gateways to remotely access resources through cloud computing. In this case, several challenges should be addressed to further advance cloud computing in order to serve as a basis to integrate 5G components and protocols.

In the context of resource management for cloud computing data centers, main research challenges could be addressed by designing management solutions based on machine learning (ML) techniques.

This work briefly discusses recent contributions on one of the most studied problems for resource allocation in cloud computing data centers: the process of selecting which requested virtual machines (VMs) should be hosted at each available physical machine (PM) of a cloud computing infrastructure, commonly known as virtual machine placement (VMP). The considered contributions focus on a two-phase optimization scheme for VMP problems [1] (see Figure 1), which takes into account incremental VMP (iVMP) and VMP reconfiguration (VMPr) as the main sub-problems with online and offline phases respectively.

The identified challenges for considered VMP problems [11] are presented on the particular context of 5G services, and mainly take into account ML techniques for addressing relevant decision making on cloud computing infrastructure operations (e.g. *when a VMPr phase should be triggered?*). Additionally, network management challenges based on software-defined networking (SDN) are also analyzed from the perspective of VMP problems, where ML techniques may result in a promising approach to support these types of operational decisions. Finally, different open challenges are discussed as future directions to further advance this active research field.

The remainder of this work is structured as follows: Section 2 briefly presents the considered two-phase optimization scheme for VMP problems, while Section 3 discusses the main opportunities for ML techniques as a promising approach to address identified research challenges. Finally, conclusions and future directions are left to Section 4.

2. TWO-PHASE OPTIMIZATION SCHEME FOR VMP PROBLEMS IN CLOUD COMPUTING

Recent research advances in VMP problems for cloud computing include proposals of complex infrastructure as a service (IaaS) environments for VMP problems, considering both service elasticity and the overbooking of physical resources [14]. In the context of 5G services, and considering smartphones as simple gateways to access remote resources as previously mentioned [17], 5G service providers should associate a cloud service infrastructure with each mobile customer. A cloud service infrastructure S_b may be composed of a set of VMs according to customer preferences or requirements, where both elasticity and overbooking should be considered, as previously proposed by the authors in [14]. In the described context, VMP problems represent an important topic for cloud computing data center management. The following sub-sections describe the highlights of a two-phase optimization scheme for VMP problems in cloud computing, representing the main focus of the challenges analyzed in this work.

2.1 Considered VMP Formulation

An online problem formulation is considered when inputs of the problem change over time and algorithms do not have the entire input set available from the beginning (e.g. online heuristics) [3]. On the other hand, if inputs of the problem do not change over time, the formulation is considered offline (e.g. memetic algorithms (MAs) proposed in [8] and [12]).

Online decisions made along the operation of a dynamic cloud computing infrastructure negatively affects the quality

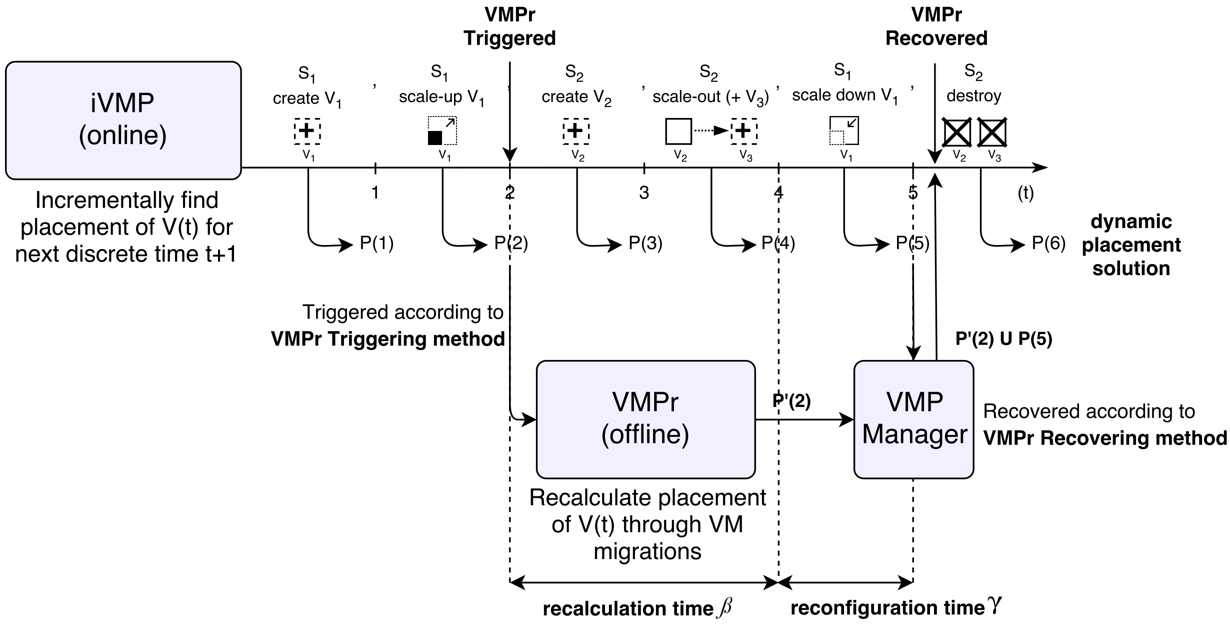


Figure 1 – Two-phase optimization scheme for VMP problems considered in this work, presenting a basic example with a placement recalculation time of $\beta = 2$ (from $t = 2$ to $t = 4$) and a placement reconfiguration time of $\gamma = 1$ (from $t = 4$ to $t = 5$).

of obtained solutions in VMP problems when compared to offline decisions [13]. Offline algorithms present a substantial advantage over online alternatives. Unfortunately, offline formulations are not appropriate for highly dynamic environments of real-world IaaS providers, where cloud services are requested dynamically according to current demand. In this context, a previously proposed two-phase optimization scheme is considered, combining advantages of online and offline VMP formulations and decomposing VMP problems into two different sub-problems: (1) (online) incremental VMP (iVMP) and (2) (offline) VMP reconfiguration (VMPr).

The iVMP sub-problem is considered for dynamic arriving requests, where VMs could be created, modified and removed at runtime. Consequently, this sub-problem should be formulated as an online problem and solved with short time constraints, where existing heuristics could be reasonably appropriate. In online algorithms for iVMP, decisions are performed at each discrete time t. The considered iVMP problem is based on [13] and could be formally enunciated as:

Given a complex IaaS environment composed by a set of PMs (H), a set of active VMs already requested before time t ($V(t)$), and the current placement of VMs into PMs (i.e. $x(t)$), an incremental placement of $V(t)$ into H for the time $t+1$ ($x(t+1)$) without migrations is sought, satisfying the problem constraints and optimizing the considered objective functions.

The considered formulation of the iVMP problem receives the following information as input data:

- a set of n available PMs and their specifications;
- a dynamic set of $m(t)$ requested VMs (already allocated VMs plus new requests) and their specifications;
- information about the utilization of resources of each active VM at each discrete time t;
- the current placement at each discrete time t (i.e. $x(t)$).

The result of the iVMP phase at each discrete time t is an incremental placement $\Delta x(t)$ for the next time instant in such a way that $x(t+1) = x(t) + \Delta x(t)$. The placement at $t+1$ is represented as a matrix $x(t+1) \in \{0,1\}^{m(t)\times n}$, as defined in Equation (*(1)*):

$$x(t+1) = \begin{bmatrix} x_{1,1}(t+1) & \dots & x_{1,n}(t+1) \\ \dots & \dots & \dots \\ x_{m(t),1}(t+1) & \dots & x_{m(t),n}(t+1) \end{bmatrix} \quad (1)$$

Formally, the placement for the next discrete time instant $x(t+1)$ is a function of the current placement $x(t)$ and the active VMs at discrete time t, i.e.:

$$x(t+1) = f\,[x(t), V(t)] \quad (2)$$

Additionally, the VMPr sub-problem is considered for improving the quality of solutions obtained in the iVMP phase, reconfiguring the placement through VM migrations. This sub-problem could be formulated offline, where alternative solution techniques could result in more suitable ones (e.g. meta-heuristics). An offline algorithm solves a VMP problem considering a static environment, where VM requests do not change over time considering the migration of VMs between PMs. The formulation of the considered VMPr problem is based on [12] and could be enunciated as:

Given a current placement of VMs into PMs ($x(t)$), a placement reconfiguration through migration of VMs between PMs for the discrete time t (i.e. $x'(t)$) is sought, satisfying the constraints and optimizing the considered objective functions.

The proposed formulation of the VMPr problem receives the following information as input data:

- a set of n available PMs and their specifications;
- information about the utilization of resources of each active VM at discrete time t;
- the current placement at discrete time t (i.e. $x(t)$).

The considered optimization scheme for the VMP problem is based on methods to decide when or under what circumstances to trigger placement reconfigurations with the migration of VMs between PMs (VMPr triggering) and what to do with cloud services requested during placement recalculation time (VMPr recovering). The VMPr phase is triggered according to a given VMPr triggering method (see Section 2.2).

Once the VMPr is triggered, the placement of VMs at discrete time t is recalculated during β discrete time slots (i.e. recalculation time). The result of the VMPr problem is a placement reconfiguration for the discrete time $t-\beta$ (i.e. $x'(t-\beta)$). It is important to note that the recalculated placement is potentially obsolete, considering the offline nature of the VMPr phase. In fact, while the VMPr is making its calculation, the iVMP still may receive and serve arriving requests, making obsolete the VMPr calculated solution; therefore, the recalculated placement must be recovered accordingly using a VMPr recovering method, before complete reconfiguration is performed. The recovering process as well as the migration of VMs are performed in γ discrete time slots (i.e. reconfiguration time), where γ may vary according to the maximum amount of RAM to be migrated. Figure 1 presents the described two-phase optimization scheme, considering $\beta = 2$, from $t = 2$ to $t = 4$ and $\gamma = 1$, from $t = 4$ to $t = 5$.

It is important to note that a large number of possible objective functions $F(x,t)$ and constraints $e(x,t)$ could be considered for a VMP problem formulation, according to provider preferences [11, 10].

2.2 Considered VMPr Triggering Methods

A VMPr triggering method defines when or under what circumstances a VMPr phase should be triggered in a two-phase optimization scheme for VMP problems. By considering studied VMPr triggering methods (see Table 1), three main approaches may be identified: (1) periodical, (2) threshold-based and (3) prediction-based. The following sub-sections describe the VMPr triggering methods evaluated in this work as part of a two-phase optimization scheme for VMP problems.

Table 1 – Summary of studied triggering methods.

References	VMPr triggering
[4, 21, 6, 9, 5, 22, 19]	Periodically
[2, 18, 20]	Threshold-based
[14]	Prediction-based

2.2.1 Periodical Triggering

As presented in Table 1, several studied works have looked at periodically triggering the VMPr phase. Periodically triggering the VMPr could present disadvantages when defining a fixed reconfiguration period (e.g. every 10 time instants). For example, a reconfiguration could be required before the established time, where optimization opportunities could be wasted or even economical penalties could impact cloud data center operation. On the other hand, in certain cases the reconfiguration may not be necessary and triggering the VMPr could represent profitless reconfigurations.

2.2.2 Threshold-based Triggering

Another regularly studied VMPr triggering method considers a threshold-based approach (see Table 1), where thresholds are defined in terms of utilization of PM resources (e.g. CPU). Thresholds indicate when a PM H_i is considered to be underloaded or overloaded, and consequently, a VMPr should be triggered. For example, fixing utilization thresholds for overloaded and underloaded PM detection, for all considered resources, to 10% and 90% respectively. The described threshold-based VMPr triggering method makes isolated reconfiguration decisions at each PM without the complete knowledge of global optimization objectives, giving place to a distributed decision approach.

2.2.3 Prediction-based Triggering

Considering the main identified issues related to the studied VMPr triggering methods, prediction-based VMPr triggering methods were recently proposed in the VMP specialized literature, statistically analyzing an objective function $F(x,t)$ that is optimized and proactively detecting situations where a VMPr triggering is potentially required for a placement reconfiguration. The considered prediction-based VMPr triggering method uses a double exponential smoothing (DES) [7] as a statistical technique for predicting values of the objective function $F(x,t)$, mathematically formulated next:

$$S_t = \alpha \times Z_t + (1-\tau)(S_{t-1} + b_{t-1}) \tag{3}$$

$$b_t = \tau(S_t - S_{t-1}) + (1-\tau)(b_{t-1}) \tag{4}$$

$$\overline{Z}_{t+1} = S_t + b_t \tag{5}$$

where:

α: Smoothing factor, where $0 \le \alpha \le 1$;
τ: Trend factor, where $0 \le \tau \le 1$;
Z_t: Known value of $F(x,t)$ at discrete time t;
S_t: Expected value of $F(x,t)$ at discrete time t;
b_t: Trend of $F(x,t)$ at discrete time t;
$\overline{Z}_{t+1}$: Value of $F(x,t+1)$ predicted at discrete time t.

At each discrete time t, the prediction-based VMPr triggering method predicts the next M values of $F(x,t)$ and effectively triggers the VMPr phase in case $F(x,t)$ is predicted to consistently increase, considering that $F(x,t)$ is being minimized.

Considering the different approaches presented in Table 1, recent research work by the authors [14] validate that algorithms considering prediction-based VMPr triggering methods for solving a VMP problem in a two-phase optimization scheme outperform other evaluated alternatives. Consequently, designing novel prediction-based VMPr triggering methods may improve operations of cloud computing data centers, where ML techniques represent a promising approach.

Additionally to the potential of applying ML techniques for VMPr triggering methods, several other issues should be considered during the reconfiguration time, once a placement reconfiguration is accepted.

In the next section, two main identified opportunities for ML techniques are summarized in order to improve cloud computing data center management.

3. MACHINE LEARNING OPPORTUNITIES

According to Mitchell et al. [15], a broadly accepted definition of algorithms in machine learning fields is that: *A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P if its performance at tasks in T, as measured by P, improves with experience E.*

Additionally, it is important to remember that machine learning may be broadly classified into [23]:

- **Supervised Learning**: where inputs and desired outputs (labels) are given to the learning algorithm as a training phase.
- **Unsupervised Learning:** where no labels are given, leaving the learning algorithm to find structure in its inputs.

In the context of the research topic presented in this work, most important applications include **Regression** (supervised learning) and **Clustering** (unsupervised learning). Section 3.1 discusses opportunities for ML techniques in **Regression** and its application to prediction problems, particularly for proposing novel VMPr Triggering, while Section 3.2 describes ML opportunities in **Clustering** and its application to cloud computing network management.

3.1 ML for VMPr Triggering

In the context of the studied two-phase optimization scheme for VMP problems in cloud computing environments, prediction-based VMPr triggering methods represent a promising triggering approach, as previously studied by the authors in [14]. To the best of the author's knowledge, existing VMPr triggering methods consider basic statistical techniques (e.g. double exponential smoothing) for deciding when or under what circumstances to trigger a VMPr phase. A regression analysis based on current operational data on cloud computing data centers may improve prediction models in real-world implementations, as 5G service providers. Consequently, exploring alternative techniques for predicting when to trigger a VMPr phase should advance the field of the studied VMP problems, considering the following research questions:

- ***RQ 1:*** *which ML techniques could be considered more appropriate for VMPr Triggering methods?*
- ***RQ 2:*** *how important is to accurately predict when to trigger a VMPr phase in VMP problems?*
- ***RQ 3:*** *rather than predicting future objective function values, what other parameters could be evaluated for VMPr Triggering methods?*

3.2 ML for Network Management

In the context of 5G networks, mobile operations should include critical and fault-tolerant services, where live migration of VMs between PMs in VMPr phases may require short-time re-routing strategies and adaptive topologies, where SDN represents a valid approach in cloud computing networks. Consequently, considering network routing reconfiguration (NRR) [16] as part of VMP problems also represent opportunities for ML techniques to predictively reconfigure networking topologies and routes in cloud services.

Additionally, several formulations consider inter-VM network traffic minimization by locating VMs with high network communication rate in the same PM, as studied in [12]. In this case, studying techniques for clustering these VMs may result in being useful for this particular operational decision making. Consequently, the following research questions may be analyzed:

- ***RQ 4:*** *which ML techniques could be considered more appropriate for predicting Network Routing Reconfiguration (NRR) as part of VMP problems in SDN implementations?*
- ***RQ 5:*** *which ML techniques could be considered more appropriate for clustering VMs for supporting placement decisions?*

It is important to note that several other challenges and opportunities may be considered for applying ML techniques to improve cloud computing data center management in 5G service operations.

4. CONCLUSIONS AND FUTURE DIRECTIONS

In the context of resource management for cloud computing data centers, several challenges may be addressed by considering state-of-the-art machine learning techniques. This paper presented identified opportunities on improving critical resource management decisions, analyzing the potential of applying machine learning to solve these relevant problems, mainly in **Regression** and **Clustering** applications. A two-phase optimization scheme for VMP problems was considered to present opportunities for machine learning techniques as a promising approach to address identified research challenges such as proposing novel prediction-based VMPr triggering methods (see Section 3.1) and applying clustering algorithms to identify VMs with high communication rates to allocate them in the same PM if possible in order to minimize inter-VM network traffic (see Section 3.2).

As a concrete summary of the presented challenges and opportunities, five relevant research questions were proposed as future directions (i.e. RQ 1 to RQ 5) to further advance this research field.

REFERENCES

[1] Augusto Amarilla, Saúl Zalimben, Leonardo Benítez, Fabio López-Pires, and Benjamín Barán. Evaluating a two-phase virtual machine placement optimization scheme for cloud computing datacenters. In *2017 Metaheuristics International Conference (MIC)*, pages 99–108, 2017.

[2] Anton Beloglazov, Jemal Abawajy, and Rajkumar Buyya. Energy-aware resource allocation heuristics for efficient management of data centers for cloud computing. *Future Generation Computer Systems*, 28(5):755–768, 2012.

[3] Anton Beloglazov and Rajkumar Buyya. Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in cloud data centers. *Concurrency and Computation: Practice and Experience*, 24(13):1397–1420, 2012.

[4] Nicolò Maria Calcavecchia, Ofer Biran, Erez Hadad, and Yosef Moatti. Vm placement strategies for cloud scenarios. In *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference on*, pages 852–859. IEEE, 2012.

[5] Fahimeh Farahnakin, Rami Bahsoon, Pasi Liljeberg, and Tapio Pahikkala. Self-adaptive resource management system in iaas clouds. In Rami Bahsoon, Pasi Liljeberg, and Tapio Pahikkala, editors, *9th International Conference on Cloud Computing (IEEE CLOUD)*, pages 553–560. IEEE, 2016.

[6] Eugen Feller, Christine Morin, and Armel Esnault. A case for fully decentralized dynamic vm consolidation in clouds. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pages 26–33. IEEE, 2012.

[7] J. Huang, C. Li, and J. Yu. Resource prediction based on double exponential smoothing in cloud computing. In *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pages 2056–2060, April 2012.

[8] Diego Ihara, Fabio López-Pires, and Benjamín Barán. Many-objective virtual machine placement for dynamic environments. In *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*, pages 75–79. IEEE, 2015.

[9] Xiao-Fang Liu, Zhi-Hui Zhan, Ke-Jing Du, and Wei-Neng Chen. Energy aware virtual machine placement scheduling in cloud computing based on ant colony optimization approach. In *Proceedings of the 2014 conference on Genetic and evolutionary computation*, pages 41–48. ACM, 2014.

[10] Fabio López-Pires and Benjamín Barán. A virtual machine placement taxonomy. In *Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on*, pages 159–168. IEEE Computer Society, May 2015.

[11] Fabio López-Pires and Benjamín Barán. Cloud computing resource allocation taxonomies. *International Journal of Cloud Computing*, 6(3):238–264, 2017.

[12] Fabio López-Pires and Benjamín Barán. Many-objective virtual machine placement. *Journal of Grid Computing*, 15(2):161–176, 2017.

[13] Fabio López-Pires, Benjamín Barán, Augusto Amarilla, Leonardo Benítez, Rodrigo Ferreira, and Saúl Zalimben. An experimental comparison of algorithms for virtual machine placement considering many objectives. In *9th Latin America Networking Conference (LANC)*, pages 75–79, 2016.

[14] Fabio López-Pires, Benjamín Barán, Leonardo Benítez, Saúl Zalimben, and Augusto Amarilla. Virtual machine placement for elastic infrastructures in overbooked cloud computing datacenters under uncertainty. *Future Generation Computer Systems*, 79:830 – 848, 2018.

[15] Ryszard S Michalski, Jaime G Carbonell, and Tom M Mitchell. *Machine learning: An artificial intelligence approach*. Springer Science & Business Media, 2013.

[16] Bruno Astuto A Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti. A survey of software-defined networking: Past, present, and future of programmable networks. *IEEE Communications Surveys & Tutorials*, 16(3):1617–1634, 2014.

[17] Peter Rost, Carlos J Bernardos, Antonio De Domenico, Marco Di Girolamo, Massinissa Lalam, Andreas Maeder, Dario Sabella, and Dirk Wübben. Cloud technologies for flexible 5g radio access networks. *IEEE Communications Magazine*, 52(5):68–76, 2014.

[18] Jiyuan Shi, Fang Dong, Jinghui Zhang, Junzhou Luo, and Ding Ding. Two-phase online virtual machine placement in heterogeneous cloud data center. In *Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference on*, pages 1369–1374. IEEE, 2015.

[19] Petter Sv, Wubin Li, Eddie Wadbro, Johan Tordsson, Erik Elmroth, et al. Continuous datacenter consolidation. In *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 387–396. IEEE, 2015.

[20] Michael Tighe and Michael Bauer. Integrating cloud application autoscaling with dynamic vm allocation. In *2014 IEEE Network Operations and Management Symposium (NOMS)*, pages 1–9. IEEE, 2014.

[21] Wenying Yue and Qiushuang Chen. Dynamic placement of virtual machines with both deterministic and stochastic demands for green cloud computing. *Mathematical Problems in Engineering*, 2014, 2014.

[22] Qinghua Zheng, Rui Li, Xiuqi Li, Nazaraf Shah, Jianke Zhang, Feng Tian, Kuo-Ming Chao, and Jia Li. Virtual machine consolidated placement based on multi-objective biogeography-based optimization. *Future Generation Computer Systems*, 54:95–122, 2016.

[23] Xiaojin Zhu. Semi-supervised learning literature survey. *Computer Science, University of Wisconsin-Madison*, 2(3):4, 2006.

CONSIDERATION ON AUTOMATION OF 5G NETWORK SLICING WITH MACHINE LEARNING

Ved P. Kafle, Yusuke Fukushima, Pedro Martinez-Julia, and Takaya Miyazawa

National Institute of Information and Communications Technology, Tokyo, Japan

ABSTRACT

Machine learning has the capability to provide simpler solutions to complex problems by analyzing a huge volume of data in a short time, learning for adapting its functionality to dynamically changing environments, and predicting near future events with reasonably good accuracy. The 5G communication networks are getting complex due to emergence of unprecedentedly huge number of new connected devices and new types of services. Moreover, the requirements of creating virtual network slices suitable to provide optimal services for diverse users and applications are posing challenges to the efficient management of network resources, processing information about a huge volume of traffic, staying robust against all potential security threats, and adaptively adjustment of network functionality for time-varying workload. In this paper, we introduce about the envisioned 5G network slicing and elaborate the necessity of automation of network functions for the design, construction, deployment, operation, control and management of network slices. We then revisit the machine learning techniques that can be applied for the automation of network functions. We also discuss the status of artificial intelligence and machine learning related activities being progressed in standards development organizations and industrial forums.

Keywords— Machine learning, artificial intelligence, 5G network, slicing, standardization

1. INTRODUCTION

The 5G networks are expected to enable ultra-high-speed data transmission (about 10Gbps) that would be about 1000 times the speed of current LTE networks, connect massive number of devices that would be 10-100 times the number of existing mobile phones, ultra-low latency (about 1ms) that would be 5 times lower than the latency of LTE networks, and highly energy efficient with 10 times longer battery life [1]. They should be possessed with the capability to satisfy the diverse requirements of various services for the fully connected smart society, such as enhanced mobile broadband (*eMBB*), massive machine type communication (*mMTC*), and ultra-reliable and low latency communication (*URLLC*). Since each of these services requires different types of network capabilities (e.g., *eMBB* services require very high bandwidth and *mMTC* services require ultra-dense connectivity), they cannot be provided effectively over a single homogeneous network. Therefore, 5G networks are being enabled with the capability of the on-demand constructions of network slices with sufficient resources by using network function virtualization (NFV) and software defined networking (SDN) technologies. A network slice is configured and controlled dynamically by software, which is also called network softwarization [2].

A huge volume of data of complex nature need to be analyzed to carry out smart decision for the design, construction, deployment, operation, administration and management of a network slice so that it can effectively satisfy the quality of service (QoS) requirements of the service intended to be delivered through it, despite time-varying workloads and network conditions. It is difficult for a human to create and operate network slices manually by processing the large volumes of data in a short time. Therefore, it is being necessary to automate these tasks. Machine learning techniques are enabler for the automation of network slicing functions. Machine learning has the capability of sensing (e.g., anomaly detection), mining (e.g., service classification), prediction (e.g., forecasting user or traffic trend), and reasoning (e.g., configuration of system parameters for adaptation) [3]. Namely, it has capabilities to analyze a huge volume of data in a very short time, learn to adjust the system to time-varying environments, make prediction of future events with reasonably good accuracy, and prescribe proactive solutions.

Machine learning has been considered for the automation of various functions of network operation and management, such as resource management, on-demand and adaptive network configuration, service creation and orchestration, fault detection, security, mobility management, user experience enhancement, and dynamic adjustment of policy [3]. Recent advancements in big data, cloud computing, cyber physical systems (CPS), and Internet of Thing (IoT) have become enabler for the realization of artificial intelligence (AI) and machine learning based network control and management technologies [4].

In this paper, we describe the envisioned 5G network slicing and elaborate the necessity of automation of network functions for the design, construction, deployment, operation, control and management of network slices. We then provide an overview of machine learning techniques that can be applied to the automation of network functions. We also discuss the status of artificial intelligence and machine learning related activities being progressed in various standards development organizations (SDO) and industrial forums. The main contribution of this paper is to highlight the essential functions of network slicing and

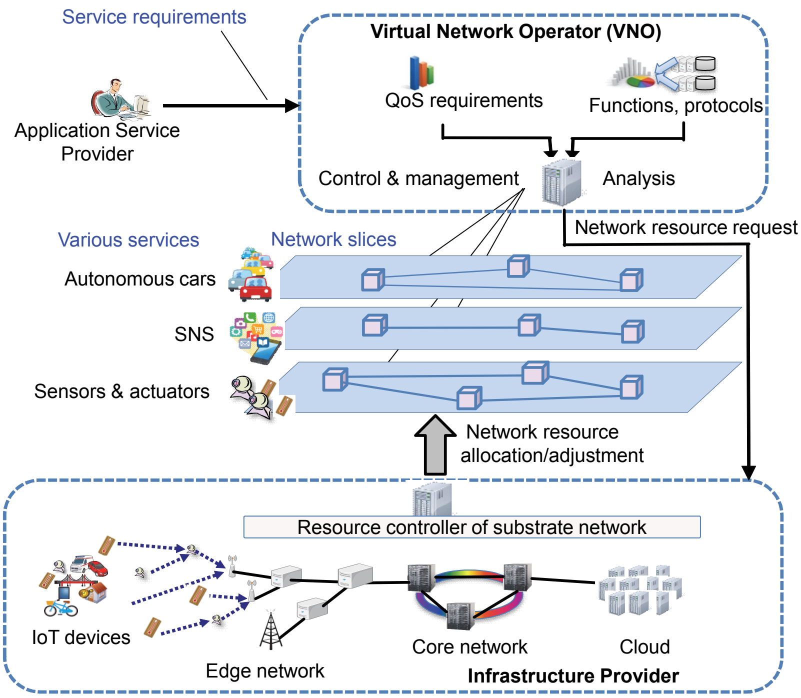


Figure 1. The concept of network slicing for 5G services.

discuss the applicability of machine learning to enable the 5G slicing functions to be executed autonomously. This discussion can be useful reference material for the development of standard technologies for the automation of 5G network slicing functions by using machine learning techniques.

The remainder of the paper is organized as follows. Section 2 gives an overview of 5G network slicing. Section 3 lists network automation functions, and Section 4 gives an overview of machine learning techniques for the automation of network slicing. Section 5 outlines the AI and machine learning activities being pursued in various SDOs and industrial forums, and Section 6 concludes this paper.

2. 5G NETWORK SLICING

Network slicing is the key design concept being introduced in 5G/IMT-2020 networks. The design consideration for IMT 2020 network architecture specified in ITU-T Recommendation Y.3102 are network capability exposure, separation of control and data planes, common interfaces to support access network agnostic common core network, and efficient support of various mobility requirements [2].

Figure 1 illustrates the structure of virtualized networking environment, considering three stakeholders: infrastructure provider, virtual network operator (VNO), and application service provider [5]. The virtualized resources are elastic in nature so that their amount can be dynamically adjusted. Unlike the conventional networks in which network nodes (e.g., routers) contain only limited resources to perform predefined packet forwarding functions while the end nodes (e.g., servers) contain plenty of computation and storage resources, the virtualized network slices can have plenty of computation and storage resources in network nodes too. These virtualized network nodes host functions such as directory service, caching, media transcoding, traffic engineering and in-network data processing, besides usual data forwarding functions. New nodes can be added or their resources can be increased dynamically as demand for the scaling of network functions.

Infrastructure providers own physical substrate networks consisting of the edge network, core network and data centers, and possess a huge amount of networking (i.e., link bandwidths and buffer size) and computing (i.e., CPU, memory and storage) resources. Edge networks are composed of equipment for collecting, processing, and transmitting data to/from various terminals such as PCs, mobile/smart phones, vehicles, robots, sensors, and other IoT devices. The substrate network is equipped with NFV and SDN capabilities so that it can be sliced and allocated to virtual network operators.

An application service provider is the entity that offers application services (e.g., automated driving and smart metering) to customers by using a virtual network slices operated and managed by a VNO. For this purpose, it provides service requirements (e.g., number and types of devices to be connected, application type, and reliability) to the VNO.

The VNO analyses the application's QoS requirements and determines about the supporting network capabilities, functions and protocols. It translates the application's QoS

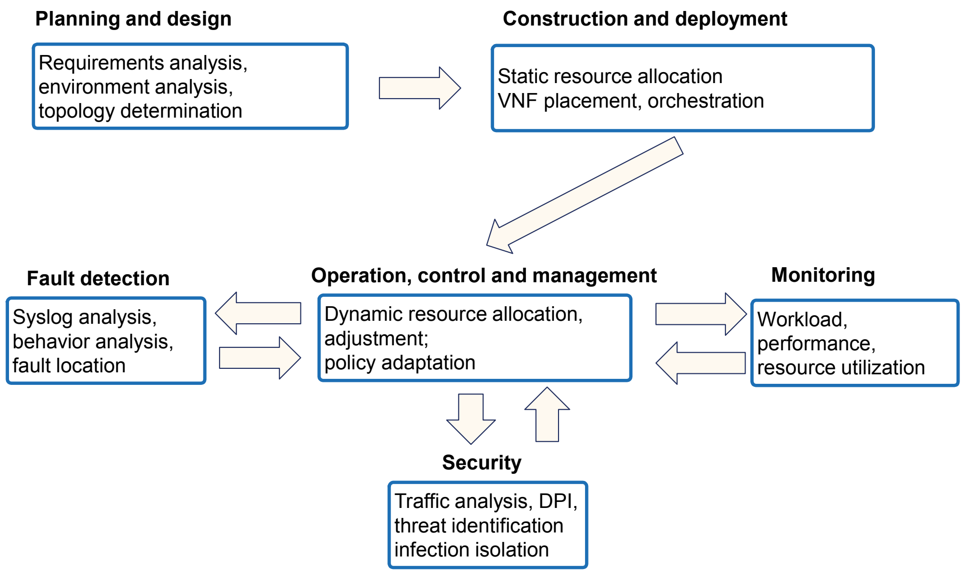


Figure 2. Functions for network automation.

requirements in terms of network performance metrics such as network latency, packet loss rate, and bandwidth. These requirements are mapped into a virtual topology containing the required amount of computing and networking resources. The VNO then sends a network resource request containing the logical topology and required performance metrics to the infrastructure provider to lease the required amount of virtualized resources.

Infrastructure provider performs mapping of the logical network topology onto the virtualized resources of substrate networks. This mapping process is also referred to as virtual network embedding. Infrastructure provider allocates the requested amount of virtualized resources and provides the corresponding resource control and management interfaces to VNO.

VNO installs necessary network functions, protocols, customer registry and software platform on the leased virtualized resources. It then deploys the virtual network for the application service and regularly monitors the performance to check if currently allocated resources are in appropriate amounts to execute the necessary network functions to process the given workload. If it determines that resources need to be adjusted, it sends resource adjustment requests containing the amounts of required resources to infrastructure provider. Alternatively, infrastructure provider may regularly monitor the utilization of virtualized resources and adjusts the resource amount according to the service level agreement made with VNOs. To monitor and adjust resources, infrastructure provider uses network and node virtualization tools such as OpenFlow and OpenStack. Open Networking Lab (onlab.us) to develop open and innovative technology called Open Network Operating System (ONOS) on top of commodity hardware.

Thanks to the technologies of NFV and SDN, each type of IoT service can be deployed in a distinct network slice configured with the appropriate amount of resources leased from the substrate networks of one or several infrastructure providers. For example, autonomous cars, social networking services and sensors/actuators of environment and weather monitoring services in Fig. 1 are connected to three different network slices. These slices are independently configured, deployed, and operated either by the same or different virtual network operators.

Since most steps involved in construction of a telecommunication network currently require manual operations, it takes about two weeks in most cases to complete the construction and start serving customers [6]. Similar amount of time would be required to construct a network slice if the operations are carried out manually. Therefore, automation technologies for the construction, deployment, operation, monitoring, and control are essential to shorten the time for on-demand construction of a network slice and enable faster roll out of new IoT services. Automation technologies would also help in dealing with the shortage of skilled manpower or avoiding human errors in the tedious manual operations. The autonomous functions carry out resource abstraction, allocation, arbitration, adjustment, and adaptation. These functions enable network slices to adapt to dynamic network environments (i.e., changing workload, customer base, and link quality). AI and machine learning based methods play a key role for enabling the automation of network control and management.

3. NETWORK AUTOMATION FUNCTIONS

In this section, we describe network functions that need to be automated by using machine learning techniques. These functions are shown in Fig. 2 and described below.

3.1 Planning and design

Planning and design of end-to-end network slices with the objective of satisfying diverse and distinct service requirements, for example ultra-low latency for *URLLC* and very high and stable throughput for *eMBB* services, requires processing lots of information coming from the items listed below.

- User requirements
- Service requirements
- Operation environment (e.g., energy consumption)
- Business goals

3.2 Construction and deployment

After the planning and design, the network slice construction and deployment phase comes into effect. In this phase, the VNO determines the optimal network topology and amount of computing and networking resources for each node and link so that the given service requirements are perfectly met. The VNO sends request to the infrastructure provider to obtain the necessary amount of resources.

In the deployment phase, the VNO places virtual network functions (VNF) on appropriate nodes that have sufficient resources required by the functions. This process is also called service function chaining (SFC), which is orchestrated from a centralized controller.

3.3 Operation and management

Operation and management is the most human resource demanding task in the networking business. Automation of operation, control and management helps in cutting down the cost significantly. The monitoring, fault detection and security functions provide input information required by the operation, control and management tasks. The following functions are performed for the operation and management of network slices.

- Dynamic resource allocation: The elastic virtualized computing and network resources (e.g., optical wavelength and radio frequency/time slots) are allocated on demand based on the number of active users or service demand.
- Resource adjustment: The elastic resources are adjusted dynamically on the basis of the values of their current utilization and corresponding impact in the network performance.
- Policy adaptation: The policies for the allocation or arbitration of limited resource between different types of network slices are dynamically adopted on the basis of the severity of performance degradation or impact in business in case of insufficient resource allocation. For example, if limited resources are shared between emergency services and entertainment services, the resource arbitration is executed with higher priority given to the emergency services when their demand increases.
- Mobility: 5G network is introducing more flexible multiple-tier mobility management states that can be tailored to the nature of devices and services demanded by vertical industries. For example, some immobile user equipment, such as *mMTC* sensor devices, are not frequently probed by the network for their stringent energy efficiency and allowed to update location only when they enter a specific region.

3.4 Monitoring

Monitoring is integral part of operation and management. It performs the following tasks.

- Acquisition of system logs and performance metrics
- Analysis of workload (traffic) by using performance models and metrics
- Classification of resource utilization status (e.g., high, moderate, and low)

3.5 Fault detection

Fault detection is also an integral part of operation and management runs continuously in the system to carry out the following tasks:

- Analysis of syslog, classification into normal and faulty stage
- Detection of usual/unusual behavior of users and traffic
- Localization of fault
- Measures for recovery

3.6 Security

Security is a very important issue in operation and management. The security system performs the following tasks:

- Traffic analysis, deep packet inspection
- Identification of security threats
- Isolation of the infected component

To realize the automation of above functions, there are challenges of ever-increasingly complicated configuration of network slices on-demand and the service provisioning through the interaction within the network system itself and with outside operating environment. The volume of performance measurement data produced by such complex networks would be too large and complex to process manually by human operators.

4. MACHINE LEARNING IN NETWORKS

Machine learning techniques are helpful for addressing the challenges of achieving automation in the network setup, control and management. They provide useful analytics to extract valuable information from raw data and generate insightful advices and predictions. Machine learning enables machines to improve performance, make decision with reasoning, creating and exploiting knowledge. It makes predictions and provides suggestions on the basis of the results obtained by processing the data sets that are too

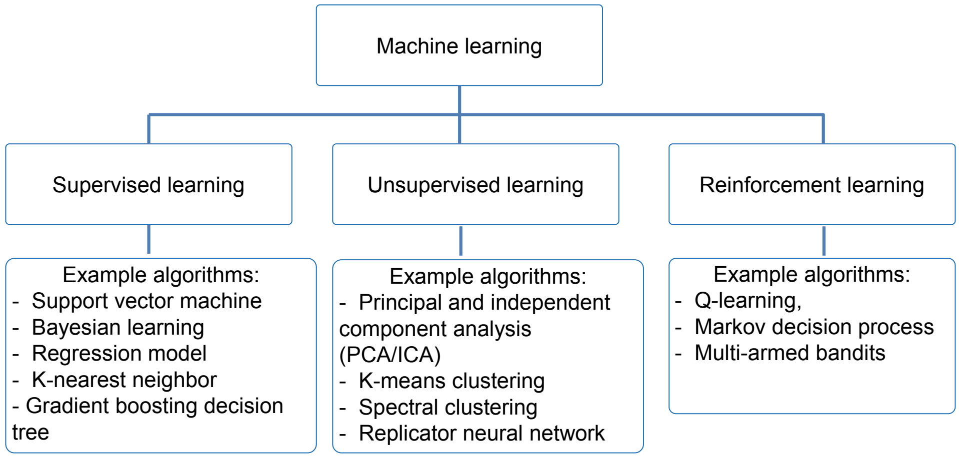


Figure 3. Classification of machine learning techniques.

large and too complex [4,9]. Thus, the autonomic adaptation of network functions through the interaction with the internal and external environments can be carried out by machine learning techniques.

In this section, we first provide an overview the machine learning techniques and then list the relevant techniques that can be used for the automation of 5G network slicing functions. As shown in Fig. 3, machine learning techniques can be broadly classified into three categories: supervised learning, unsupervised learning, and reinforcement learning [10].

The supervised learning techniques learn (or deduce) a function from training data, which comprise of pairs of input and desired outputs. The output of the function can be continuous values (called regression) or a class label of the input values (called classification). After training, the learning agent or element predicts the value of function for any valid input from unseen situations in a reasonably valid way. Thus, supervised learning principle can be expressed as follows: Given a training set of N examples $\{x_i, y_i = f(x_i)\}$, where each y_i was generated by unknown function f, discover a function h (hypothesis) such that it approximates the true function f (i.e., $h \approx f$). Support vector machine (SVM), Bayesian learning, and regression models are the popular supervised learning techniques applicable for solving network problems.

Unsupervised learning is based on unstructured or unlabeled data. The learning agent learns patterns in input data even though no explicit feedback is provided. Unsupervised learning techniques are used for data clustering, dimensionality reduction, density estimation, etc.. K-means clustering, principal component analysis (PCA), and independent component analysis (ICA) are often used algorithms for clustering and dimensionality reduction of system data collected for network control and management.

Reinforcement learning performs iterative learning through a series of reinforcements by rewards or punishments. It learns to achieve its goal from its own experience. Unlike supervised learning, reinforcement learning does not require provisioning of correct input/output data pairs and explicit correction of sub-optimal actions. As shown in Fig. 4, the reinforcement learning agent receives percepts containing the state of environment (or system) through its sensors and performs actions through its actuators in such a way that it maximizes the cumulative rewards. The agent interacts with its environment in discrete time steps. At each time t, the agent receives a percept p_t, which includes the reward r_t. It then chooses an action a_t from the set of available actions and sends to the environment. The environment moves to a new state s_{t+1} and reward r_{t+1} associated with the transition $(s_{t+1}|s_t,a_t)$ is determined. The goal of a reinforcement learning agent is to collect as much reward as possible. There are two factors that characterize reinforcement learning techniques: transition model from s to s' with action a, i.e., probability $P(s'|s,a) = Pr(s_t{+}1{=}s'|s_t{=}s, a_t{=}a)$, and policy for applying an action in a given state. The transition model is known (e.g., in Markov decision process) or unknown (in Q-learning). The goal of Q-learning is to learn a policy and maximize its total (future) reward. It does this by adding the maximum reward attainable from the future states to the reward in its current state, thus effectively influencing the current action by the potential reward in the future. This reward is a weighted

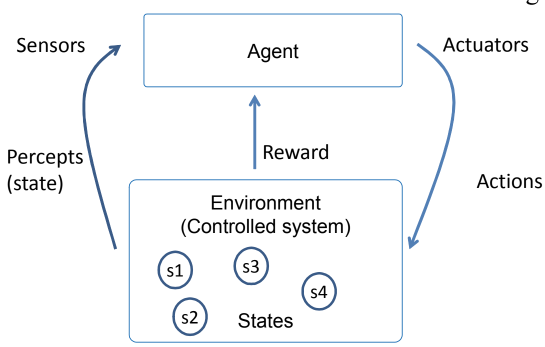


Figure 4. Reinforcement learning components.

Network functions	Machine learning techniques	Purposes
Planning and design	Support vector machine Gradient boosting decision tree Spectral clustering Reinforcement learning	- Classification of service requirements - Forecasting trend, user behavior - Configuration of parameters
Operation and management	K-mean clustering Deep neural network Reinforcement learning	- Clustering cells, users, devices - Routing, forwarding, traffic control - Decision making for dynamic resource control, policy formulation - Reconfiguration of parameters
Monitoring	Spectral clustering K-mean clustering Support vector machine Deep neural network	- Clustering of syslog data - Classification of operation modes - Forecasting resource utilization trend
Fault detection	Principal component analysis Independent component analysis Logistic regression Bayesian networks	- Classification of operation data - Detection of network anomaly - Predicting unusual behavior
Security	Deep neural network Principal component analysis	- Clustering users and devices - Detecting malicious behavior - Intrusion detection

Table 1. Network functions and relevant machine learning techniques.

sum of the expected values of the rewards of all future steps.

In between supervised and unsupervised learning, there is semi-supervised learning, which is given a few labeled example data but can perform on a large collection of unlabeled data. Deep learning, which is based on artificial neural network, belongs to a broader family of machine learning methods. Its learning can be supervised, semi-supervised or unsupervised. Unlike the other machine learning techniques that require highly tuned and many rules to solve specific problems, deep learning techniques can successfully deal with huge volumes of data to learn and recognize abstract patterns by using vast, virtual neural networks [12].

Machine learning techniques are being considered useful for various functions of network services; mainly, planning and design, operation, control and management, monitoring, fault detection, and security. They enable machine to recognize patterns and anomalies that human may not notice or take unacceptably long time. Table 1 shows the list of relevant machine learning techniques for the automation of these networking functions.

Planning and design involve decision making based on the information provided about service requirements and expected user behavior. The design process can exploit machine learning techniques for data acquisition (extracting relevant data), processing data for knowledge discovery, and using the knowledge for reasoning and decision making [11]. Supervised learning techniques, such as support vector machine and gradient boosting decision tree, and unsupervised learning, such as spectral clustering, can be used for classifying a new service in one of *eMBB*, *eMTC*, and *URLLC* categories on the basis of requirements in terms of bandwidth, latency, bit-error rate, etc. Similarly, reinforcement learning can be applied for reasoning to determine the appropriate values of parameters for the optimal network setup. It would help in designing network slices that would be suitable for continuously evolving new services and use cases by provisioning optimal amount of resources.

Operation and management involve tasks for efficient use of resources while optimally satisfying the service and user requirements all the time. They require understanding the variations in system states, learn uncertainties, (re)configure the network, forecast immediate challenges, and suggest appropriate solutions timely. The resource allocation and management take into account node computation capacity, link bandwidth, radio spectrum, and energy currently available and in use. They require clustering of cells (for frequency allocation and power management), users and devices for intelligent mobility management or establishing device to device (D2D) networks for optimal management of available spectrum and energy in mobile devices. Unsupervised learning techniques such as K-mean clustering are suitable for the clustering. Similarly, deep learning has been shown to be effective in control of heterogeneous network traffic [12] to achieve high throughput of packet processing. Reinforcement learning is applicable in decision-making for the reconfiguration of network parameters and dynamic adjustment of resources such as channel selection. Smart reconfiguration of parameters for faster adaptation of service is very important for 5G because the number of configurable parameters in 5G would be fairly large, 2000 or more [3]. Bandwidth control for *eMBB* and latency control for *URLLC* services can be performed with reinforcement learning and deep learning. Reinforcement learning, especially multi-armed bandit, can be used to model a resource arbitration problem in which a fixed limited amount of resources have to be proportionally allocated to competitive services whose properties are only partially known at the time of resource allocation [9].

Monitoring, fault detection and security involve functions for sensing the system, collecting huge amounts of syslog and performance data, classification and clustering of data for contextualization, forecasting usual/unusual user behavior and network resource utilization trend. For these purposes, unsupervised learning techniques such as spectral clustering, K-mean clustering, and principal component analysis, supervised learning techniques such as support vector machine and logistic regression, as well as deep learning and reinforcement learning are applicable.

For the detection of network anomaly, principal and independent component analysis techniques can be used because they can easily identify statistically unusual behavior from the system operation data. Similarly, traffic analysis by various unsupervised learning techniques can help in the detection of intrusion and spoofing attacks. Logistic regression of supervised learning can be used to predict unusual behavior of devices or users based on their traffic characteristics. Deep learning would help in detecting unprecedented security issues that may come up with new types of services.

Although in Table 1 and above discussion we have mentioned only the classical methods of machine learning, they can be modified for improving accuracy, reducing complexity or their trade-off, when applying to network slicing functions. Many variations of their extensions are available in literature. However, their applicability in network slicing is yet to be studied.

5. AI AND MACHINE LEARNING IN SDOs AND FORUMS

In several standards development organizations (SDO) and industrial forums, AI and machine learning techniques are being investigated for enabling systems to make autonomic decision by processing large amounts of data, learning from own operations, and adapting to changing environment. Although both AI and machine learning are often used interchangeably, they are subtly different. AI comprises multi-disciplinary techniques such as machine learning, optimization theory, game theory, control theory, and meta-heuristic analytics [7]. Thus, machine learning can be considered as a form of or subfield of AI that enables machines to learn by themselves by providing them access to large amounts of data. In this section, we provide an overview of AI and machine learning related technological discussion being carried out in ITU, ETSI, ISO/IEC, and TM Forum.

5.1 ITU FG-ML5G

The ITU Focus Group on Machine Learning for Future Networks including 5G (FG-ML5G) [13] has been established in November 2017 to study network architectures, protocols, interfaces, use cases, algorithm and data formats for the adoption of machine learning methods in 5G and future networks. It is an open platform for experts from ITU members and non-members to quickly progress studies on machine learning methods for networks. In its lifetime of one year (which can be extended if necessary), FG-ML5G is mandated to hold meetings several times to review the contributions received from participants and develop deliverables. It has formed three working groups to progress work simultaneously on (1) use cases, services and requirements; (2) data format and techniques; and (3) machine learning aware network architecture. FG-ML5G has not produced any publicly available document yet. Its deliverables will be handled over to ITU-T Study Group 13 for further study and development of formal standards (called ITU-T Recommendations) on the basis of these deliverables.

5.2 ETSI ISG ENI

ETSI has created the Industrial Specification Groups (ISG) “Experiential Network Intelligence” (ENI) in February 2017 with the purpose of defining a cognitive network management architecture based on the “observe-orient-decide-act” control model [14]. It uses AI techniques and context-aware policies for dynamically adjusting network services in response to changing user demands, network conditions and business goals. It envisions making the system capable of learning from its own operations and instruction given by human operators (thus called experiential). It would be instrumental in the automation of network configuration and monitoring processes, thus reducing the operational cost, human errors, and time to market the service. ISG ENI aims at studying various AI methods for enabling model-driven architecture for adaptive and intelligent service operations. The architecture accommodates different types of policies and selects the best-fitted one to adaptively drive the network system according to the changes in user behavior, service requirements, network conditions, and business goals. ISG ENI is open for participants from all ETSI member as well as non-member organizations that sign ISG Agreements. ISG ENI has already released five specifications (as of June 2018) on use case, requirements, context-aware policy management, terminology and proof-of-concept (PoC) framework. These deliverables can be accessed freely from its website [14].

Closely related another ISG is Zero-touch network and Service Management (ISG ZSM), which focuses on developing standards for automation of network operation control and management functions.

5.3 ISO/IEC JTC 1/SC42

ISO/IEC JTC 1/SC42 Artificial Intelligence [15] has been created in October 2017 to serve as the focus and proponent for ISO/IEC JTC 1's standardization program on artificial intelligence, and guide JTC 1, IEC, and ISO committees for the development of AI applications. It has been developing several ISO standards on big data and AI, such as big data reference architecture, AI concepts and terminology, and framework for AI systems using machine learning. It has not yet started developing documents on the application of AI or machine learning techniques on networks.

5.4 TM Forum Smart BPM

TM Forum's Catalyst Project on Smart BPM (Business Process Management) is investigating the applicability of AI-based decision modeling in telecom business processes such as resource provisioning, fault management, QoS assurance, and customer management [16]. AI support makes the workflow system capable of reacting to exceptional conditions in the network service lifecycle orchestration that includes planning, delivery, deployment, and operation functionalities. In their approach, the AI support system works as a secretary to recommend appropriate actions for handling exceptions. They mainly consider using Multi-label Deep Neural Network in AI support system, which takes input data from the orchestrator, alarm management system, and other network functions. TM Forum has demonstrated the concept model for the interaction between AI and human for network fault detection and recovery on the basis of training data including operator's feedback.

6. CONCLUSION

In this paper, we presented the 5G network slicing scenarios and list of tasks for the automation of slicing functions. We then discussed some machine learning techniques that support for the automation of network functions. We also gave the overview of AI and machine learning related activities being carried out in various standards development organizations and industrial forums.

In future work, we extend this work by detail investigation of a few representative machine learning techniques for making autonomic decision to allocate and adjust the computing and network resources of network slices on the basis of service requirements and time-varying network workloads. We will also bring this research outcome gradually to ITU and other SDOs for standardization.

REFERENCES

[1] Recommendation ITU-R M.2083-0 (2015) "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond".

[2] Recommendation ITU-T Y.3102 (2018) "Framework of IMT-2020 network".

[3] R. Li et al., "Intelligent 5G: When cellular networks meet artificial intelligence," IEEE Communications Magazine, Vol. 24, No. 5, pp. 175-183, Mar. 2017.

[4] M.G. Kibria et al., "Big data analytics, machine learning and artificial intelligence in next-generation wireless networks," IEEE Access (Early Access), May 2018.

[5] T. Miyazawa, M. Jibiki, V.P. Kafle, and H. Harai, "Autonomic resource arbitration and service-continuable network function migration along service function chains," IEEE/IFIP Network Operations and Management Symposium (NOMS2018), Apr. 2018.

[6] K. Katsuura, M. Miyauchi, T. Numazaki, Y. Kurogouchi, Y. Satoh, and T. Koseki, "IaaS Automated operations management solutions that improve virtual environment efficiency," NEC Technical Journal, vol.8, no.2, Apr. 2014, pp. 29-32.

[7] J. Qadir et al., "Artificial intelligence enabled networking," IEEE Access, vol. 3, 2015, pp. 3079-3082.

[8] X. Wang, X. Li, and V.C.M. Leung, "Artificial intelligence based techniques for emerging heterogeneous network: State of the arts, opportunities and challenges," IEEE Access, vol. 3, 2015, pp. 1379-91.

[9] C. Jiang et al., "Machine learning paradigms for next-generation wireless networks," IEEE Wireless Commun., vol. 24, no. 2, Apr. 2017, pp. 98-105.

[10] E. Alpaydm, Introduction to Machine Learning, Third Edition, MIT Press, 2014.

[11] T.E. Bogale, X. Wang, and L. Le, "Machine intelligence techniques for next-generation context-aware wireless networks," ITU Journal: ICT Discoveries, Special Issue No. 1, Feb. 2018.

[12] N. Kato et al., "The deep learning vision for heterogeneous network traffic control: proposal, challenges and future perspective," IEEE Wireless Communications, vol. 24, no. 3, June 2017, pp. 146-153,

[13] Focus Group on Machine Learning for Future Networks including 5G, https://www.itu.int/en/ITU-T/focusgroups/ml5g/Pages/default.aspx, Visited 22 June 2018.

[14] ETSI ISG Experiential Network Intelligence (ENI), http://www.etsi.org/technologies-clusters/technologies/experiential-networked-intelligence, Visited 22 June 2018.

[15] ISO/IEC JTC 1/SC42 Artificial Intelligence, https://www.iso.org/committee/6794475.html, Visited 22 June 2018.

[16] TM Forum Catalyst Project: Artificial Intelligence makes Smart BPM Smarter, https://www.tmforum.org/catalysts/smart-bpm, Visited 22 June 2018.

SESSION 4

OPTIMIZATION OF DATA MANAGEMENT WITH MACHINE LEARNING

A DEEP REINFORCEMENT LEARNING APPROACH FOR DATA MIGRATION IN MULTI-ACCESS EDGE COMPUTING

Fabrizio De Vita[1]; Dario Bruneo[1]; Antonio Puliafito[1]; Giovanni Nardini[2]; Antonio Virdis[2]; Giovanni Stea[2]

[1]University of Messina, Department of Engineering
{fdevita, dbruneo, apuliafito}@unime.it
[2]University of Pisa, Department of Information Engineering
{g.nardini}@ing.unipi.it, {antonio.virdis, giovanni.stea}@unipi.it

ABSTRACT

5G technology promises to improve the network performance by allowing users to seamlessly access distributed services in a powerful way. In this perspective, Multi-access Edge Computing (MEC) is a relevant paradigm that push data and computational resources nearby users with the final goal to reduce latencies and improve resource utilization. Such a scenario requires strong policies in order to react to the dynamics of the environment also taking into account multiple parameter settings. In this paper, we propose a deep reinforcement learning approach that is able to manage data migration in MEC scenarios by learning during the system evolution. We set up a simulation environment based on the OMNeT++/SimuLTE simulator integrated with the Keras machine learning framework. Preliminary results showing the feasibility of the proposed approach are discussed.

Keywords - Multi-access Edge Computing, 5G, LTE, Deep Reinforcement Learning, Data Migration, SimuLTE

1. INTRODUCTION

Smart services represent the core element in a smart city environment; thanks to IoT diffusion together with the advancement of technology in terms of computation, nowadays users can access a large number of applications that usually communicate with the Cloud which provides support to them [1]. However, applications are becoming more and more resource demanding and they have reached a level where the cloud paradigm can no more guarantee low latencies especially when the distance between it and the user device is very large. In such a context, Multi-access Edge Computing (MEC) can address this problems by moving data and computational resources nearby the user [2]. 5G technology has the ambition to realize a framework where different technologies can cooperate to improve the overall performance, also leveraging context-related information and real-time awareness of state of the local network (e.g., congestion, types of services enabled). MEC is regarded as a key enabler for the 5G key performance indicators, such as low latency and bandwidth efficiency. In a 5G system, MEC is expected to interact with the rest of the network to improve traffic routing and policy control. The adoption of the MEC paradigm in the new 5G-enabled systems is a hot research topic with different solutions already presented in the literature. In this paper, we will focus on the data migration problem taking as reference a MEC system composed of a LTE network with some MEC servers attached to the eNodeb (eNB) base stations. Our intent, is to build a self-adaptive AI-powered algorithm capable to understand the system status and accordingly migrate users applications data with the final goal to improve the user Quality of Service (QoS). Thanks to machine learning capability to build complex mathematical models which allow a system to learn intricate relationships among a large number of parameters, we believe that such a technique could be an enabling technology for the future 5G systems where context aware network infrastructures must be able to make decisions in an autonomous way in order to improve their performance. In the literature, we found some papers that face this problem with different approaches. The authors in [3] adopts a traditional machine learning approach using LibSVM toolkit to have a forecast on users mobility and implement a proactive migration mechanism in order to minimize the downtime of the system. However, as the author remark, this kind of technique is more resource demanding if compared with discrete models like Markov Decision Processes (MDP). The approach described in [4], uses a multi-agent reinforcement learning scheme where agents compete among themselves in order to establish the best offload policy. In this paper, we present a deep reinforcement learning approach to deploy an optimal migration policy in order to improve user QoS. The main difference between our work and the others consist in the use of a deep learning technique instead of traditional machine learning algorithms or formalisms like MDPs. We believe that the use of deep learning can be a valid solution in order to build a system which is capable to adapt to changes by understanding the network state and performing actions autonomously. The paper contribution is twofold: we designed a deep RL algorithm that can be used as a general purpose and self-adaptable algorithm to manage complex MEC systems without needing an explicit knowledge of all the involved aspects; we realized a Deep RL environment by integrating SimuLTE and Keras that can be used as a *gym* where different RL approaches can be realized and tested in LTE/5G scenarios.

The paper is organized as follows. Section 2 introduces the 5G and MEC technologies focusing also on the main challenges which is necessary to address in this context. Section 3 contains the problem formulation and the details about the algorithm we designed to train the proposed deep RL agent. Section 4 provides a description of the simulation environment that we used to retrieve the data necessary for the system training. Section 5 describes the scenario we realized and provides the results we obtained by comparing the policy learned by the agent with respect to a simple policy. Finally Section 6 concludes the paper and gives some details about future developments.

2. MULTI-ACCESS EDGE COMPUTING

Multi-access Edge Computing (MEC) is recently being standardized by the European Telecommunications Standards Institute (ETSI) [5]. It consists in placing nodes with computation capabilities, namely the MEC servers, close to the elements of the network edge like, e.g., base stations in a cellular environment. MEC differs from Fog Computing since it is able to interact with the network elements and can gather information on the network environment, such as resource utilization and users' location. This information can be obtained via a standard Application Programming Interface (API) and allows operators and/or third-party developers to offer new context-aware services and applications to the users. The latter can also experience lower latency and larger bandwidth with respect to a cloud-based application. Those services are created within a virtualized environment that allows to optimize the computational load of MEC servers and/or users' requirements. Moreover, MEC applications can also migrate between MEC servers to better accommodate mobile users, e.g. cellular users moving moving to another cell. Connected vehicles, video acceleration and augmented reality are some of the use cases identified by ETSI that can benefit from the introduction of MEC [6]. LTE is the cellular technology for which MEC was first proposed, and will be part (in its current state, or – more likely – leveraging an evolved physical and MAC layers) of the 5G ecosystem. In an LTE radio access network (see Fig. 1), eNBs create radio cells, to which User Equipments (UEs) attach. The entry/exit point for traffic in an LTE Evolved Packet System (EPS) network is the Packet Data Network Gateway (PGW). Traffic destined to the UE arrives at the PGW, where it is tunneled using the GPRS Tunneling Protocol (GTP). Tunneled traffic traverses the EPS network. The exit point of the GTP tunnel is on the serving eNB. At the eNB, the packet is extracted from the tunnel and transmitted over the air interface. A handover procedure is initiated by a UE to leave a cell and join another, typically when the signal strength of the new eNB exceeds the current one's. In this case, downstream traffic is steered from the PGW towards the new eNB, and the traffic still in transit at the handover may either be discarded or forwarded by the "old" eNB using the X2 interface, which connects eNBs in a peer-to-peer fashion. MEC servers can be deployed at any point in the EPS. However, it is foreseen that they will be either co-located with eNBs, in order to minimize the latency, or deployed close to them, so that a single MEC server will serve a geographic region area covering a limited number of contiguous cells. In these cases, functions are required to maintain service continuity and QoS for UEs using MEC services while in mobility. In fact, it may well happen that a UE moves too far away from its MEC server, in which case the communication latency increases beyond reasonable and context awareness becomes less effective. In such a scenario, it is preferable to move the server-side MEC application to a nearer MEC server. Besides providing functions to achieve this, policies are also required in order to understand when it is best to migrate a MEC application, and where to. These policies may take into account physical constraints (e.g., the availability of MEC services on particular servers), network-side QoS parameters (such as latency and communication bandwidth in the cell), server-side QoS parameters (such as available computation power and storage).

3. RL TECHNIQUES FOR MEC

During the last years, mobile traffic data is increasing and it is expected to raise in the next future. Such a trend, has lead to the start of a process which aims to improve the network infrastructure in order to address all the problems related to a such massive amount of data [7]. 5G system is expected to reach far better performance in terms of speed and energy efficiency if compared with the actual Long Term Evolution (LTE) and 3G technologies; 5G architecture takes advantage of Software Defined Networks (SDN) and Network Function Virtualization (NFV) in order to improve network management and dynamic resource allocation [8]. In such a context, where the network infrastructure is starting to become very complex, machine learning can be an useful technique to use in order to face the environment dynamics by finding an optimal strategy to improve the overall system performance.

3.1 Reference Scenario

The proposed reference scenario consists of a MEC-enabled LTE network where eNBs can be directly connected to MEC servers which contain application data, as depicted in Fig. 1. Such servers can be used as local repositories by serving those users attached to the corresponding eNB thus reducing the network latency as well as the amount of data traveling on the core network. One of the key issues of this schema is to find an optimal migration schema that opportunely moves data from one server to another in order to improve a specific objective function.

In particular, in this paper we are interested in the development of a machine learning algorithm based on reinforcement learning (RL) for the deployment of an optimal policy which establishes when is necessary to migrate data to another eNB depending on the user position and on the current state of the network in order to improve the user QoS. RL is a machine learning technique used to observe the dynamics of an environment thus learning an optimal policy with respect to one or more performance indexes. In many contexts where it is impossible to work with labeled data, RL is the only feasible solution to correctly train a system. In fact,

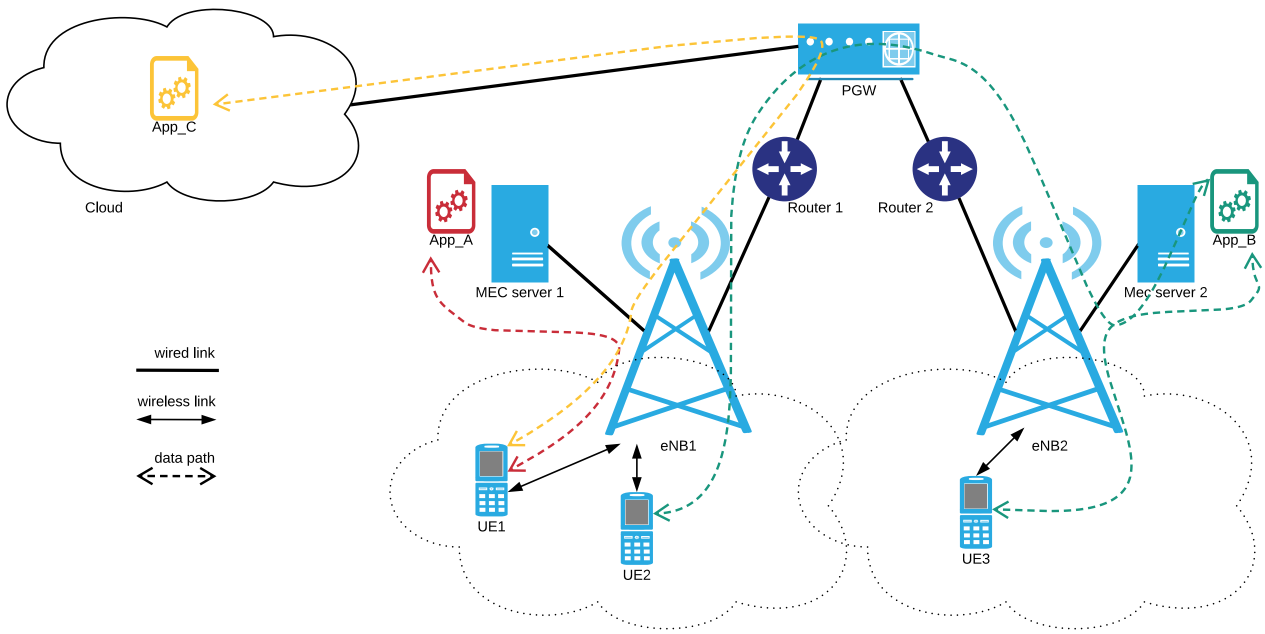


Figure 1 – The MEC-enabled LTE scenario.

its ability to learn through a trial and error process, which is very similar to the human being learning one, makes it the best choice to solve decision making problems. RL adopts, as a basic model, the MDP formalism which is a framework for modeling the decision making in stochastic environments. From a mathematical point of view, an MDP is defined as follows:

- set of states $\mathcal{S}$ that the environment can assume;
- set of actions $\mathcal{A}$ that the agent can perform;
- probability transition matrix P;
- reward function $R(s)$ $S :\rightarrow \mathbb{R}$
- discount factor $\gamma \in [0,1]$ which defines the importance we are giving to future rewards

In such a context, we define the figure of the RL agent whose objective is to find an optimal policy in order to maximize the reward function in each state of the environment. Using the MDP definition, the agent is able to run across the environment states several times and change the system policy to improve the reward accordingly. *Bellman equation* expresses the relationship between the utility of a state and its neighbors [9]:

$$U(s) = R(s) + \gamma \cdot max_{a\in\mathcal{A}} \sum_{s'} P(s'|s,a)U(s') \qquad (1)$$

where $U(s)$ is the immediate reward obtained in the state s assuming that the agent will choose the optimal action.
When the probability transition matrix is not known, a typical RL approach is the Q-learning [9], a *model free* technique which tries to learn the relationship between the execution of an action on a given state and the associated reward or utility through the concept of Q-value $Q(s,a)$ which returns the value of doing action a when the agent is in the state s:

$$Q(s,a) = Q(s,a) + \alpha(R(s + \gamma max_{a'}(Q(s',a') - Q(s,a)) \quad (2)$$

$$U(s) = max_a(Q(s,a)) \qquad (3)$$

where α is the learning rate and γ is the discount factor.
When the environment has a large number of states, it is impossible to use traditional Q-learning. In fact, the time to converge increases as the state space becomes larger, so if we consider a scenario with a huge number of states (e.g. 10^{20} or even more), it is impossible to think that the agent should visit all of them multiple times to learn a good policy [9]. One way to address this kind of problem is the quantization which consists in the process of grouping a set of states into a single one thus reducing the number of states which describe an environment. However, such a technique is not helpful especially in those cases where the state space reduction would result in a too large quantization error that could lead the agent to learn a wrong policy.
A very interesting alternative is provided by the use of a Deep Neural Network (DNN) to create a function approximator capable to predict the Q-values for a given state without explicitly using eqs. ((2))-((3)) and the corresponding MDP. Deep Reinforcement Learning is a technique which has been pioneered by DeepMind [10]. The idea comes from the necessity to find a new way to represent complex environments, where the dimension of the state space and action space is very large making impossible to solve them by using traditional approaches. The key idea at the base of the deep reinforcement learning consists in the use of two separated DNNs parameterized with θ and $\widehat{\theta}$ respectively: the *Main* DNN used to predict the Q values associated to a generic state and the *Target* DNN used to generate the target

Q values in the update rule which can be expressed as follows:

$$y_{j,a} = r_j + \gamma \max(\widehat{Q}(s_{j+1}, \widehat{\theta})) \tag{4}$$

where $y_{j,a}$ is the Q-value associated to the state j when the agent performs the action a,r_j is the reward associated to the state s_j, and $\widehat{Q}(s_{j+1}, \widehat{\theta})$ is the output layer of target DNN network which contains the Q-values estimation for the state s_{j+1}. By using two networks instead of just one, the obtained result is a more stable training which is not affected by learning loops due to the self-update network targets that sometimes can lead to oscillations or policy divergence.

3.2 Problem Formulation

In order to properly design a deep RL algorithm, it is first of all necessary to define the environment in which the RL agent will operate. In this subsection, we will formalize the MEC scenario we are interested in.

We start defining as $\mathcal{N}$ the number of eNBs present in the MEC-enabled LTE network. For the sake of simplicity and without loss of generality, let us assume that to each eNB is attached one and only one MEC server. Then, let us define the set, with cardinality $\mathcal{N} \in \mathbb{N}$, of the MEC servers attached to the eNBs as:

$$MEC = [MEC_1, MEC_2, MEC_3, ..., MEC_{\mathcal{N}}] \tag{5}$$

Users are free to move around the MEC environment and attach to different eNBs through seamless handover procedures. Moreover, they run several applications whose data is contained in the Cloud or inside one of the MEC servers. Regarding the applications that users can run and the number of devices attached to the eNBs, we can define the following sets:

$$Apps = [app_1, app2, app_3, ..., app_{\mathcal{M}}] \tag{6}$$

$$Devices = [UE_1, UE_2, UE_3, ..., UE_{\mathcal{K}}] \tag{7}$$

with $\mathcal{M}, \mathcal{K} \in \mathbb{N}$. With respect to the actions that the agent can perform in the environment, let us define the set of actions with cardinality $\mathcal{Z} \in \mathbb{N}$ as:

$$Actions = [a_1, a_2, a_3, ..., a_{\mathcal{Z}}] \tag{8}$$

where each element represents an app migration from the Cloud towards one of the servers defined in the MEC set, from one MEC server to the Cloud, or among MEC servers. Another important element that we have to introduce is the concept of *state* which is made of a t-uple containing all the information related to the users position and the app distribution over the network which is defined as follows:

$$s = <(s_1, s_2, s_3, ..., s_{\mathcal{T}})> \tag{9}$$

Finally, with respect to the reward, we define it as a number $r \in \mathbb{R}$ that is computed as a combination of several network performance indexes.

Algorithm 1: *Deep RL*

initialize experience replay memory E to {}
random initialize main DNN network weights θ
set target DNN network weights $\widehat{\theta}$ equal to θ
set discount factor γ
set batch size
set update step U
set waiting time t
set exploration rate ϵ
set decay rate d
for episode = 1 to *end*:
  observe current state s_j
  p = *random([0,1])*
  if $\epsilon > p$:
    action = *random([1,$\mathcal{Z}$])*
  else:
    action = *argmax*(Q(s_j,θ))
  end if
  execute the action
  wait(x seconds)
  observe the new state s_{j+1}
  observe the reward r
  store the t-uple (s_j,$action$,s_{j+1},r) in E
  sample a *batch* from E
  y = Q(s_j,θ)
  $y_{target} = \widehat{Q}(s_{j+1},\widehat{\theta})$
  y_{action} = r + $\gamma \cdot max(y_{target})$
  execute one training step on main DNN network
  every U steps set $\widehat{\theta} = \theta$
end for

3.3 Proposed Algorithm

In this paragraph, we describe the proposed deep RL approach shown in Algorithm 1. Line 1 is dedicated to the set up of the replay memory E which is a data structure containing the experiences made by the agent. It plays a very important role since it stores all the data necessary for the DNN training. At the beginning, the two neural network weights are set to the same values (lines 2-3), then other parameters are set in lines 4-9. At each for-loop iteration, the agent observes the current state (line 11) and selects the action to perform depending on the exploration rate ϵ which establishes if the action has to be chosen randomly (line 12) from the action set we previously defined in Section 3.2 or if has to be returned by the main DNN (line 16). Then, after taking the action, the agent waits for x seconds (line 19) and observes again the state reached by the environment and the correspondent reward (lines 20,21). At this point the algorithm stores the experience made by the agent inside E (line 22). The core of the code is in lines 24-27. First of all, the main Q network predicts the Q-values for the given state s_j (line 24). In particular y is an array with a number of elements equal to the number of possible actions that can be executed. Then, target Q-values are evaluated through the target DNN network (line 25) and used in the *Bellman* update formula (line 26); to be more specific, only the Q-value related to the action sampled from the batch will be updated leaving the other values untouched. After the update, the main DNN network is trained by executing one training step on the cost function (line 27) and if U steps have been executed, the target DNN network weights are set equal to the main DNN network ones (line 28).

4. A SIMULATION ENVIRONMENT

Designing and testing deep RL algorithms requires the presence of an operative environment where status can be *sensed* and actions can be performed by receiving the corresponding rewards.

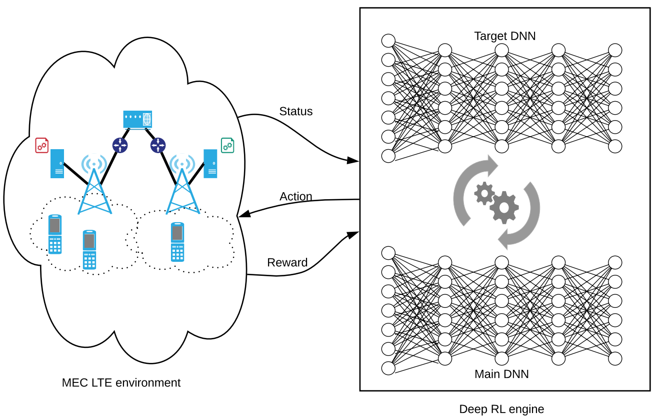


Figure 2 – Deep RL environment.

The general schema of a deep RL environment is depicted in Fig. 2 and consists of a *deep RL engine* where the algorithm (composed of the two DNNs) is running and an *environment* that in our case is composed of a LTE MEC with different MEC servers where different mobile users move while accessing some service. Due to the complexity of the LTE MEC environment and to the high number of actions that have to be tried by the deep RL algorithm before learning a good policy, we decided to simulate such an environment by using OMNeT++ [11]. The latter is a well-known event-driven simulator, written in C++, which allows us to model the network at a system level and a good level of detail, while scaling efficiently with the number of simulated nodes. Moreover, thanks to its large community of researchers and developers, OMNeT++ comes with a large set of pre-made and tested frameworks to simulate various portion of the network.
To model our MEC-enabled scenario, we used and integrate two of these simulation frameworks: SimuLTE [12] and INET [1]. The former models two main aspects of an LTE network, i.e., the 4G-based radio-access network and the EPC. The latter, instead, implements all the relevant TCP/IP protocols and layers, application and mobility models. In Fig. 3 we represent the high-level architecture and layering of the main communicating nodes, where grayed elements are from SimuLTE, whereas withe ones are from INET. The UE and the eNB nodes are provided with an LTE NIC, which provides wireless connectivity through the radio-access network, and implements a model of the LTE protocol stack, i.e. with PHY, MAC, RLC and PDCP, layers. Each UE can be configured with multiple TCP- or UDP-based applications, which can communicate both with the internet or with the MEC server(s). Moreover, the UE includes a module to model the mobility of the node itself. In the scenarios simulated within this paper, we used a waypoint-based mobility model, wherein UEs move linearly and at constant speed between randomly generated waypoints. The eNB is connected with the UE through the LTE NIC on one side, with the EPC through the GTP layer on the other. The EPC has also a model of the PGW (not shown in Fig. 3), and of the MEC server, which includes a complete TCP/IP stack. EPC nodes can be configured to have various L1/L2 types, e.g. based on PPP, ethernet, etc. Moreover, the parameters of the physical connections among nodes, such as bandwidth, delay, etc., can be configured to model various degrees of congestion within the network.

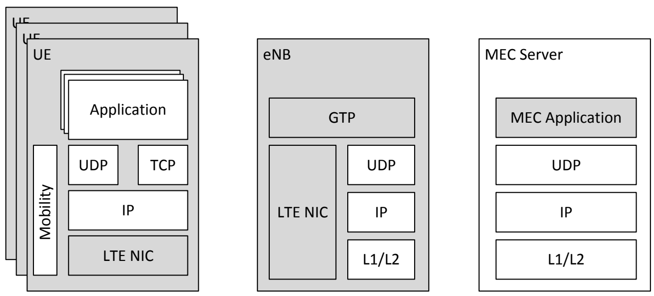


Figure 3 – High-level view of the simulator's architecture and layering. Grayed elements are from SimuLTE, white ones are from INET.

With respect to the deep RL engine, we used Keras [13] an open source library written in Python which runs on top of

[1] Available at "https://inet.omnetpp.org/", last accessed Jul 2018

machine learning frameworks like: TensorFlow, Theano and others. The main feature of this library is its simplicity, that allows to build complex neural network topologies with just a few lines of code in a *scikit-learn* fashion, but keeping at the same time the power of the neural network engine that runs underneath. Using Keras, we built a feedforward fully connected deep neural network composed of n hidden layers in between the input layer whose dimension is given by the cardinality $\|\mathcal{T}\|$ of the state t-uple, and the output layer whose dimension is given by the cardinality $\|\mathcal{Z}\|$ of the action set. In order to integrate the two systems which run respectively on Python and on C++ environments, we implemented a mechanism to let them communicate using text files. With reference to Fig. 2, the deep RL engine waits for the generation of the files containing the current state of the system, once it receives the data it generates as output a text file which contains the action to execute on the simulator. On the OMNeT++ side, we used an asynchronous timer which checks periodically for the action file availability, as soon as the file is available, the simulator is able to read the action code and change the server destination address for the *UEs* that are running the application indicated in the action thus emulating the data migration of the application from a server to another. After the action execution, the RL agent observes the reward obtained as the combination of several performance indexes provided by the OMNeT++ simulator by checking if the action performed has increased it or not. The reward in this sense is used by the agent as a feedback which helps it to understand if the action executed is a valid choice in that specific system state.

5. RESULTS

In this section, we present a preliminary scenario that we built to test the feasibility of the system where we only consider the presence of MEC servers without the possibility to use the Cloud. Fig.4 shows the structure of the network composed of three eNBs a set of devices with $\mathcal{K} = 9$, a set of MEC servers with $\mathcal{N} = 3$, a set of applications with $\mathcal{M} = 3$, and a set of actions with $\mathcal{Z} = \|\mathcal{N}\| \cdot \|\mathcal{M}\|$ where each action corresponds to the migration of an app taken from the *Apps* set to a server taken from the *MEC* set. The datarate connection provided by the cables which connect the eNBs is equal to 10 Gbps except for the ones that connect the routers to the PGW where the datarate is 3 Mbps to emulate a traffic congestion, thus creating a real scenario where we can test the performance of our algorithm. On the OMNeT++ side, it is possible to set several parameters for the simulation by using a configuration file called *omnetpp.ini*; since the number of parameters to set is very large, we synthesized them in a table.

Table 1 shows the main parameters we set for the simulation, we consider a total number of nine users who follow a random mobility motion pattern moving at speed equal to 1.5 mps which is a fairly good approximation for the human walking speed. With respect to the applications, we consider three constant bit rate applications (CBR) that can be run by only one MEC server per time. As already said at the beginning of this section, our goal is to test the feasibility of the technique

Configuration Parameters	
Number of users	9
User mobility	*RandomWayPointMobility*
User speed	1.5 mps
Number of applications	3
Application type	*UDP ConstantBitRate*
Packet size	1500*B*
Simulation Time	420 *seconds*

Table 1 – omnetpp.ini configuration.

we are proposing, for this reason, we decided to realize a scenario with manageable number of users and applications in order to keep the training time of the DNN not too high. In such a context, the state which defines the network can be expressed as follows:

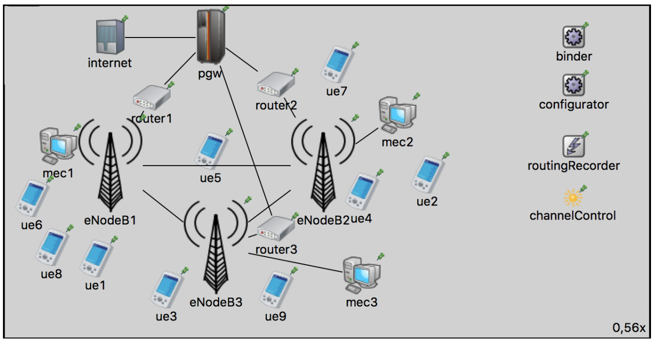


Figure 4 – OMNeT++/SimuLTE simulation scenario.

$$\begin{aligned} s =< (&UE_{eNB1}, UE_{eNB2}, UE_{eNB3}, \\ &eNB^1_{app1}, eNB^1_{app2}, eNB^1_{app3}, \\ &eNB^2_{app1}, eNB^2_{app2}, eNB^2_{app3}, \\ &eNB^3_{app1}, eNB^3_{app2}, eNB^3_{app3}, \\ &Mec^1_{app1}, Mec^1_{app2}, Mec^1_{app3}, \\ &Mec^2_{app1}, Mec^2_{app2}, Mec^2_{app3}, \\ &Mec^3_{app1}, Mec^3_{app2}, Mec^3_{app3}) > \end{aligned} \tag{10}$$

where:

- UE_{eNB_j} represents the number of devices connected to the j-th eNB;
- eNB^j_{appk} represents the number of devices which are running the k-th application in the j-th eNB;
- MEC^i_{appk} is a boolean flag that indicates if the i-th MEC server is running the k-th application.

With respect to the reward, we first defined as a QoS performance index the percentage of received data corresponding to the i-th application app_i as:

$$D^{app_i} = \frac{Received_{THR}}{\sum Sent_{THR} \cdot packetSize} \tag{11}$$

where the sum is extended to all the UEs that run the i-th application. In particular, we evaluated the average of the percentage of received data, for all the applications obtaining the final performance index value D. In order to observe the index after the action execution, we wait for ten seconds. Depending on the difference between the indexes evaluated before and after the execution on an action in the environment, we were able to define the reward as a number r which can assume the following values: [-1,-2/3,-1/3,0,1/3,2/3,1] where a value nearby one means that the action performed resulted in an improvement of system performance while a value nearby minus one means that the action performed resulted in a decrease of the system performance. For the sake of simplicity, we considered that UEs can only run one application per time. Our goal is to produce an optimal policy, which is able to address the problem related to the user's mobility inside the network in order to improve user QoS.

With respect to the DNN we designed, here we sum up the main parameters in the following table:

DNN parameters	
Number of hidden layers	3
Number of neurons	15
Input dimension	21
Output dimension	9
Learning rate	0.001
Activation function	*ReLU*
Update step	50
Batch size	32
Experience replay dimension	2000

Table 2 – Deep Neural Network parameters.

With reference to Table 2, by doing multiple tests, we were able to establish that 3 hidden layers create a good topology which is able to properly fit the desired output. Moreover, we fixed 15 neurons for each layer which is a number that stays in between the input layer dimension and the output one. With respect to the activation function, we used the *Rectified Linear Unit* (ReLU) which resulted in a faster learning if compared with other functions like the sigmoid. Since our DNN has to predict the state Q-values which are values defined in the set of $\mathbb{R}$, the problem we tried to solve is a *regression*. For this reason, the cost function we used is the *Mean Squared Error* (MSE) which is typical for this kind of problems and defined as:

$$MSE = \frac{1}{n}\sum_{i}^{n}(y_i - \widehat{y_i})^2 \qquad (12)$$

where y is the real output and $\widehat{y_i}$ is the output predicted by the DNN. Regarding the update step, the batch size, and the experience replay dimension, the values we set has been obtained empirically by trying different values.

In Fig.5 we show a comparison between the policy learned after training for 25000 seconds of simulation our Deep RL algorithm and a scenario without any policy where we simply distributed one application for each MEC server. For a fair comparison, we used the same random seed in order to maintain in both simulation the same user mobility pattern. Plots show that the Deep RL algorithm is able to improve the overall system performance, in particular except for a little period between 100 and 200 seconds where the Deep RL algorithm encounters a little decrease (mainly due to the stochasticity of the environment), the results are in general good reaching an average of 0.60 which is better if compared with the no policy average equal to 0.54. As we are writing, we are trying to extend the training time with the aim to further improve the obtained results.

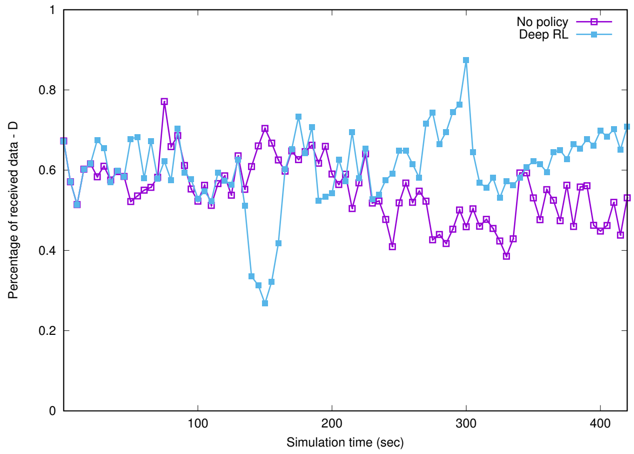


Figure 5 – Comparison between the performance obtained by the Deep RL policy and a scenario where the data migration is not enabled.

6. CONCLUSIONS

In this paper, we presented a deep reinforcement learning approach to address the problem related to the network environment dynamics. We designed a Deep RL algorithm and tested it in a real scenario demonstrating the feasibility of the technique. Future works will be devoted to implement a better integration with the OMNeT++ environment by using the Tensorflow C++ frontend, to compare with other solutions,to use more realistic traffic and mobility models, and to the investigation of new indexes with the aim to further improve the system performance.

REFERENCES

[1] D. Bruneo, S. Distefano, F. Longo, G. Merlino, and A. Puliafito, "I/Ocloud: Adding an IoT Dimension to Cloud Infrastructures," *Computer*, vol. 51, no. 1, pp. 57–65, January 2018.

[2] R. Dautov, S. Distefano, D. Bruneo, F. Longo, G. Merlino, and A. Puliafito, "Data processing in cyber-physical-social systems through edge computing," *IEEE Access*, vol. 6, pp. 29822–29835, 2018.

[3] P. Bellavista, A. Zanni, and M. Solimando, "A migration-enhanced edge computing support for mobile devices in hostile environments," in *2017 13th International Wireless Communications and Mobile*

Computing Conference (IWCMC), June 2017, pp. 957–962.

[4] M. G. R. Alam, Y. K. Tun, and C. S. Hong, "Multi-agent and reinforcement learning based code offloading in mobile fog," in *2016 International Conference on Information Networking (ICOIN)*, Jan 2016, pp. 285–290.

[5] ETSI, "Mobile edge computing (mec); framework and reference architecture," March 2016.

[6] ETSI, "Mobile edge computing (mec); service scenarios," Tech. Rep., November 2015.

[7] X. Xia, K. Xu, Y. Wang, and Y. Xu, "A 5g-enabling technology: Benefits, feasibility, and limitations of in-band full-duplex mmimo," *IEEE Vehicular Technology Magazine*, pp. 1–1, 2018.

[8] J. Li, Z. Zhao, and R. Li, "Machine learning-based ids for software-defined 5g network," *IET Networks*, vol. 7, no. 2, pp. 53–60, 2018.

[9] Stuart J. Russell and Peter Norvig, *Artificial Intelligence - A Modern Approach (3. internat. ed.)*, Pearson Education, 2010.

[10] Mnih Volodymyr *et al.*, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, Feb. 2015.

[11] András Varga and Rudolf Hornig, "An overview of the omnet++ simulation environment," in *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, ICST, Brussels, Belgium, Belgium, 2008, Simutools '08, pp. 60:1–60:10, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[12] A. Virdis, G. Stea, and G. Nardini, "Simulte - a modular system-level simulator for lte/lte-a networks based on omnet++," in *2014 International Conference on Simulation and Modeling Methodologies, Technologies and Applications (SIMULTECH)*, Aug. 2014, vol. 00, pp. 59–70.

[13] François Chollet et al., "Keras," `https://keras.io`, 2015.

Predicting Activities in Business Processes with LSTM Recurrent Neural Networks

Edgar Tello-Leal[1]*; Jorge Roa*[2]*; Mariano Rubiolo*[2,3]*; Ulises M. Ramirez-Alcocer*[1]

[1]Faculty of Engineering and Science, Autonomous University of Tamaulipas, Victoria, Tamaulipas, Mexico, 87000
[2]CIDISI, Santa Fe Regional Faculty, National Technological University, Lavaisse 610, (S3004EWB) Santa Fe, Argentina.
[3]Research Institute for Signals, Systems and Computational Intelligence, sinc(i), FICH/UNL-CONICET, Ciudad Universitaria, (3000) Santa Fe, Argentina.

ABSTRACT

The Long Short-Term Memory (LSTM) Recurrent Neural Networks provide a high precision in the prediction of sequences in several application domains. In the domain of business processes it is currently possible to exploit event logs to make predictions about the execution of cases. This article shows that LSTM networks can also be used for the prediction of execution of cases in the context of an event log that originates from the IoT and Industry 4.0 domain. This is a key aspect to provide valuable input for planning and resource allocation (either physical or virtual), since each trace associated with a case indicates the sequential execution of activities in business processes. A methodology for the implementation of an LSTM neural network is also proposed. An event log of the industry domain is used to train and test the proposed LSTM neural network. Our preliminary results indicate that the prediction of the next activity is acceptable according to the literature of the domain.

Keywords - LSTM, event log, process mining, business process

1. INTRODUCTION

In a knowledge-based economy, public and private organizations require proper knowledge asset management to maintain a competitive advantage in global markets or in government services. With the advent of robotics, machine learning, and 5G networks there will be a wealth of opportunities for cooperation between robots and humans improving productivity and speeding up the delivery of services for citizens. In this context, the Business Process Management (BPM) is considered a key component to managing the life-cycle of business processes that orchestrate the activities performed in organizations as well as the resources (humans, robots, or information systems) that execute such activities.

A *business process* consists of a set of activities that are performed in a coordinated way in an organization in a technical environment, and have at least one correlated business goal [1]. The standard language for modeling business processes is BPMN (Business Process Modeling Notation) [2]. Information technologies in general and information systems in particular play an important role in the management of business processes, because a large number of activities that organizations perform are supported by information systems. Several types of activities contained in the business processes can be executed automatically by the information systems, without the participation of a human.

The convergence of solutions and products towards the BPM and the Service Oriented Architecture (SOA) paradigm adopted for industrial systems contributes to the improvement in the reactivity and performance of industrial processes such as manufacturing or logistics among others [3]. This is leading to a situation where information is registered in event logs, making it available in near-real time based on asynchronous events, and to business-level applications that are able to use high-level information for various purposes, such as diagnosis, performance indicators, or traceability. [3].

In this context, predicting the behavior of a business process, i.e. exploiting event logs to make predictions about the execution of activities [4], is a key aspect in order to provide valuable input for planning and resource allocation [4]. There are two main factors for the growing interest in predicting business process behavior. On the one hand, with the advent of 5G and the Internet of Things (IoT) in the context of Industry 4.0 [3], more and more events are recorded due to the great number of devices connected to the Internet, providing detailed information about the history of business processes. On the other hand, there is a need to improve and support business processes in competitive and rapidly changing environments.

Process mining techniques [5, 6] are capable of extracting knowledge from event logs, commonly available in information systems. These techniques provide new means to discover, monitor and improve business processes in a variety of application domains. However, standard process mining techniques cannot deal with predicting process behavior.

The recurrent neural network (RNN) architecture has become a model of the neural network implemented in different domains, due to its natural ability to process sequential entries and to know their long-term dependencies [7]. Unlike the feed-forward neural network, the RNN neurons are connected to each other in the same hidden layer and a training function is applied to the hidden states repeatedly [7]. The Long Short-Term Memory (LSTM) neural network is an extension of the RNN, which has achieved excellent performance in various tasks, especially for sequential problems [8], [9], [10]. The implementation of LSTM neural networks for the discovery of events or activities of a business process through predictive analysis can be considered an important strategy as a technique of process mining and has been used with success in this domain [4, 11].

In this work, we propose an approach for the discovery of events and activities of a business process through predictive analysis from traces contained in event logs taken from the IoT and Industry 4.0 domain. The predictive model is based on an LSTM recurrent neural network that is trained with event logs, enabling the prediction of the following activity in a trace of execution that follows another activity or a set of activities given as input. In order to validate the approach and show the applicability to the proposed domain we present preliminary results based on a dataset with 255 traces. The test carried out on the trained LSTM network shows that it has the capacity to predict the next activity of a business process model.

This work is structured as follows. Section 2 presents the background. Section 3 presents an introductory example. Section 4 introduces an approach to predict business process behavior. Section 5 shows the results. Section 6 presents related work. Finally, Section 7 concludes this work and proposes future work.

2. BACKGROUND

2.1 Process Mining

Process mining is an area of research that is located, on the one hand, between computational intelligence and data mining, and on the other hand, between business process modeling and analysis. There are several areas that are included in process mining, such as process discovery, compliance verification, process improvement, organizational mining, process model extension, automatic repair of process models, case prediction, automatic construction of models based on simulation, and recommendations based on the history of execution of processes.

In process mining, it is assumed that it is possible to record events sequentially since each event has a reference to an activity and is related to a particular case (an instance of the process) [6]. Then, the input data in the process mining is an event log. An *event log* is a hierarchically structured file with data on the executions of business processes [12]. This file contains data on several executions of the same business process. An *event* is the atomic part of the execution of a specific process and may contain a large number of attributes. Event data, generated by information systems, is usually found as updates to a state (for example, the status of "sent invoice" changes to the status "paid invoice"), or also as activity records (for example, " email sent to the client "). A *trace* is a set of events that belong to the same execution of a business process. Therefore, event logs can contain additional information about events, such as the user who runs the activity or device that initiates the activity, the time the event started, the duration of the event, among others.

The main tasks of process mining are discovery, compliance and process improvement [6]. *Process discovery* consists of using an event log as input and producing a business process model without using a-priori information [6]. The model discovered is typically a business process model represented using a graphical notation such as the BPMN language [2], Petri nets [13, 14, 15], Event-driven Process Chains (EPC) [16], or UML activity diagrams [17]. *Process conformance* consists of comparing a business process model with the event record generated by the execution of the same process model [6]. Conformance verification can be used to evaluate whether the information stored in the event log is equivalent to the model and vice versa. *Process improvement* consists of extending or improving an existing process model using the stored information of the current process in the event log.

2.2 LSTM Neural Networks

Recurrent neural networks (RNN) with Long Short-Term Memory (LSTM) emerged as an effective and scalable model for learning problems related to sequential data [18]. RNNs have two types of input, the present, and the recent past. RNN use both types of input to determine how they behave with respect to new data. This means that the output of a RNN at time step *t*-1 affects its output at time step *t*. LSTMs are general and effective at capturing longterm temporal dependencies [18].

The information contained in LSTMs are outside the normal flow of the recurrent network in a gated cell. Information can be stored, written or read from a cell, similar to data in a computer's memory. The cell makes decisions about what should be stored and when it should be allowed to read, write and delete, through gates that open and close. These gates are implemented with the multiplication of elements by sigmoids, which are all in the range of 0-1.

3. INTRODUCTORY EXAMPLE

Industries work to increase the overall effectiveness of their plants and equipments, in order to get better system integration, availability, maintainability, performance, quality, or functionality. [3]. The example analyzed in this paper is based on [19] and focuses on the control of a plant to increase its overall performance, including predictive maintenance. The plant produces parts made of metal such as spurs, fastener, ball nuts, discs, tubes, wheel shafts, or clamps. To build these parts there are 28 machines for lapping, milling, turning, sinking, wire cutting, turning and milling, laser marking, and round and flat grinding.

Table 1 shows an excerpt of the event log of the process that controls the logic of the plant. The complete log can be found in [19]. The dataset contains process data from a production process, including data on cases, activities, resources, timestamps, and more data fields.

It is known that, in general, with higher quality and information coming from sensors in the process and the critical equipment for the control of the plant, it is possible to improve the plant operation and production planning [3]. In this scenario, exploiting event logs, that provide detailed information about the history of business processes and register sensor information, for predicting the next activity to be executed in a business process is important to provide valuable input for planning and resource allocation, such as

preparing a machine or a resource to be ready and on time for production.
Besides physical resources, the planning and allocation of resources could also refer to the cloud. With the advent of the Industry 4.0 and the automation of cyber-physical systems, many information systems are being executed in the cloud. In this context, on-demand elasticity is a key aspect. In cloud computing, elasticity is defined as "the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible" [20]. Knowing from advance which one is the next activity of a business process that is going to be executed is key to pro-actively release or reserve resources to support elasticity on the cloud.

4. PREDICTING BUSINESS PROCESS ACTIVITIES

This Section introduces a methodology to predict activities in business processes from information registered in event logs derived from the execution of business processes.
The proposed methodology is based on the LSTM neural network and consists of three phases: 1) pre-processing of the event log, 2) categorization, and 3) prediction model based on LSTM, as shown in Figure 1.

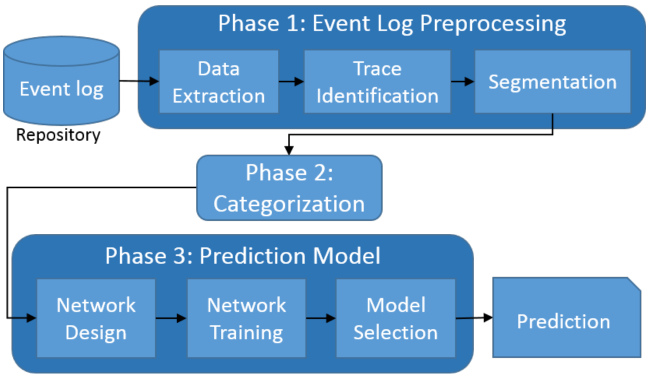


Figure 1 – The methodology for predicting activities of a business process using the proposed approach.

4.1 Phase 1: Event Log Preprocessing

The pre-processing phase of the event log consists of the following stages:

Data Extraction. A detailed analysis of the event logs is performed (.XES file format), which allows the identification of the different attributes contained in the event log, allowing to select the attributes required for a prediction, in this case, the attribute "*activity*".

Trace Identification. It consists of identifying and obtaining the traces, with their respective events. Then, the traces are added in a text file maintaining their order of appearance.

Segmentation. A segmentation task is applied to the text file generated in the previous stage, which consists of creating a list of all the events of a trace, using a criterion of separation between each event. Then, each event is represented as a unique integer, allowing the traces to be converted into a sequence of integers, generating two sequence lists of "integers", the first list consisting of input activities (X), and the second list of output activities (Y). Finally, the sequence list of input activities is transformed into a two-dimensional matrix (number of sequences, the maximum length of sequences).

4.2 Phase 2: Categorization

The intermediate categorization phase consists of a process to categorize the sequence of integers corresponding to the output activities (Y), in a one hot encoding representation type, specifying that the number of classes will be equal to the size of the vocabulary.

4.3 Phase 3: Prediction Model

The prediction model phase based on LSTM network is composed of the following stages:

Network Design. It consists of generating a design of the LSTM network by layers. First, an input layer is generated (embedding) to the network, then the hidden layer (LSTM units) is created so that finally an output layer is built. In each of these layers, some necessary parameters are defined.

Network Training. The training of the LSTM network is carried out using as training data the sequence list of integers represented by the activities contained in the matrix (X) and in the representation one hot type (Y).

Model Selection. The results of the training will allow choosing a model of the LSTM network as the final model to be implemented. A network with training with a high degree of accuracy should be selected as the model to make the predictions. Otherwise, it is recommended to modify the design of the network, adjusting the required parameters and execute network training again.

Prediction. It is the output generated by the LSTM neural network, which through a training stage allows predicting the next activity in a business process model, from an input activity or a sequence of input activities, which is explained in the following sections of the document.

4.4 Implementation

The proposed approach is based on the definition of a recurrent neural network LSTM, considered as a network of a special structure consisting of memory blocks and memory cells, together with the gate units that contain them [21], i.e, an LSTM unit consists of a cell and three gates (input, forget, and output). Through this special structure, an LSTM network can select which information is forgotten or remembered.

Table 1 – Excerpt of event log based on [19]

Case ID	Activity	Resource	Time-stamp
Case 1	Turning & Milling - Machine 4	Machine 4 - Turning & Milling	29/1/2012 23:24
Case 1	Turning & Milling - Machine 4	Machine 4 - Turning & Milling	30/1/2012 05:44
Case 1	Turning & Milling - Machine 4	Machine 4 - Turning & Milling	30/1/2012 06:59
Case 1	Turning & Milling - Machine 4	Machine 4 - Turning & Milling	30/1/2012 07:21
Case 1	Turning & Milling Q.C.	Quality Check 1	31/1/2012 13:20
Case 1	Laser Marking - Machine 7	Machine 7- Laser Marking	1/2/2012 08:18
Case 1	Lapping - Machine 1	Machine 1 - Lapping	14/2/2012 00:00
Case 1	Lapping - Machine 1	Machine 1 - Lapping	14/2/2012 00:00
Case 1	Lapping - Machine 1	Machine 1 - Lapping	14/2/2012 09:05
Case 1	Lapping - Machine 1	Machine 1 - Lapping	14/2/2012 09:05
Case 1	Round Grinding - Machine 3	Machine 3 - Round Grinding	14/2/2012 09:13
Case 1	Round Grinding - Machine 3	Machine 3 - Round Grinding	14/2/2012 13:37
Case 1	Final Inspection Q.C.	Quality Check 1	16/2/2012 06:59
Case 1	Final Inspection Q.C.	Quality Check 1	16/2/2012 12:11
Case 1	Final Inspection Q.C.	Quality Check 1	16/2/2012 12:43
Case 1	Packing	Packing	17/2/2012 00:00
...	...	...	...
Case 253	Flat Grinding - Machine 11	Machine 11 - Grinding	10/1/2012 11:59
Case 253	Lapping - Machine 1	Machine 1 - Lapping	11/1/2012 00:00
Case 253	Laser Marking - Machine 7	Machine 7- Laser Marking	11/1/2012 14:23
Case 253	Final Inspection Q.C.	Quality Check 1	15/1/2012 06:50
Case 253	Packing	Packing	16/1/2012 00:00
Case 253	Packing	Packing	16/1/2012 00:00
Case 254	Laser Marking - Machine 7	Machine 7- Laser Marking	2/1/2012 10:15
Case 254	Flat Grinding - Machine 11	Machine 11 - Grinding	2/1/2012 14:00
Case 254	Flat Grinding - Machine 11	Machine 11 - Grinding	3/1/2012 17:04
Case 254	Flat Grinding - Machine 11	Machine 11 - Grinding	4/1/2012 10:28
Case 254	Final Inspection Q.C.	Quality Check 1	4/1/2012 15:26
Case 254	Packing	Packing	6/1/2012 00:00
Case 254	Final Inspection Q.C.	Quality Check 1	6/1/2012 10:24
Case 255	Turning - Machine 8	Machine 15 - Turning	2/1/2012 07:00
Case 255	Turning Q.C.	Quality Check 1	5/1/2012 13:58
Case 255	Laser Marking - Machine 7	Machine 7- Laser Marking	10/1/2012 09:22
Case 255	Final Inspection Q.C.	Quality Check 1	11/1/2012 10:22
Case 255	Packing	Packing	16/1/2012 00:00

The multiplicative input gate units are used to avoid the negative effects that unrelated inputs can create. The input gate controls the input flow to the memory cell, and the output gate controls the output sequence of the memory cell to other LSTM blocks.

The forget gate in the structure of the memory block is controlled by a single-layer of the neural network. At a time t, the components of the LSTM unit are updated by means of equation *(1)* [22, 9].

$$f_t = \sigma(W[x_t, h_{t-1}, C_{t-1}] + b_f) \qquad (1)$$

where x_t is the input sequence, h_{t-1} is the previous block output, C_{t-1} is the previous LSTM block memory, and b_f is the polarization vector. W represents separate weight vectors for each input and σ is the logistic sigmoid function. The sigmoid activation function, which is the output of the forgetting gate, is applied to the previous memory block by multiplication by elements. Therefore, the degree to which the previous memory block will be effective in the current LSTM is determined. If the activation output vector contains values close to zero, the previous memory will be forgotten. The input gate is a section where the new memory is created by a simple neural network with the activation function $tanh$ and the previous memory block. These operations are calculated using equations *(2)* and *(3)*.

$$i_t = \sigma(W[x_t, h_{t-1}, C_{t-1}] + b_i) \qquad (2)$$

$$C_t = f_t.C_{t-1} + i_t.tanh(W[x_t, h_{t-1}, C_{t-1}] + b_c) \qquad (3)$$

Finally, the output gate is the section where the probabilities of the current LSTM block are generated [9]. The output is calculated by means of equations *(4)* and *(5)*.

$$o_t = \sigma(W[x_t, h_{t-1}, C_{t-1}] + b_o) \qquad (4)$$

$$h_t = tanh(C_t).o_t \quad (5)$$

5. RESULTS

Keras [23] was used for the implementation, which is a Python library that allows building models of deep learning networks. The implementation parameters of the LSTM network are presented in Table 2.

Table 2 – Configuration parameters of the LSTM neural network

Parameter	Value
epochs	500
batch size	20
optimizer	Adam
loss	categorical_crossentropy
LSTM units	50

The LSTM neural network was trained with an event log described in Section 3. This event log includes 255 traces of the business process model. There are 56 different activities contained in the log. The number of sequences identified during the network training was 4541. The LSTM network accepts as input data an activity, in order to predict the next activity of the sequence. The neural network was configured to predict three outputs per instance, ordered by a higher to lower probability. The objective is to know the prediction capacity of the neural network of the next activity. The algorithms and datasets can be accessed at `\http://dx.doi.org/10.17632/trskzyg3j9.1`.

Table 3 summarizes the activities in the event log and their acronyms. The name of the activities in the table are acronyms from the real name included in the event log. For instance: "Turning & MillingQ.C." (TMQC), "LaserMarking-Machine7" (LMM7).

Table 4 presents an extract of the results obtained in the prediction of the neural network using the Event Log presented before. In the column "Input Activity" it is mentioned the activity used as a new input for the LSTM network in the prediction process. The "Target Activity" is the expected activity (or activities) for the corresponding input activity, that is, the activities with the highest probability of prediction by the neural network, based on the weights of each activity. Each row in the table shows a case of prediction of the next activity from the input one. The "Output Activity" column presents the activities that the LSTM neural network predicted from the input activity.

The test carried out on the trained LSTM network shows that it has the capacity to predict the next activity of a business process model. For the cases number 3, 5, 7 and 8, the network was able to predict the exact next activity. For instance, in the third case, receiving the GRM27 as input, the LSTM network was able to predict the expected FIQC (the output activity is included in the target activity list, with the highest probability). In other cases, as the number 1, 2, 4 and 6, the most of the target activities were identified, missing

Table 3 – List of activities and acronyms

Activity name	Acronym
Turning&Milling-Machine	TMM
Turning&MillingQ.C.	TMQC
LaserMarking-Machine	LMM
RoundGrinding-Machine	RGM
RoundQ.C.	RQC
FinalInspectionQ.C.	FIQC
Packing	PACK
TurningQ.C.	TQC
GrindingRework-Machine	GRM
GrindingRework	GR
WireCut-Machine	WCM
Fix-Machine	FM
NitrationQ.C.	NQC

Table 4 – An extract of the prediction from LSTM

No.	Input Activity	Target Activity	Output Activity 1	Output Activity 2
1	TMQC	LMM7 | LPM1 | TMM4	LMM7	LPM1
2	PACK	FIQC | FM15	FIQC	
3	GRM27	FIQC	FIQC	
4	GR	LPM1 | TMQC	LPM1	
5	WCM18	TQC	TQC	
6	RGM19	RGM12 | FIQC	RGM12	
7	NQC	TMM5 | TMQC	TMM5	TMQC
8	RQC	PACK | FIQC	PACK	FIQC
9	FM15	PACK	PACK	TMQC
10	FGM26	FIQC	PACK	MM14

one that was not predicted. For instance, in the first case, were predicted the LMM7 and LPM1 activities, but not the TMM4. However, in these cases, the next activity that is predicted is the one with the highest probability. Furthermore, in the case number 9 in which the prediction obtain the desired activity but one of them was not expected in the target. In this instance, using the FM15 as input, it was expected that the LSTM throw as output only the PACK, but the TMQC was also included as a response. At last, in the case number 10, the target activity is FIQC, but the LSTM network predicts two activities that do not match with activity what was expected.

6. RELATED WORK

The development of technological solutions for event log analysis for business process discovery using the principles of data mining has been previously studied in [6, 12]. The most relevant proposals that are related to the approach proposed in this research work are discussed in this section. However, existing techniques are not able to predict at runtime the next activities that are going to be executed in a business process. We expect that techniques based on LSTM neural networks, like the proposed in this work, can also be of help in the discovery of business process models.

There are a few approaches using patterns and statistical models to predict activities in business processes. The approach described in [24], aims at identifying partial business process models to be used for training predictive models. It infers two types of predictive models. The first model is used to identify frequent partial processes in form of frequent activity sequences, the sequences are extracted using a frequent pattern mining algorithm and are represented in form of sequence trees. The second model is used for the estimation of the completion time, associating each node of the tree a specific prediction model that takes into account attributes such as the performer of each activity, the cost associated to the event or the place where the event is performed. In [25], authors propose Markov chains to estimate the instance-specific probabilistic process model (PPM) that can take as input a running process instance, and compute the probability of execution of a particular task in that instance. An instance-specific PPM serves as a representation to predict the likelihood of different outcomes. Similarly, in [26] authors propose methods which use sequential k-nearest neighbor and higher order Markov models for predicting the next tasks in a business process instance. The sequential k-nearest neighbor technique is applied when the default prediction is required (when the given sequence cannot be found in the transition matrix). The matching procedure is applied in order to extract the given sequence's most similar sequences (patterns) from the traces.

The use of neural networks to predict activities is a recent field. In [11], the author presents an approach to predict the next process event using deep learning based on an LSTM recurrent neural network. The proposed approach is based on the prediction of the next word in a sentence (natural language processing), i.e., by interpreting process event logs as text, process traces as sentences, and process events as words. The implementation of the LSTM network is through an architecture of two hidden layers. The approach is evaluated on two real datasets commonly used in the state-of-the-art, presenting better results in prediction precision. Similarly, in [4], authors propose a method based on LSTM that allows predicting the next activity and its time-stamp per case contained in an event record. The authors mention that the results of the neural network are outstanding using real-life data sets compared to traditional methods of automatic learning. Additionally, the authors conclude that predicting the next activity and its time-stamp via a single model yields a higher accuracy than predicting them using separate models.

In our proposal, the sequences of the traces identified in the event record are conserved, which allows us to improve the accuracy of the model. In addition, the use of a one-hot encoding is proposed, allowing to increase the percentage of the prediction of the next activity. Additionally, the proposed LSTM neural network has the ability to predict the next activity from one or more input activities, as well as to predict one to three output activities, ordered from highest to lowest probability of occurrence.

7. CONCLUSIONS AND FUTURE WORK

With the advent of 5G, IoT, and Industry 4.0 there is a growing interest in predicting business process behavior. More and more events are recorded due to the great number of devices connected to the Internet, providing detailed information about the history of business processes.

In this work, a methodology for the prediction of business process activities has been proposed. The methodology is based on an LSTM recurrent neural network and exploit event logs to make predictions about the execution of cases. This is key to provide valuable input for planning and resource allocation (either physical or virtual), specially in competitive and rapidly changing environments.

The proposed methodology considers event log preprocessing, categorization, and prediction model, and allows identifying the phases required to predict the next activity or event, through the implementation of the LSTM neural network. The novelty of this approach resides in the use of event logs that originates from an IoT domain within the context Industry 4.0.

In order to validate the approach and show the applicability to the proposed domain we present preliminary results based on a dataset with 255 traces. The test carried out on the trained LSTM network shows that it has the capacity to predict the next activity of a business process model. However, in order to fully validate the approach, more tests are needed.

It is also necessary to take into account that, since the LSTM cells maintain the state, the order in which the traces are used to train the network has a direct effect on the result. In addition, the selection of the trace set of an event log (training data) also influences results, and hence, results obtained with a particular sample may not be generalized to other cases (or event logs).

The predictive analysis implemented in this work allows us to obtain useful information to determine the next activity to be executed based on event logs. Our next steps deal with expanding our study to other event logs with a greater number of traces, as well as considering including two or more classes to predict the next activity or event.

REFERENCES

[1] M. Weske, "Business process management architectures," in *Business Process Management*. Springer, 2012, pp. 333–371.

[2] BPMN 2.0, "Business Process Modeling Notation 2.0," http://www.omg.org/spec/BPMN/2.0/, 2011.

[3] A. W. Colombo, T. Bangemann, S. Karnouskos, J. Delsing, P. Stluka, R. Harrison, F. Jammes, J. L. Lastra *et al.*, *Industrial cloud-based cyber-physical systems*. Springer, 2014.

[4] N. Tax, I. Verenich, M. La Rosa, and M. Dumas, "Predictive business process monitoring with LSTM neural networks," in *Advanced Information Systems Engineering*, E. Dubois and K. Pohl, Eds. Cham: Springer International Publishing, 2017, pp. 477–492.

[5] W. Van Der Aalst, A. Adriansyah, A. K. A. De Medeiros, F. Arcieri, T. Baier, T. Blickle, J. C. Bose, P. van den Brand, R. Brandtjen, J. Buijs *et al.*, "Process mining manifesto," in *International Conference on Business Process Management*. Springer, 2011, pp. 169–194.

[6] W. M. Van der Aalst, *Process mining: data science in action*. Springer, 2016.

[7] W. Xia, W. Zhu, B. Liao, M. Chen, L. Cai, and L. Huang, "Novel architecture for long short-term memory used in question classification," *Neurocomputing*, vol. 299, pp. 20–31, 2018.

[8] Y. Li and H. Cao, "Prediction for tourism flow based on LSTM neural network," *Procedia Computer Science*, vol. 129, pp. 277–283, 2018.

[9] B. Cortez, B. Carrera, Y.-J. Kim, and J.-Y. Jung, "An architecture for emergency event prediction using LSTM recurrent neural networks," *Expert Systems with Applications*, 2017.

[10] F. Liu, Z. Chen, and J. Wang, "Video image target monitoring based on RNN-LSTM," *Multimedia Tools and Applications*, pp. 1–18, 2018.

[11] J. Evermann, J.-R. Rehse, and P. Fettke, "Predicting process behaviour using deep learning," *Decision Support Systems*, vol. 100, pp. 129 – 140, 2017, smart Business Process Management.

[12] T. Baier, J. Mendling, and M. Weske, "Bridging abstraction layers in process mining," *Information Systems*, vol. 46, pp. 123–139, 2014.

[13] K. Jensen and L. M. Kristensen, *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*, 1st ed. Springer Publishing Company, Incorporated, 2009.

[14] J. Roa, O. Chiotti, and P. Villarreal, "Behavior alignment and control flow verification of process and service choreographies," *Journal of Universal Computer Science*, vol. 18, no. 17, pp. 2383–2406, sep 2012.

[15] E. Tello-Leal, O. Chiotti, and P. D. Villarreal, "Software agent architecture for managing inter-organizational collaborations," *Journal of applied research and technology*, vol. 12, no. 3, pp. 514–526, 2014.

[16] F. Gottschalk, W. M. van der Aalst, and M. H. Jansen-Vullers, "Merging event-driven process chains," in *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*. Springer, 2008, pp. 418–426.

[17] UML 2.0, "Unified Modeling Language 2.0," http://www.omg.org/spec/UML/2.0/, 2005.

[18] K. Greff, R. K. Srivastava, J. Koutník, B. R. Steunebrink, and J. Schmidhuber, "LSTM: A search space odyssey," *IEEE transactions on neural networks and learning systems*, vol. 28, no. 10, pp. 2222–2232, 2017.

[19] D. Levy, "Production Analysis with Process Mining Technology. Dataset," 2014. [Online]. Available: https://data.4tu.nl/repository/collection:event_logs

[20] H. N. Roman, S. Kounev, and R. Reussner, "Elasticity in cloud computing: What it is, and what it is not," in *Proceedings of the 10th International Conference on Autonomic Computing (ICAC 2013)*, 2013.

[21] H. Sak, A. W. Senior, and F. Beaufays, "Long short-term memory recurrent neural network architectures for large scale acoustic modeling," in *15th Annual Conference of the International Speech Communication Association*, September 2014, pp. 338–342.

[22] S. Hochreiter and J. Schmidhuber, "Long Short-Term Memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[23] Chollet, F. Keras, "Keras: The Python Deep Learning library," https://github.com/fchollet/keras, 2018.

[24] M. Ceci, P. F. Lanotte, F. Fumarola, D. P. Cavallo, and D. Malerba, "Completion time and next activity prediction of processes using sequential pattern mining," in *Discovery Science*, S. Džeroski, P. Panov, D. Kocev, and L. Todorovski, Eds. Cham: Springer International Publishing, 2014, pp. 49–61.

[25] G. T. Lakshmanan, D. Shamsi, Y. N. Doganata, M. Unuvar, and R. Khalaf, "A markov prediction model for data-driven semi-structured business processes," *Knowledge and Information Systems*, vol. 42, no. 1, pp. 97–126, Jan 2015. [Online]. Available: https://doi.org/10.1007/s10115-013-0697-8

[26] M. Le, B. Gabrys, and D. Nauck, "A hybrid model for business process event prediction," in *Research and Development in Intelligent Systems XXIX*, M. Bramer and M. Petridis, Eds. London: Springer London, 2012, pp. 179–192.

SESSION 5

NETWORK APPLICATIONS OF MACHINE LEARNING

SMART USAGE OF MULTIPLE RAT IN IOT-ORIENTED 5G NETWORKS: A REINFORCEMENT LEARNING APPROACH

Ruben M. Sandoval, Sebastian Canovas-Carrasco, Antonio-Javier Garcia-Sanchez, and Joan Garcia-Haro

Department of Information and Communication Technologies, Technical University of Cartagena, Cartagena, Spain.
Emails: {ruben.martinez, sebas.canovas, antoniojavier.garcia, joang.haro}@upct.es

ABSTRACT

Smart Cities and Smart Industries are the flagships of the future IoT due to their potential to revolutionize the way in which people live and produce in advanced societies. In these two scenarios, a robust and ubiquitous communication infrastructure is needed to accommodate the traffic generated by the 10 billion devices that are expected by the year 2020. Due to its future world-wide presence, 5G is called to be this enabling technology. However, 5G is not a perfect solution, thus providing IoT nodes with different Radio Access Technologies (RATs) would allow them to exploit the various benefits offered by each RAT (such as lower power consumption or reduced operational costs). By making use of the mathematical framework of Reinforcement Learning, we have formulated the problem of deciding which RAT should an IoT node employ when reporting events. These so-called transmission policies maximize a predefined reward closely related to classical throughput while keeping power consumption and operational costs below a certain limit. A set of simulations are performed for IoT nodes provided with two RATs: LoRa and 5G. The results obtained are compared to those achieved under other intuitive policies to further highlight the benefits of our proposal.

Keywords – 5G, IoT, Reinforcement Learning, Multi-RAT, LPWAN, Machine Learning

1. INTRODUCTION

The growing demand for automatization mechanisms in all quotidian areas has led to the Internet of Things (IoT) paradigm. This technological revolution has enabled the interconnection of all sorts of devices, known as *things*, by equipping them with a communication module and a basic sensor, memory, and computing unit. It is now extensively demonstrated that endowing things with some intelligence has a positive impact on the entire society, leading to a better management of critical resources such as water [1], energy [2] and city assets in general [3], [4].

The progressive integration of different automation systems in urban environments is leading to the so-called *Smart City*. In these Smart Cities ubiquitous machine-to-machine (M2M) and machine-to-human (M2H) communications enable cleaner, sustainable and more cost-efficient urban spaces, ultimately improving citizens' quality of life. A similar concept emerges in the manufacturing and productive sector, where the term *Smart Industry* (SI) has been coined and received increasing attention in past years. In this particular communication environment, most of generated data is derived from M2M interactions, either from monitoring, actuation, or a combination of both -which gives rise to modern autonomous systems (e.g. control and actuation on industrial plants)-. This computerization entails a significant reduction in both cost and safety risks, since a real-time monitoring of critical facilities can be performed without the requirement of additional human resources.

This increase in the number of control, monitoring and actuation communication tasks in both cities and industries lead to a prominent rise in data generated. Since most IoT devices communicate via wireless communications, several efforts are being devoted to the development of new Radio Access Technologies (RATs) to alleviate the expected network congestion. Among these RATs, 5G excels as a promising solution to enable power and cost-efficient wireless network infrastructures. Long Term Evolution (LTE), that can be considered to have laid the foundations for the 5G revolution, has already had a measurable positive impact on the performance of cellular networks (one of the most popular RATs for IoT). However, the number of IoT devices is expected to reach 10 billion by the year 2020 [5]. This sheer increment in data transmitted along with the particularities of IoT-generated traffic, as discussed below, have posed serious doubts about the sustainability of the current and future cellular networks as an effective RAT for the IoT [6], [7].

It is worth mentioning that the traffic generated by the IoT is nothing like traditional phone-generated data, for which cellular networks are very well suited for. This traffic is mainly characterized by the transmission of sporadic small bursts of data that, in most cases, should reach the destination without an excessive delay. The large volume of aggregated traffic (considering the expected 10 billion of devices) and the sporadic nature and on-demand usage of the network, implies a heavy signaling overhead that can potentially hinder the performance of both, cellular network infrastructure and IoT devices [6], [8], [9].

This work has been supported by the project AIM, ref. TEC2016-76465-C2-1-R (AEI/FEDER, UE). Ruben M. Sandoval and Sebastian Canovas-Carrasco also thank the Spanish MECD for an FPU (refs. FPU14/03424 and FPU16/03530) pre-doctoral fellowship.

Conversely, cellular-oriented communication protocols, like LTE and the much-anticipated 5G, are geared towards faster, more stable transmissions of information that, indeed, can be of interest to certain situations -e.g. to transmit a daily report of an important asset, or in general, to deliver large packets-. For all other situations, and with the aim of maximizing network and cost efficiency, a promising suite of solutions that make use of the unlicensed ISM (Industrial, Scientific and Medical) bands is being extensively used as a RAT for the IoT. As one of the main key features of Smart Cities/Industries is the large areas to be covered, low-power wide area networks (LPWAN) technologies are called to be the de-facto mean of communication for those small and sporadic transferences of information. The distinguishing feature of LPWAN is the long-range radio links forming a star network topology, in which end devices (nodes) are directly connected to a collector device (gateway) that provides access to the IP network. These networks are designed to notably improve the battery life of nodes and support on-demand bursty traffic by reducing the signaling overhead to a minimum.

However, the main drawback of LPWAN technologies is its low bitrate. Depending on the technology and configuration, it fluctuates from one hundred bits per second to a few thousands of bits per second, potentially being insufficient for handling all the traffic generated by an IoT device. Such low bitrate is due to the modulation techniques employed in most LPWAN, that focus on being as much robust as possible against interferences and increasing the receiver sensitivity (depending on the specific technology, up to -150 dBm) to achieve large link distances. Therefore, a trade-off between data rate and sensitivity arises. For instance, in LoRa [10], one of the most popular LPWAN technologies, this trade-off can be tuned by the so-called Spreading Factor (SF) parameter, which controls the spreading of the signal. For larger values of SF, the sensitivity increases (achieving longer transmission distances) whereas the data rate decreases.

Furthermore, with the aim of reducing cost, most of these LPWAN work in ISM bands. Unfortunately, in many countries, these bands are subject to strong regional regulations. For example, in Europe, China and Japan, communication devices that do not provide Listen-Before Talk techniques cannot exceed a certain transmission Duty Cycle (DC) limit [11]. This value is defined as the percentage of time that a given device can transmit in a particular frequency band, usually measured over an hour. In Europe, the maximum DC for some bands is limited to 1%, that is, a node cannot occupy the channel for more than 36 seconds per hour [12]. To accomplish this restriction, after each transmission, LoRa nodes remain silent during a time period known as off-period (t_{off}). The duration of such t_{off} follows the expression: $t_{off} = \frac{t_{on}}{DC} - t_{on}$, where t_{on} stands for the duration of the transmission.

As can be seen, there are at least, two competing RATs that cannot, on their own, successfully support the traffic generated by the IoT, either due to a lack of specialization in sporadic traffic and very low energy consumption (cellular technologies) or to a low offered bitrate (LPWAN). Therefore, there is an increasing trend toward the use of multiple RATs in the IoT to minimize this problem. However, although many works look into employing heterogeneous RATs in wireless networks (as will be commented in the Related Work section), to the best of our knowledge, very few studies tackled this problem from a mathematical point of view –that is, how nodes optimally decide which RAT should be used at any given time–. With the interest of filling this gap, and by making use of the mathematical framework of Reinforcement Learning (RL), a subfield of Machine Learning (ML), we propose a mechanism to derive transmission policies that optimally determine the RAT to be employed for each transmission. These transmission policies consider the global state of the node and are oriented to maximize some predefined performance metric while being computable in very hardware-constrained devices.

Therefore, the contribution of this work is threefold: (i) a methodological and thorough justification for the need of multiple RATs in IoT-oriented 5G networks; (ii) a mathematical formulation that models performance of IoT nodes as an RL problem that truly embraces the nature of these devices; and (iii) the proposal of a state-of-the-art ML technique to solve such an RL problem and its analysis, via simulation, to highlight the importance of ML-oriented transmission policies in 5G deployments.

The rest of the paper is organized as follows. In Section 2, a review of the related work is presented. Next, in Section 3 we describe the positive impact of ML techniques to the problem under consideration and its importance to the future 5G standard. The mathematical framework is discussed in Section 4, where a generic RL-based model of nodes is formulated for an arbitrary number of RAT. Furthermore, in this section, a popular ML genetic algorithm is also proposed for deriving the optimal transmission policy. This generic model is particularized for IoT nodes endowed with multiple RATs in Section 5. Next, in Section 6, the proposed model is used to simulate IoT nodes fitted with two RATs: 5G and LPWAN. The ML-derived policy is compared to three other intuitive policies to further highlight the scope of application and benefits of our proposal. Finally, Section 7 concludes.

2. RELATED WORK

Nowadays, the wide variety of RATs available on the market (cellular networks, LPWAN, Bluetooth, WiFi, ZigBee, etc.) makes the idea of adopting a unique and normalized solution for IoT, a priori, an unfeasible approach. This is why, in the related literature, we can find different reviews and surveys comparing RATs, each with advantages and disadvantages. In [6], a complete survey about the enabling RATs for the IoT is conducted, paying special attention to the different LPWAN technologies available for long-range communications (LoRa, Sigfox, and Ingenu). Following a similar approach, in [13], an analysis of the potential RATs for IoT in a 5G ecosystem is performed. Short-range transmission technologies (ZigBee, Bluetooth, and Low-Power WiFi), LPWAN, and cellular networks from 2G to 5G are considered. The wide diversity of RATs available on the market is remarked, as well as the necessity for finding a way to combine them.

On the other hand, preliminary works about multi-RAT support for 5G can be found in the literature. Authors in [14] bring to light the need of heterogeneous Radio Access Networks (RAN) to alleviate the congestion and overload of the cellular infrastructure. The mixture of cellular networks with RATs working on ISM frequency bands, such as WLAN technologies, is proposed for the forthcoming 5G. This concept is also remarked in [15], where authors claim that the intelligent integration of WiFi and cellular networks can duplicate or even triplicate the quality of service and network performance.

In this framework, very few papers apply ML techniques to smartly optimize the access to the medium in 4G/5G for M2M communication. Authors in [16] proposed an RL-based algorithm for cellular networks that enables Machine Type Communication devices to cooperatively communicate to minimize the network congestion. This is accomplished by the intelligent selection of the base station to transmit from the device-side. The use of ML techniques is also exploited in [17], where authors introduced an ant-colony heuristic algorithm to smartly decide which RAT should be used by users. These decisions were made to maximize system utility and better balance resource utilization. The RATs considered were LTE, WiMAX, and WiFi and the results obtained showed a performance improvement between 20% and 70% with respect to other RAT usage strategies. However, none of these ML works consider the nature of IoT devices (low-power consumption and limited hardware resources) or the use of LPWAN technologies (which are known to be well-suited for IoT devices).

3. IMPORTANCE OF THE PROPOSED SOLUTION TO THE 5G STANDARDIZATION PROCESS

As shown in previous sections, the use of cellular networks is gathering momentum as an enabler for the IoT due to the need for global coverage in most user and industrial applications. This requirement can be met by employing the infrastructure of the Mobile Network Operators (MNO), which already offers an almost-global coverage. This solution also reduces the installation cost of IoT systems by avoiding the acquisition of specific equipment to connect IoT devices to the Internet. In this context, several efforts are devoted to make cellular networks more suitable for the IoT, leading to the emergence of the 5th Generation of mobile networks (5G). 5G is envisaged to adapt the advantages of cellular networks to the characteristics of the IoT, that is, massive number of devices, enabling lower end-to-end latency and energy consumption, and global coverage [7].

However, there are still some shortcomings that may delay the ubiquitous use of 5G in IoT. The first stems from the cost of using licensed frequency bands. Using such private parts of the spectrum entails a cost that may turn unaffordable as the number of deployed IoT devices grows; either due to the expenses derived from renting the infrastructure to the MNO or due to the direct cost of licensing the bands from the competent authorities. Even if data transmissions are sporadic, the total aggregated traffic of the network may render cellular-based IoT deployments hard to maintain in terms of operational costs. On the other hand, and although 5G is envisioned to reduce power consumption, cellular-based nodes are intrinsically dependent on signaling. This overhead in the communications unavoidably lead to an increase in power consumption of IoT devices [18].

Under these circumstances, the use of multiple RATs is one of the key tools of 5G deployments to benefit from the advantages of each wireless technology. However, the scientific community has focused on a set of supporting technologies (WiFi/WiMAX/mm-wave/etc.) potentially ill-suited to IoT devices [19], [20]. First, due to the large power consumption of such technologies (in particular when compared to LPWAN alternatives), and second due to the cost increase of their respective radio transceiver (especially for WiMAX/mm-wave and, again, when compared to LPWAN technologies such as LoRa). Furthermore, previous studies in this field have solely focused on alleviating network congestion, neglecting the intrinsic requirements of IoT deployments, that is, their low-cost and low-power nature.

As 5G ultimately aims to encompass a wide variety of traffic-generating devices, the authors believe that the future 5G standard releases should devote further efforts to acknowledge the limitations of IoT networks. In this paper we have made a step forward in this direction, by not only maximizing throughput of IoT nodes, but also considering potential restrictions in the usage of the different RATs (such as battery limitation, daily transference quota, etc.) In this sense, we believe, and have demonstrated in this work, that Machine Learning techniques can play an essential role in deriving optimal transmission policies for the future 5G. Therefore, we envisage that 5G could potentially benefit from this subfield of the Artificial Intelligence area and hence, should be paid more attention by the standardization bodies.

4. MATHEMATICAL FRAMEWORK

As discussed above, the objective of the policy-derivation algorithm is to determine which RAT should be used by an IoT device in any given situation. This can be translated into the RL jargon as determining the optimal action a to take (out of a set of $\boldsymbol{A}$ allowed actions, being $a \in \boldsymbol{A}$) given a state s (a description of the internal/external state of the IoT node, with $s \in \boldsymbol{S}$). Having performed action a in the state s, some *reward* is obtained -this feedback signal helps nodes understand what actions are better to take than others-. This reward can, for instance, measure how much information has been reported, how important such information was, etc. The function $\mathcal{R}$ mathematically defines such a reward as a mapping between state-action pairs and real numbers, that is, $\mathcal{R}: \boldsymbol{S} \times \boldsymbol{A} \to \mathbb{R}$.

After receiving some reward, that can be positive or negative, IoT nodes shift from one state to another, again, depending on the previous state-action pair. These transitions can be stochastic to allow RL entities to probabilistically transition from one state to another. Formally, $\wp$ models the transition from one state to another by mapping a tuple $(\boldsymbol{S}, \boldsymbol{A}, \boldsymbol{S})$ to a real number –representing the probability of transitioning from state s to state s' after taken action a–. That is, $\wp: S \times A \times S \to \mathbb{R}$.

The goal of RL algorithms is to find an optimal action policy (π^*) that maximizes the expected total reward obtained over some finite or infinite horizon (such accumulated reward is denoted as γ). In the former case, the reward is aggregated for T units of time -e.g. T seconds- whereas in the latter, it is the average reward per unit of time what it is maximized. Therefore, the objective of π^* is to, being the IoT node in a certain state s, propose an action a to take such as the total expected attained reward γ is maximized. Following the above formulation, an action policy π can be mathematically represented as a mapping between states and actions, that is, $\pi: S \to A$. This optimal policy can be implemented either as a tabular solution (i.e. for each state, a table stores the optimal action to take) or approximated by a function (i.e. there is a function that takes states as inputs and returns actions as outputs). When the process under optimization is relatively complex, the number of potential different states (the space of S) is too large to be tabulated. Being function approximators the only feasible alternative, and due to the recent successes of Artificial Neural Networks (ANN) in approximating functions, a plethora of ANN-based algorithms have recently emerged in the RL field. The basic idea is to have an ANN that, when fed with the current state of the RL entity (the IoT node in our case), it returns the most promising action to follow.

Among all ANN-based alternatives, Evolution Strategies (ES) [21] has recently demonstrated to be one of the best-suited alternatives to derive optimal policies; especially when the effects of the actions are long-lasting (that is, taking the action a at a given instant t has a measurable non-negligible effect at time t', with $t' \gg t$). ES is a type of Genetic Algorithm [22], a black-box optimization meta-heuristic loosely inspired in natural selection. By iteratively tweaking the parameters of the ANN via *natural selection*, the modeled policy π tends to improve in proposing actions to take.

5. APPLICATION TO THE PROBLEM

Let an IoT network monitor a set of critical assets with some parameters of interest. Such a network is, in turn, composed of IoT nodes provided with different RATs that can be used to report certain detected events. Thus, having detected an event, an IoT node must decide whether to report it or not. If it chooses to report it, it also has to determine which RAT to use. Thus, the set of all allowed actions $\boldsymbol{A}$ is composed of $\{a_0, a_1, \ldots, a_N\}$, where N is the number of allowed RATs to use, and a_0 models the action of not reporting but dropping the event. Each of these generated events can have a different priority (G). For instance, if a malfunction in a life-supporting device is detected, a top-priority event must be sent. Contrary, if a regular event is detected (such as mild vibrations in an engine), a low-priority event could be generated. Priorities are let to vary in a range from 0 to 1 to illustrate different event priorities –where 1 means top priority–.

To model the nature of wireless communications, each RAT may have a limit on its usage. This can be due to two different reasons: (i) a limit in the total expenditure allowed, e.g. per day, derived from using such technology –for example, IoT nodes may not be allowed to spend more than 1$ a day when using 5G transmissions–. Or (ii) a limit on the traffic generated by any given technology, this can be expressed in bytes (e.g. per day) or in packets –for example, Sigfox nodes cannot generate more than 140 packets a day [23], or nodes making use of cellular technologies may not generate more than 1Mb of traffic a day–. Therefore, when action a_i (with $i \neq 0$) is taken, the state s of the IoT mote changes since the usage of the technology i, denoted as u_i, is also updated. When the usage of technology i reaches its limit, u_i^{MAX}, such a technology is no longer available that day. Without any loss of generality, periods of 24 hours (1 day) are considered in limiting the usage of RAT.

Furthermore, each action/RAT entails a different energy consumption (denoted as c_i for action i). Since a single battery per node is assumed, if battery level (denoted as b) drops to zero, no further events can be reported. To complete the definition of the node state, the length (L) of the generated packet (created as a response to an arising event) must be considered. It should be noted that the event-generation process is modeled as a Poisson distribution with an average rate of λ events per second.

As commented in the Introduction, some LPWAN technologies, depending on the country, must undergo an enforced off-period (t_{off}) after every transmission. To model this and, at the same time, packet buffering capabilities, individual infinite queues are assumed to exist for each RAT (that is, there exist N different queues in each node). Therefore, the transmission time of a packet does not only depend on the length of such a packet (L) but also on the occupation of the queues (denoted as o_i for the i-th RAT). If an off-period of t_{off} seconds is enforced in an IoT node as a result of a packet transmission, the LPWAN queue of that node is not only filled with such a packet, but also artificially extended with another fictitious packet that would take t_{off} seconds to be transmitted. Note that this artificially generated packet has no impact on the obtained reward. Using this trick, we force nodes not to use the LPWAN RAT for, at least, t_{off} seconds -and thus, to comply with regional regulations-.

Finally, from the mathematical point of view, the state s of a node is the vector conformed by

$(L, G, b, t, u_1, u_2, \dots u_N, o_1, o_2, \dots, o_N)$. That is, the state is defined by the length of the generated packet, the priority of such a packet, the remaining battery of the node, the time of the day (t), the usage level of each RAT, and the occupation of their corresponding queues. When the above vector is fed into the ANN-based policy, an action that maximizes the expected total reward is obtained. In turn, we have mathematically modeled the reward obtained for each action as follows:

$$R(s, a_i) = G \cdot \frac{L}{delay(a_i)}$$

The reward is modeled as the priority multiplied by the length of the transmitted packet (in bits), divided by the delay in the transmission. This way, nodes are encouraged to report events as fast as possible, while prioritizing their importance. The units of this reward are bits per second, which match the units of a throughput metric. Hence, what the reward function maximizes is the *prioritized* throughput of an IoT node. Note that the *delay* of the action a_i is not only related to the bitrate of the i-th RAT but also to the occupation of the queue of such a RAT. Also, since battery depletion prevents nodes from reporting more events (and hence, 0 reward is obtained from that point onwards), π^* naturally optimizes energy consumption as well.

6. SIMULATIONS AND RESULTS

To evaluate the mathematical framework and its solution via RL, we have simulated an IoT network in which nodes support two RATs (that is, $N = 2$): a cellular-based connection (this might represent future 5G cellular links) and a LoRa transceiver. Thus, a_1 and a_2 indicate the actions of using 5G and LoRa respectively. It is very common, and will be even more popular in 5G deployments, that parts of the licensed spectrum are sub-rented or even get offered in an auction-based fashion to third parties (this is the cornerstone of, e.g., cognitive spectrum applications in 4G/5G networks [24], [25]). These third parties may be, for example, operators of IoT networks or governments that need a wireless infrastructure for their Smart City initiatives. We have modeled this spectrum renting scheme and assumed that a sub-band of a wider licensed band is at the disposal of the IoT nodes, offering a transmission speed of 100kbps. For the LoRa connection, we assume that devices transmit with SF=7, and thus, have a throughput of 2.43kbps. Regarding band usage limitations, we limit to 1Mb per day the use of 5G networks (u_1^{MAX} = 1 Mb/day) to reduce operational costs. We do not set any daily restrictions on LoRa ($u_2^{MAX} = \infty$). To illustrate the impact of the off-period policies (imposed in most European countries) on the performance of IoT networks, we simulate two environments, one with such a policy enforced and one without it. Energy consumption of both RATs is taken from [26] and [27] for cellular and LoRa-based RAT respectively –as determining it is out of the scope of this work–. We assume that IoT motes are powered by two AA batteries designed to last, at least, for three years (i.e. the maximum allowed energy consumption for a day is $\frac{1}{1095}$ the total energy stored in such batteries, where 1095 is the number of days in three years). The average event-generation rate is varied between 1 packet every 30 seconds ($\lambda = \frac{1}{30}$) and 1 packet every 10 minutes ($\lambda = \frac{1}{600}$) to assess the influence of this figure on the total attained reward –these values are in-line with typical wireless monitoring networks [28]–[30]–. Furthermore, packets of varying sizes are assumed to be generated; specifically, lengths are randomly generated with uniform distribution between 30 and 200 bytes (being, again, in accordance with typical IoT deployments [11]. Similarly, priorities of packets are also uniformly distributed between 0 and 1. Finally, Table 1 specifies all considered parameters.

Table 1 – Parameters of the simulation

Parameter	Value
5G rate	100kbps
LoRa rate	2.43kbps
LoRa T_{off} (if applies)	$\frac{T_{on}}{DC} - T_{on}$ with $DC = 0.01$
5G usage limitation (u_1^{MAX})	1Mb/day
LoRa usage limitation (u_2^{MAX})	∞
5G power consumption (c_1)	2.15W
LoRa power consumption (c_2)	0.1353W
Battery of nodes (b)	2AA batteries (30780 joules in total, 28.1 joules/day)
Average events per second (λ)	Varied from $\frac{1}{30}$ to $\frac{1}{600}$
Packet length (L)	$U(30, 200)$ bytes
Packet priority (G)	$U(0, 1)$

Evolution Strategies algorithm has been allowed to run for 1000 iterations to iteratively tune the ANN-defined policy. This ANN is, in turn, composed of two hidden layers of 45 and 5 neurons with *tanh* as an activation function [31]. Figure 1 shows the training phase of the ANN-based policy. In this process the expected total reward obtained for a whole day (that is, γ) increases as the policy π improves by iteratively applying the ES algorithm. This illustrates that the obtained policy is being more and more refined to make IoT nodes act wiser. Note that transmission policies are trained off-line in more powerful computers while the practical use

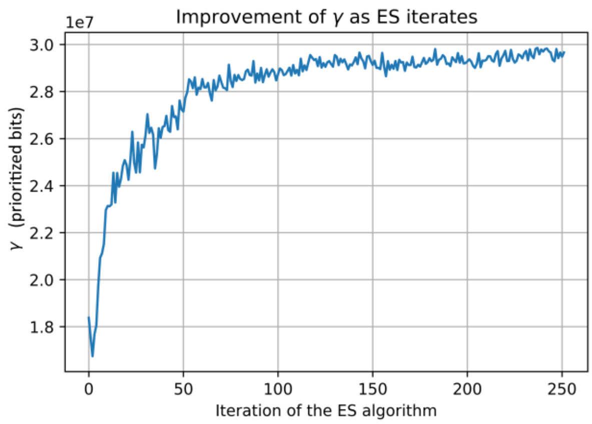


Figure 1 – Evolution of γ as ES algorithm iterates (first 250 iterations are shown). Obtained for $\lambda = {}^1/_{90}$ and off-period not enforced. Note that γ ultimately indicates the average number of prioritized bits transmitted in a day.

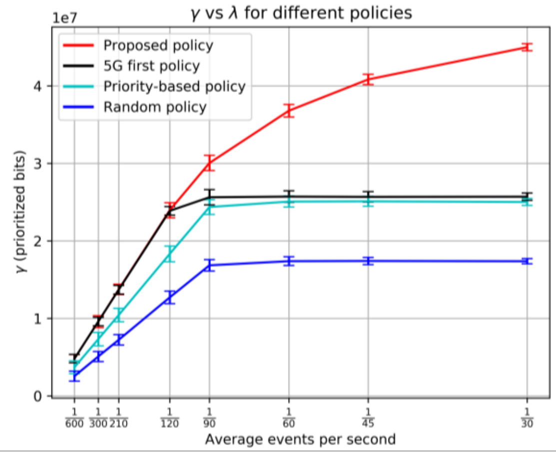


Figure 2 – Total reward (γ) as a function of the event-generation rate. Off-period not enforced. Error bars represent the standard deviation around the mean value.

of such policies is a light-weight process that simply entails a *forward pass* of the ANN (a task computationally viable even for very hardware-constrained IoT devices).

In order to further show the benefits of the proposed solution, the γ obtained under the proposed solution is compared to the γ obtained when three other policies are employed:

(i) randomly chose a RAT (5G/LoRa) –denoted as *random* policy–, (ii) start with 5G until its exhaustion and then use LoRa if necessary –denoted as *5G-first* policy–, and (iii) consider important events those with $G > 0.5$ and thus, only employ 5G for those critical transmissions (and employ LoRa when $G \leq 0.5$ or when 5G has been exhausted) – denoted as *priority-based* policy–.

Figure 2 depicts the obtained results for different values of λ. It is worth mentioning that, γ values obtained when an off-period is enforced after every transmission are remarkably close to those obtained when such limitation is not considered (differences are, in average, less than 0.047%). Therefore, due to space limitations, we have only included the results obtained when an off-period is not enforced. These small differences indicate that, for typical IoT event-generation rates (i.e. those evaluated in this simulation), forcing motes endowed with multiple RATs to undergo an off-period in their LPWAN transceivers, does not have a measurable effect on their performance. We argue that, if event-generation rate were dramatically increased (thus, forcing motes to transmit a larger number of packets), this forced off-periods may have a non-negligible effect. However, we also acknowledge that IoT nodes are not conceived, nor enabled to transmit at such excessive data rates (mainly due to their limited hardware and energy resources).

Regarding the results presented in Figure 2, it is worth noting how the ANN-based proposed policy clearly outperforms the rest of them when the event-generation rates are larger than $\frac{1}{120}$. Specifically, when the proposed policy is preferred over the second-best policy (*5G-first*), γ increases 75.6%, 59.0%, 43.1%, and 17.1% for the four highest event generation rates respectively. If λ is smaller or equal to $\frac{1}{120}$, the relatively low event-generation rates make the *5G-first* policy perform similarly to our proposal. For these small values of λ, employing the 5G RAT for all transmissions is always the best option, since neither the 5G daily quota nor the battery allowance exhaust; thus, both policies attain similar values of γ. As can be noted, ANN-based policy is properly adapted to different event-generation rates, always achieving an optimal performance. Unarguably, these results are subject to change when the 5G daily quota or the battery capacity changes; however, we believe that the main idea is adequately pinpointed: as nodes transmit more and more data, long-lasting technologies such as LoRa (both in terms of extending lifespans of the nodes and in their usage limitation) should be progressively embraced. Another interesting fact should be highlighted: if non-adaptive policies (such as *5G-first*, *priority-based*, or *random*) are applied, and the event-generation rates are relatively high ($\frac{1}{30}$ to $\frac{1}{60}$), it is the battery capacity the limiting factor in attaining larger values of γ. These rates make batteries deplete half-way through the 24-hour simulation, and thus, larger values of λ do not lead to larger values of γ for the three aforementioned policies. This reveals that, when designing transmission policies for hardware-constrained IoT devices with multiple RAT, it is the battery consumption, and not the bitrate of their

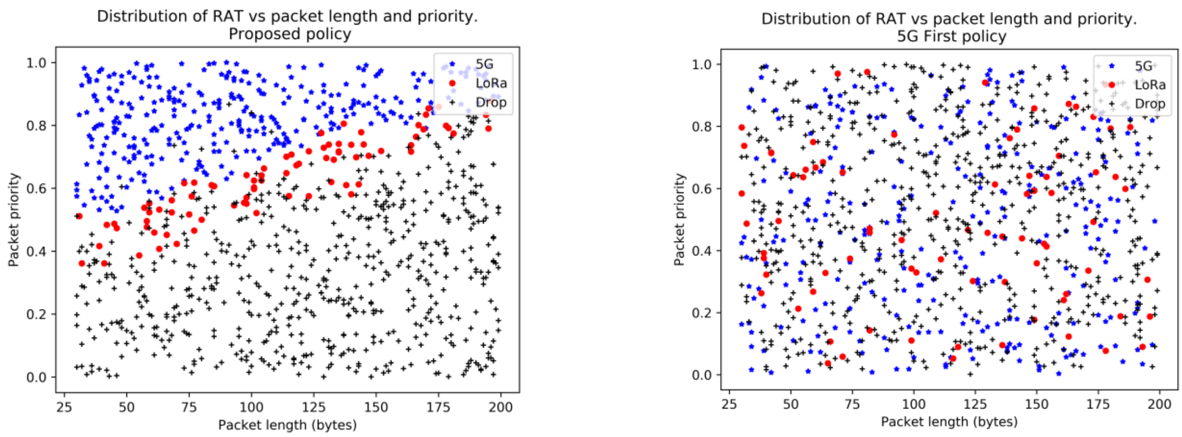


Figure 3 – RAT usage for the two best policies: the proposed one (left) and the *5G-first* (right) for 1000 packet transmissions. Obtained for $\lambda = {}^{1}/_{30}$ and off-period not enforced.

transceivers, the main limiting factor in increasing network performance. By carefully discarding non-critical events in more demanding scenarios (i.e. where larger values of λ are present), our proposed policy can get the most out of the allocated resources (battery and 5G daily quota) to maximize obtained rewards. Figure 3 corroborates this statement by analyzing the typical usage of each RAT made by our proposed policy and the *5G-first* policy. 5G transmissions are depicted in blue stars, LoRa transmissions in red circles, and discarded packets in black crosses. Two variables are analyzed: packet length and packet priority (the rest of variables are not shown for the sake of clarity, although they still play an important role in deciding on the RAT). Note how the proposed policy (left picture) tends to discard large non-important packets (shown in the bottom right side of the picture) while high-importance packets are normally transmitted via 5G-cellular links. LoRa is employed when either the packet priority is not high, the packet is relatively large or the 5G daily quota has been exhausted (this variable is not shown in Figure 3). Conversely, the *5G-first* policy disregards packet properties and makes an excessive early use of 5G transmission (note that there are far more blue stars than red circles) until 5G daily quota is exhausted and LoRa comes into play. Discarded packets are not prioritized by their importance and thus, there is a homogenous distribution of black dots.

The reason why the *priority-based* policy performs worse than the *5G-first* policy lies in the usage of the 5G RAT. The former tends to systematically underuse 5G, whose daily quota is not met even for the lowest values of λ (in such scenarios, it is the battery and not the 5G daily quota the limiting factor). Finally, the *random* policy makes the same mistakes as the *priority-based* policy while also disregarding event priorities; hence the lower attained γ.

7. CONCLUSION

5G has proved itself to be a future revolution in the way in which, not only users, but also machines could communicate with their peers. It is precisely in this type of communications (machine-to-machine) in which the IoT paradigm will play a major role. However, cellular networks may not be fully geared towards the very sporadic and bursty nature of IoT data transfers, and many authors have argued that IoT devices could potentially benefit from having multiple Radio Access Technologies (RAT). These RATs would be used intelligently and on-demand to access the wireless shared medium.

To evidence this, we have presented a mathematical model that lies the foundations for improving the performance of IoT devices fitted with multiple RAT. To optimize such a figure of merit, we have resorted to a set of analytical tools popularized by the Machine Learning (ML) research field. In particular, a Genetic Algorithm known as Evolution Strategies has been used to derive optimal transmission policies. These policies are shown to outperform other intuitive approaches in different simulated scenarios while still being computationally light-weight enough to run in hardware-constrained IoT devices. The solution based on an Artificial Neural Network (ANN) optimizes the use of the available RATs (5G and LoRa), leading to an improvement in the attained rewards of up to 75.6% when compared to other policies. Although the precise presented results depend on the parameters of the simulated network (and, deeply studying other scenarios is left as a future work), we truly believe that this work has served its purpose: to raise awareness about the potential use of ML techniques in deriving transmission policies that could make the future 5G standard feasible for the IoT revolution.

Furthermore, there are plans to extend the presented work with traffic traces generated from IoT devices –so that the derived ANN-based transmission policy can learn from real data–. Nevertheless, authors believe that the traffic generation patterns are in-line with actual IoT deployments (as indicated in the Simulation Section).

8. REFERENCES

[1] P. Kulkarni and T. Farnham, “Smart City Wireless Connectivity Considerations and Cost Analysis: Lessons Learnt From Smart Water Case Studies,” *IEEE Access*, vol. 4, pp. 660–672, 2016.

[2] R. Martinez-Sandoval, A. J. Garcia-Sanchez, F. Garcia-Sanchez, J. Garcia-Haro, and D. Flynn, “A comprehensive WSN-based approach to efficiently manage a smart grid,” *Sensors*, vol. 14, no. 10, pp. 18748–18783, Jan. 2014.

[3] F. Orfei, C. Benedetta Mezzetti, and F. Cottone, “Vibrations powered LoRa sensor: An electromechanical energy harvester working on a real bridge,” in *2016 IEEE SENSORS*, 2016, pp. 1–3.

[4] J. G. James and S. Nair, “Efficient, real-time tracking of public transport, using LoRaWAN and RF transceivers,” in *TENCON 2017 - 2017 IEEE Region 10 Conference*, 2017, vol. 2017–Decem, pp. 2258–2261.

[5] A. Orsino, G. Araniti, L. Militano, J. Alonso-Zarate, A. Molinaro, and A. Iera, “Energy Efficient IoT Data Collection in Smart Cities Exploiting D2D Communications,” *Sensors*, vol. 16, no. 6, p. 836, Jun. 2016.

[6] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, “Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios,” *IEEE Wirel. Commun.*, vol. 23, no. 5, pp. 60–67, Oct. 2016.

[7] M. Agiwal, A. Roy, and N. Saxena, “Next Generation 5G Wireless Networks: A Comprehensive Survey,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[8] A. Biral, M. Centenaro, A. Zanella, L. Vangelista, and M. Zorzi, "The challenges of M2M massive access in wireless cellular networks," *Digit. Commun. Networks*, vol. 1, no. 1, pp. 1–19, 2015.

[9] T. Wild, F. Schaich, and Y. Chen, "5G air interface design based on Universal Filtered (UF-)OFDM," in *2014 19th International Conference on Digital Signal Processing*, 2014, pp. 699–704.

[10] LoRa-Alliance, "LoRa," 2017. [Online]. Available: https://www.lora-alliance.org/. [Accessed: 22-Feb-2018].

[11] R. M. Sandoval, A.-J. Garcia-Sanchez, J. Garcia-Haro, and T. M. Chen, "Optimal policy derivation for Transmission Duty-Cycle constrained LPWAN," *IEEE Internet Things J.*, pp. 1–1, 2018.

[12] ETSI, "Final draft ETSI EN 300 220-1 V2.4.1 (2012-01)," 2012.

[13] M. R. Palattella *et al.*, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, 2016.

[14] W. H. Chin, Z. Fan, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," *IEEE Wirel. Commun.*, vol. 21, no. 2, pp. 106–112, 2014.

[15] N. Himayat *et al.*, "Multi-radio heterogeneous networks: Architectures and performance," *2014 Int. Conf. Comput. Netw. Commun. ICNC 2014*, pp. 252–258, 2014.

[16] M. Hasan, E. Hossain, and D. Niyato, "Random access for machine-to-machine communication in LTE-advanced networks: Issues and approaches," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 86–93, 2013.

[17] J. Li, X. Zhang, S. Wang, and W. Wang, "Context-oriented multi-RAT user association and resource allocation with triple decision in 5G heterogeneous networks," *China Commun.*, vol. 15, no. 4, pp. 72–85, Apr. 2018.

[18] P. Andres-Maldonado, P. Ameigeiras, J. Prados-Garzon, J. Navarro-Ortiz, and J. M. Lopez-Soler, "Narrowband IoT Data Transmission Procedures for Massive Machine-Type Communications," *IEEE Netw.*, vol. 31, no. 6, pp. 8–15, Nov. 2017.

[19] M. R. Palattella *et al.*, "Internet of Things in the 5G Era: Enablers, Architecture, and Business Models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, 2016.

[20] J. Navarro-Ortiz, S. Sendra, P. Ameigeiras, and J. M. Lopez-Soler, "Integration of LoRaWAN and 4G/5G for the Industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 60–67, 2018.

[21] T. Salimans, J. Ho, X. Chen, S. Sidor, and I. Sutskever, "Evolution Strategies as a Scalable Alternative to Reinforcement Learning," *ArXiv e-prints*, Mar. 2017.

[22] D. Whitley, "A genetic algorithm tutorial," *Stat. Comput.*, vol. 4, no. 2, pp. 65–85, 1994.

[23] R. Sanchez-Iborra, J. Sanchez-Gomez, J. Ballesta-Viñas, M.-D. Cano, and A. F. Skarmeta, "Performance Evaluation of LoRa Considering Scenario Conditions," *Sensors*, vol. 18, no. 3, 2018.

[24] X. Wang, Z. Li, P. Xu, Y. Xu, X. Gao, and H. H. Chen, "Spectrum Sharing in Cognitive Radio Networks #x2014;An Auction-Based Approach," *IEEE Trans. Syst. Man, Cybern. Part B*, vol. 40, no. 3, pp. 587–596, 2010.

[25] D. C. Parkes, L. H. Ungar, and D. P. Foster, "Accounting for Cognitive Costs in On-line Auction Design," in *Agent Mediated Electronic Commerce*, 1999, pp. 25–40.

[26] B. Dusza, C. Ide, L. Cheng, and C. Wietfeld, "An accurate measurement-based power consumption model for LTE uplink transmissions," in *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2013, pp. 49–50.

[27] L. Casals, B. Mir, R. Vidal, and C. Gomez, "Modeling the Energy Performance of LoRaWAN," *Sensors*, vol. 17, no. 10, 2017.

[28] D. Bankov, E. Khorov, and A. Lyakhov, "Mathematical model of LoRaWAN channel access," in *18th IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, WoWMoM 2017 - Conference*, 2017, no. 15, pp. 1–3.

[29] D. Bankov, E. Khorov, and A. Lyakhov, "Mathematical model of LoRaWAN channel access with capture effect," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017, vol. 2017–Octob, no. 14, pp. 1–5.

[30] B. Afzal, S. A. Alvi, G. A. Shah, and W. Mahmood, "Energy efficient context aware traffic scheduling for IoT applications," *Ad Hoc Networks*, vol. 62, pp. 101–115, Jul. 2017.

[31] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Proceedings of the thirteenth international conference on artificial intelligence and statistics*, 2010, pp. 249–256.

MESSAGE COLLISION IDENTIFICATION APPROACH USING MACHINE LEARNING

Juan Pablo, Martín[1]*; Bruno, Marengo*[1]*; Juan Pablo, Prina*[1]*; Martín Gabriel, Riolfo*[1]

[1]GICom, Facultad Regional San Nicolás - Universidad Tecnológica Nacional, Argentina

ABSTRACT

Machine learning algorithms, in particular k-nearest neighbors (kNN) and support vector machine (SVM), are employed to estimate the potential success in decodifying ADS-B messages in highly congested areas. The main aim of this study is to optimize automatic dependent surveillance-broadcast (ADS-B) reception on-board low Earth orbit satellites. In this first approach, simulations are performed to obtain the training and testing signals. First, ADS-B communication system is described; second, machine learning, kNN and SVM are introduced. Third, the developed simulator is presented and the kNN and SVM algorithms are described with its results. Finally, the performance of these two is compared.

Keywords - Automatic Dependent Surveillance-Broadcast, Support Vector Machine, k-Nearest Neighbours

1. INTRODUCTION

Low Earth orbit (LEO) satellites have been widely used for both voice and data communications since many years ago[1]. After the disappearance of the flight MH370, the terrestrial ADS-B system was studied in order to extend its coverage. To achieve that, the reception of those signals on-board LEO satellites was first studied at the International Telecommunication Union (ITU)[2].

In 2015, ITU included the agenda item 1.10 to the World Radiocommunication Conference 2019 (WRC-19) with the subject "Studies on spectrum needs and regulatory provisions for the introduction and use of the Global Aeronautical Distress and Safety System". Furthermore, the Conference Preparatory Meeting 2019 invited the ITU Radiocommunication Sector and Working Party 5B "... to conduct the relevant studies, taking into account information and requirements provided by ICAO for both the terrestrial and satellite components, including: a) quantification and characterization of radiocommunication requirements related to GADSS..."[3].

The main purpose of this study is, with the aid of machine learning techniques, to estimate if a given ADS-B message was collided or if it is possible to decode its information on-board satellites.

The study is based on a simulator that recreates the reception of position messages on-board satellites in high air traffic density conditions.

1.1 Considerations on ADS-B Satellite Reception

ADS-B is a communication system that operates at 1 090 MHz, and based on data from an aircraft's on-board systems, transmits its position and status. That frequency range is shared with other International Civil Aviation Organization (ICAO) and non-ICAO standardised aeronautical applications. Extending the coverage of existing terrestrial receptors of ADS-B signal by a satellite network needs different analysis from many perspectives, using as many methods as possible.

While it is possible to use a LEO satellites or other types of non-geostationary satellites to receive ADS-B signals, there are some operational considerations to be taken into account. It is needed to de-garble the ADS-B signals from other aeronautical systems signals operating in the same frequency band (undesired signals), such as replies to secondary surveillance radar (SSR) interrogations, DME and tactical air navigation system (TACAN). Even further, depending on the region, there could be a great number of planes emitting messages at the same time, so the objective of this study is to provide an algorithm that is able to detect when a message from an aircraft can be successfully decoded.

1.2 Detection Problem

The general detection problem can be written as:

$$\begin{cases} \omega_0 : x = b & \text{hypothesis: noise} \\ \omega_1 : x = b + s & \text{hypothesis: identifiable signal} \end{cases} \tag{1}$$

The objective is then to be able to detect whether the received signal is only noise, or if it contains information. Therefore a detector d is built such that the following error probability is minimized.

$$P_e(d) = p\left(d(\boldsymbol{X}) \neq Y\right) \tag{2}$$

The classical hypothesis testing problem is a method of statistical inference, which, in fact, is the process of using data analysis to deduce properties of an underlying probability distribution[5]. A dataset obtained by sampling is compared against a synthetic dataset from an idealized model following:

$$\begin{cases} H_0 : X \in \omega_0 & X \sim p(X \mid \omega_0) \\ H_1 : X \in \omega_1 & X \sim p(X \mid \omega_1) \end{cases} \tag{3}$$

The distribution of the random process $\boldsymbol{X}$ has to be known to use the former method, but this is usually not possible. In

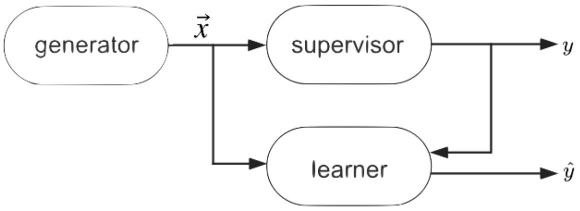


Figure 1 – Learning model

such cases, another method must be employed in order to get successful results.

1.3 Machine Learning

Machine Learning is one of the most active research areas within Artificial Intelligence. It consists of constructing learning systems that use a large amount of past data to infer solutions for new problems. In other words, this is done by analyzing a training dataset and using that information to predict behaviour, values or make a decision upon new data.
Supervised Machine Learning refers to learning algorithms that extract specific features from the training dataset to approximate the mapping function that relates an input variable to an output variable. A common supervised learning problem is a classification problem, where the output is a category and the input variable should be classified. Two supervised learning methods used as classifiers are support vector machines (SVMs) and k-nearest neighbors (kNNs).
The learning model is composed of three elements as shown in Fig. 1. A random variables generator that generates samples $x \sim \boldsymbol{X} \subset R^l$ of dimension l, feeds the supervisor and learner. Also, the learner needs to be filled with the output of the supervisor $y \sim \boldsymbol{Y} \subset R$, to estimate $\hat{y}$.

1.4 Feature extraction

The input data of a specific problem is usually too large to be processed, and also redundant. In order to solve this, the input data can be turned into a reduced representation set of features. When the features are carefully chosen, the representation has relevant data and gathers the desired information. By this method, it is possible to perform the desired task using reduced information, and make the algorithm more efficient.
Generally a complex analysis of data with large number of variables require a large amount of memory and computational power. Furthermore, too much information may cause a classification algorithm to poorly generalize new samples by overfitting to the training samples. By using feature extraction, these problems can be solved[11].

1.5 k-Nearest Neighbors

The k-Nearest Neighbors (kNN) search is a generalization of the optimization problem of finding the closest point to a given point in a determined set. This algorithm classifies the point by counting from which class are the k-nearest training points in the feature space (see Fig. 2). The classes do not need to be linearly separable, and the boundary between them

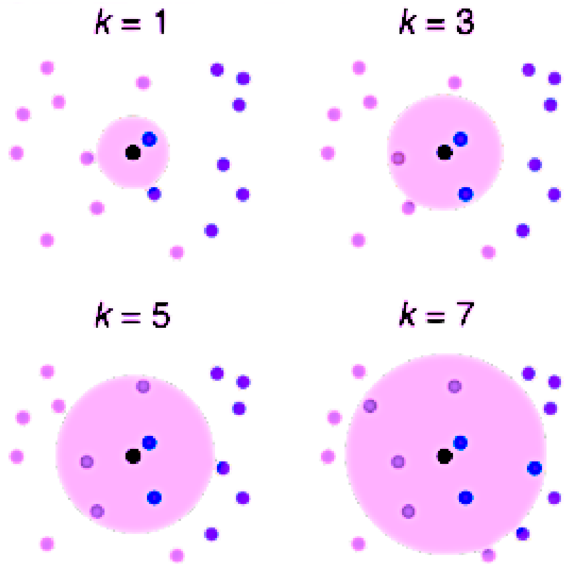
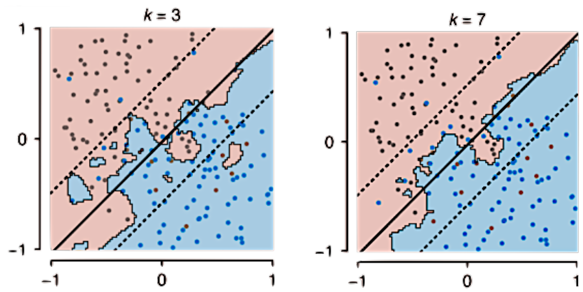


Figure 2 – Example of finding k near neighbours.



(a) Boundary using 3 neighbours.

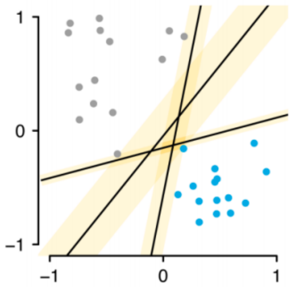
(b) Boundary using 7 neighbours.

Figure 3 – Effect of choosing different k.

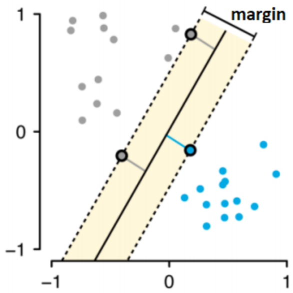
can be chosen as close as needed. However, this could lead to problems in the stability of the predictions, as shown in Fig. 3a and 3b.
The training phase of the algorithm consist of storing vectors in a multidimensional feature space, labeling them with classes. These vectors are generated with the training samples. Then, in the classification phase, an unlabeled vector, is assigned to the class which is most frequent among the k closest training samples to that point. Euclidean distance is a commonly used distance metric for continuous variables.
The choice of k impacts on the classification result. Depending on the problem, and specially on the nature of the data, larger values of k can reduce the effect of the noise on the classification, but it could cause wrong predictions between less distinct classes. Moreover, it is helpful to choose an odd k if it is a binary classification problem in order to prevent ties[9].
For multi-class kNN classification, it is proved an upper bound error rate of:

$$R^* \leq R_{kNN} \leq R^* \left(\frac{2 - MR^*}{M - 1} \right) \qquad (4)$$

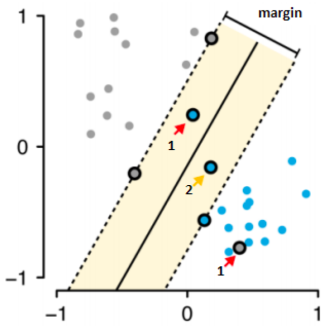
where R^* is the Bayes error rate, R_{kNN} is the kNN error rate,



(a) Linearly separable classes.



(b) Maximum margin.



(c) Margin violation and misclassification.

Figure 4 – SVM using a linear classifier

and M is the number of classes in the problem.

1.6 Support Vector Machine

When the classes are linearly separable, a straight line can be drawn that perfectly separates the classes and the margin is the perpendicular distance between the closest points to the line from each class as seen in Fig. 4a. This method is called Support vector Machine (SVM)[12]. Nevertheless, many possible separating lines exists that separates the classes and SVM finds the one with the widest margin (Fig. 4b). If the dimension of the sample is greater than three, the separating line becomes and hyperplane. The closest samples to the margin, or the ones that violates are called support vectors and are the only samples that are considered to define the separating hyperplane[7].

When the classes are linearly separable, the wider the margin, the confidence in the classification is higher because it indicates that the classes are less similar. Usually, it is difficult to obtain samples or data sets that are linearly separable and any separating hyperplane will not be useful. It is said that the margin is violated by a sample whether it is beyond the separating hyperplane as shown in Fig 4c with arrows marked as ‘1’. Also, the case where the samples are on the correct side, but are inside the margins has to be considered and an example is marked with the arrow and ‘2’ in Fig. 4c.

To take into account violations, penalty is considered proportional to the distance between each violating sample and the corresponding margin. Then the problem is reduced to the minimization of the risk::

$$1/\rho + C\sum \xi_i \qquad (5)$$

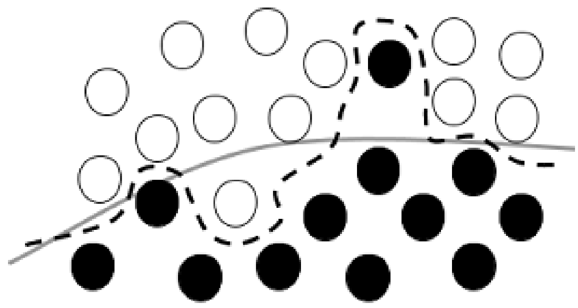


Figure 5 – Overfitted samples

where ρ is the margin width, ξ_i is the cost paid of the ith violating sample and C is a parameter that enables to tune the tradeoff between the width of the margin and the amount of violating samples.

If C is large, there will be fewer training errors, meaning that fewer samples from the training set will be misclassified, also known as overfitting. When overfitting occurs, as shown by the dashed line in Fig. 5, classes are perfectly separated, but the separation is greatly influenced by noise, potentially leading to greater classification errors.

On the contrary, when C is small, there will be more misclassified samples, but the margin will be greater, as showed by the grey continuous line in Fig. 5. To improve the final result of the algorithm this parameter has to be chosen using cross-validation[8].

1.7 Comparison

The selection of the best algorithm heavily depends on the nature of the problem and the features used. Nevertheless, SVM is less computationally demanding than kNN and is easier to interpret but can identify only a limited set of patterns. On the other hand, kNN can find very complex patterns but its output is more challenging to interpret[6].

2. TRAINING SIMULATOR

A simulator was developed in order to model the received signals on-board a LEO satellite and, by using machine learning algorithms, determine whether the messages can be decodified. In the machine learning model (Fig. 1), this simulator is the generator as it creates the signal x and also the supervisor as it labels the data (y signal).

2.1 Signal Generator and Supervisor

An ADS-B message consists of a preamble of $8\mu s$ and a data block of $112\mu s$. The message is Manchester-coded, meaning that each bit is represented with two states (high and/or low) that last half a bit time (see Fig. 6). Finally, the signal is modulated using on-off keying (OOK).

Each plane transmits messages with random periodicity with mean of $161ms$ (i.e. 6 messages every second), to avoid synchronized collisions with other aircraft.

In order to set the scenario, aircraft-to-satellite distances were randomly generated considering 1000 planes uniformly distributed in the footprint of a LEO satellite orbiting at

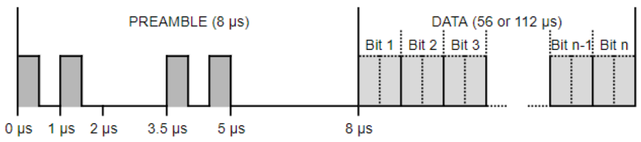


Figure 6 – ADS-B Signal.

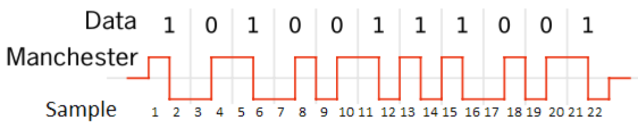


Figure 7 – Manchester codification.

$400km$ above the earth surface. A specific gain was assigned to each aircraft-to-satellite channel[10]. For the simulated period of time, the gain for each channel was considered constant. Neither Doppler effect, nor phase rotation of the signal were considered in this study. Finally, white gaussian noise was added to the signal.
The resulting signal models the demodulated RF signal that contains all the messages received on-board the satellite during the simulation time. Two samples per bit time were taken, resulting in a test signal of 760000 samples.
Two classes were defined based on whether the message could be decodified or not. This mainly depended on the received power of that message -e.g. a received power above the receiver's sensitivity- and on if there were collisions between messages with comparable power.

3. ADS-B SIGNAL FEATURE EXTRACTION

In order to generate the feature vector, samples of the same length of the data block of one ADS-B message, were taken. Then, the means of consecutive pair of samples starting from the first one, and starting from the second one were computed. For example, in Fig. 7, one set would have the means of samples 1 and 2, 3 and 4, etc., while the other set would have the means of samples 2 and 3, 4 and 5, etc.
After that, the variance of each set was calculated. Continuing with the example in Fig. 7, the variance of the means of the first set would be zero. The two chosen features were the greatest and the smallest value of the two variances and were arranged in a vector.
This process was done for every sample of the signal to generate the vector $\vec{x}$ containing the value of the two features for each sample.

4. MACHINE LEARNING CLASSIFICATION

Once the vector $\vec{x}$ and the labels y were obtained, they were introduced into a kNN classifier and a SVM. The performance was recorded with the error probability P_e as key indicator and time/computational consumption as secondary one.
Moreover, both methods needs parameters depending on the chosen structure. As there is no rule to chose them, many techniques are usually employed. For this study, k-fold cross-validation method was chosen as is widely used. In k-fold cross-validation, part of the original samples are used as training data, and the remaining subset of samples to test

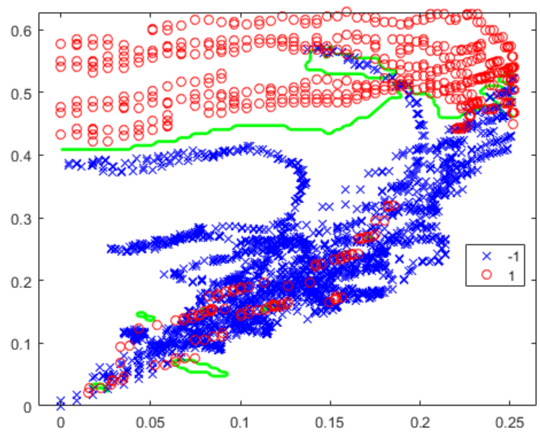


Figure 8 – 11NN Classification results.

the model. The partition of the samples is randomly chosen and this process is repeated k times. In order to obtain a single estimation, the k results are averaged. Furthermore, all observations are used for both training and validation, and each one only once for validation. k is an unfixed parameter and usually, 5-fold cross-validation is used.[13].

4.1 kNN Method Performance

The only parameter that had to be chosen for this method was k, the number of neighbours considered.
As previously detailed, to choose the optimal k (the one that committed fewer errors), k-fold cross-validation method was employed. It was obtained a $P_e = 0.059$ for $k = 11$.
As there is no actual learning process before the search, the complete training dataset was one of the inputs of the machine and could not be reduced. It is important to be aware that every search takes non-neglectable time to compute its result, even when code optimization techniques are applied.
The contour for this method is shown in Fig. 8.

4.2 SVM Method Performance

For this method, two main parameters had to be set; C of eq. *(5)* and the kernel used. For this approach, a Gaussian kernel was chosen. The only additional parameter required by the kernel was σ or the bandwidth.
Once again, using k-fold cross-validation the optimal $C = 11 \times 10^5$ and $\sigma = 0.0433$ were obtained. Training the SVM classifier with those parameters, the performance regarding the error probability was $P_e = 0.049$.
Furthermore, despite that the training phase took an important amount of time, the classification of every new sample could be done very fast or with little computational effort.
The contour for this method is shown in Fig. 9.

4.3 Performance Comparison

To evaluate the two studied methods, results were condensed in table 1. Comparing those results with similar studies [14] [15] [16], kNN or SVM performed better, under the spacial ADS-B circumstances.

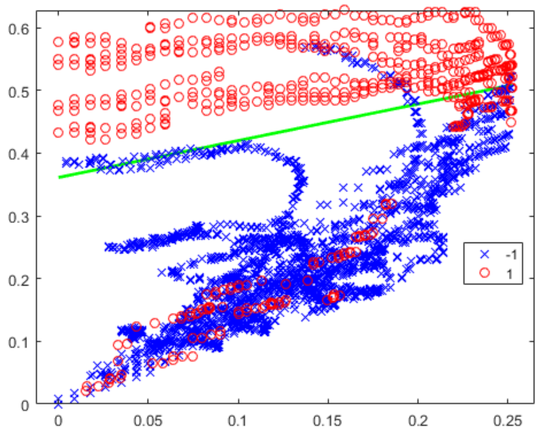


Figure 9 – SVM Classification results.

Table 1 – kNN vs. SVM

Method / Indicator	kNN	SVM
P_e	0.059	0.049
Classification	Slow	Very fast
Training time	No training time	Time consuming

5. CONCLUSION

It is shown that, under the hypothesis stated, both methods perform with little difference. It is clear that SVM is about 1% better than kNN. Under that circumstance, other indicators have to be analyzed in order to define which method will be better.

One of the most important indicators is the time that takes to classify a new sample. In that case, SVM performs better. Nevertheless, if kNN is manipulated in order to obtain a single and simpler boundary, it can be approximated by a function, reducing computation complexity. But, in many cases that method is not applicable, especially when the dimension of the samples (i.e. the amount of features used) is increased.

Despite that the training time for SVM is important, this phase can be done offline, and once the system is trained, the classification process itself is fast.

Nonetheless, only one kernel was used to test SVM. The results show that a simpler kernel can be used, improving the performance of the method.

Finally, after some fine tuning, the SVM method proof to be the best choice for this problem.

5.1 Future Work

It is planned to further improve the signal modeling. This will be done by including phenomena such as doppler shift and phase shift. However, these additions to the model would only give more information and the performance would only increase. Thus, using the actual model, worst case in this sense is taken into account. Also, different scenarios can be modeled such as different aircraft densities and altitudes.

Furthermore, different strategies of pattern recognition and feature extraction could be considered to be certain that there is no other available method to this problem that performs better.

In addition, experimental tests have to be conducted in order to evaluate the actual performance of the algorithm. In future studies, the algorithm will be tested with a real signal received on orbit.

By accurately estimating the potential success in decodifying the received messages, a considerable amount of computational resources, and therefore power consumption is expected to be economized. Further studies should be carried out in this field, in order to confirm the impact of the use of these algorithms in a satellite's lifetime.

Furthermore, international recommendations can be developed including all the available information, simulations and experimental data already obtained. Those standards can be developed by organisms like the International Telecommunication Union and can aid in the design and implementation of spatial ADS-B receivers.

Moreover, the International Civil Aviation Organisation should regulate the mandatory use of ADS-B equipment and also make mandatory the use of tamper proof devices.

5.2 Potential Impact

The previous study presents a different way to deal with the, already known, problem of receiving ADS-B messages in congested airspaces. Using machine learning and pattern recognition methods is a novel analysis that can increase the amount of messages that a receiver could decode. This new technique can contribute to International Recommendations and Standards to improve them, not only in a particular assumption, but also in the way that parameters are chosen.

If the addition of this method makes the system more efficient, the lifespan of the satellites will be improved due to reduction in energy consumption. Consuming less energy not only impacts on the battery depth of discharge, but also makes the satellite cheaper due to smaller electronic parts. Therefore, using machine learning techniques could potentially reduce the overall cost of satellite missions carrying ADS-B receivers.

Making ADS-B a standard real-time global solution for civil flight tracking enables safer flights and thus a potentially increase the aircraft density.

REFERENCES

[1] R. Cochetti, "Low Earth Orbit (LEO) Mobile Satellite Communications Systems," Wiley Telecom, pp. 264, 2015.

[2] ITU-R WP5B, "Reception of automatic dependent surveillance broadcast via satellite and compatibility studies with incumbent systems in the frequency band 1 087.7-1 092.3 MHz," Recommendation M.2413-0, International Telecommunication Union Radiocommunication Sector", 2017.

[3] ITU BR Director, "Results of the first session of the Conference Preparatory Meeting for WRC-19 (CPM19-1)," International Telecommunication Union Radiocommunication Sector", 2015.

[4] E. Valovage, “Enhanced ADS-B research,” 25th Digital Avionics Systems Conference, IEEE/AIAA, pp. 1-7, 2006.

[5] G. Upton,I. Cook, “Oxford Dictionary of Statistics,” OUP, ISBN 978-0-19-954145-4, 2008.

[6] D. Bzdok, M. Krzywinski, N. Altman, “Machine learning: Supervised methods, SVM and kNN,” Nature Methods, Nature Publishing Group, pp.1-6, 2018.

[7] T. Hastie, R., Tibshirani, J. Friedman, “The Elements of Statistical Learning,” Springer Series in Statistics, Heidelberg, 2001.

[8] J. Lever, M. Krzywinski, N. Altman, “Points of Significance: Model selection and overfitting,” Nature Methods 13, pp.703-704, 2016.

[9] B. S. Everitt, S. Landau, M. Leese, D. Stahl, “Miscellaneous Clustering Methods, in Cluster Analysis,” 5th Edition, John Wiley & Sons, Chichester UK, 2011.

[10] J. P. Martín, B. Marengo, J. P. Prina, P. López, M. Folonier, M. Podestá, M. Riolfo, G. Gonzalez, “Aircraft to Low Orbit Satellite L Band-Link Characterization,” IEEE Argencon 2018, 2018.

[11] E. Alpaydin, “Introduction to Machine Learning. London,” The MIT Press, pp. 110, 2010.

[12] N. Cristianini, J. Shawe-Taylor, “An Introduction to Support Vector Machines and Other Kernel-based Learning Methods,” Cambridge University Press, 2000.

[13] G. James, D. Witten, T. Hastie, R. Tibshirani, “An Introduction to Statistical Learning: with Applications in R,” Springer Texts in Statistics, Springer, 2017.

[14] H. Zhao,B. Zhao, Quan-Houde, Y.-P. Zhang, “Source Number Estimation Methods Base On Support Vector Machine Algorithm,” PACIIA 2009 - 2009 2nd Asia-Pacific Conference on Computational Intelligence and Industrial Applications, pp. 272-275, 2009.

[15] Z. Qiu, Zi. He, M. Cui, “A method for signal source number estimation based on MUSIC algorithm,” 2015 IEEE International Conference on Communication Problem-Solving (ICCP), pp. 344-346, 2015.

[16] W. Hu, R. Liu, X. Lin, Y. Li, X. Zhou, X. He, “A deep learning method to estimate independent source number,” 2017 4th International Conference on Systems and Informatics (ICSAI), pp. 1055-1059, 2017.

OPTICAL FLOW BASED LEARNING APPROACH FOR ABNORMAL CROWD ACTIVITY DETECTION WITH MOTION DESCRIPTOR MAP

Dhananjay Kumar, Govinda Raj Sampath Sarala

Department of Information Technology, Anna University, MIT Campus, Chennai

ABSTRACT

Automated abnormal crowd activity detection with faster execution time has been a major research issue in recent years. In this work, a novel method for detecting crowd abnormal activities is proposed which is based on processing of optical flow as motion parameter for machine learning. The proposed model makes use of magnitude vector which represents motion magnitude of a block in eight directions divided by a 45 degree pace angle. Further, motion characteristics are processed using Motion Descriptor Map (MDP), which takes two main parameters namely aggregate magnitude of motion flow in a block and Euclidean distance between blocks. Here, the angle of deviation between any two blocks determines which among the eight values in the magnitude vector to be considered for further processing. The algorithm is tested with two standard datasets namely UMN and UCSD Datasets. Apart from these the system is also tested with a custom dataset. On an average, an overall accuracy of 98.08% was obtained during experimentation.

Keywords – Optical flow, Euclidean distance, K-means, Angle of deviation

1. INTRODUCTION

In the recent years, there has been considerable interest on computer vision to identify human activities and detect abnormal scenarios from video input. It has been established that with the increase in the number of security cameras, the efficiency and accuracy of human operators have reached the limit. The automated system not only need to detect and locate abnormal behavior in real time, but also notify the agent through a report. The design and implementation process is challenging due to lack of specific knowledge of the scene and target activities. Abnormal activity detection may differ from suspicious activity detection. An activity if not been previously trained in the system, will be recognized as abnormal. But this activity may or may not be suspicious depending on the human perception.

Many approaches have been adopted for global unusual activity detection by modeling the behavior of the crowd itself. In some early approaches crowd behaviors are described by means of the Social Force model [1-2], with no human detection or tracking processes involved. The interaction force is measured by computing the difference between the desired and actual velocities obtained from the particle advection on the optical flow field. The major drawback of these systems is that the social force optical flow features are directly used to detect patterns, which may lead to poor accuracy as even slight deviation from normal may be detected as abnormal. Social behavior using interaction energy potential [3] could be considered in activity detection. The interaction energy potential is estimated from the velocity of the space–time interest points to explain whether they will meet in the near future.

Deep learning technique can also be used to anomalous event detection. However, there is a need for a model that trains a convolutional neural network (CNN) using spatiotemporal patches from optical flow images as input [4]. Even though these methods produce state of the art results, computation complexity is very high and hence it takes a lot of time to process the results.

The proposed framework work (Fig. 1) to detect abnormal behavior (event detection) in the scene, confirm to intelligent video surveillance system mentioned in ITU-T recommendation F.743.1 – "Requirements for intelligent visual surveillance". The output of alarm is based on polygonal region demarcated by the user. The basic requirement in F.743.1 is: when the retention time of an object in polygon area exceeds a prescribed threshold, an alarm needs to be triggered. The fraud detection system builds a profile of normal activity and uses a behavior analysis function to send alerts on deviations.

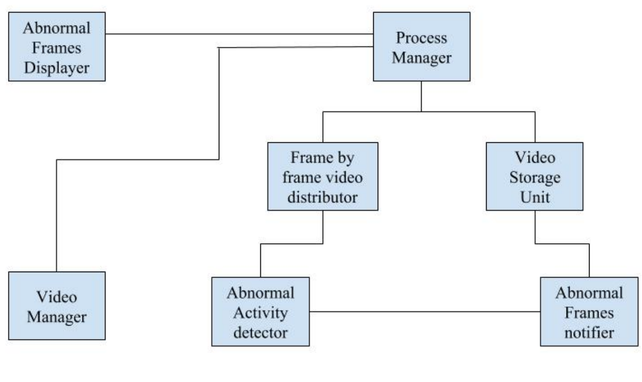


Figure 1 - Functional components of the abnormal activity detection system

As per the ITU-T recommendation X.1157 – "Technical capabilities of fraud detection and response for services with high assurance level requirements", behavior profiling employs a learning phase that builds profiles of normal activity for discrete event sources collected by monitoring capabilities. The proposed system is implemented in a desktop environment and tested with standard data set and also in a locally defined scenario, which can be used further in standardization of future intelligent surveillance systems.

2. RELATED WORKS

2.1. Statistical and Probabilistic Methods

In abnormal activity modeling and prediction, many techniques are based on Gaussian Mixture Model (GMM) and Hidden Markov model (HMM). In [5], a multilevel HMM is used to predict anomalous events in specific regions of the crowd. Markov models allow the analysis of the scene [6-7]. The expectation maximization algorithm [2] has been also employed as a predictor for anomaly. A two levels of feature analysis and Gaussian regression process can employed to improve performance [8]. However, a robust approach can use a hierarchical mixture of dynamic textures to describe the frame [9].

Many group modeling approaches [10-11] were proposed in recent years which used Gaussian process, codebook, bag of features (BOF) etc. Some anomaly detection frameworks used spatio-temporal system context [12]. They presented instant behaviors of a single object using an atomic event, which contained the location, sense of movement, and velocity of an object. Because of the huge fluctuations in appearance, scale, lighting, and pose, it's hard to detect or track individuals in crowded scenes.

A probabilistic framework can be used for automatically interpreting the visual crowd behavior using crowd event detection and classification in optical flow manifolds (OFMs)[13].

2.2. Context based methods

Behaviors differ radically from one place to another, since a human activity that is considered abnormal in one scenario may be normal in another. To make the system detect context based abnormal behaviors has been an important goal to accomplish. A context based method [14] attempts to solve these problems by providing automatic detection of suspicious behavior that uses contextual information. The idea of using context space model for abnormal activity detection used by Xiang et al. [15] models both abnormal and normal behaviors. The main difficulty with this system is that all normal behaviors can't be accurately modeled. The major drawback of these works is that the system always needed a lot of contextual training to build the model.

The Structural Context Descriptor (SCD) [16] can be used for describing the crowd individual. By online spatiotemporally analyzing the SCD variation of the crowd, the abnormality is localized. Tracking individuals in the crowd to detect abnormal activities performs good to identify individual abnormal activities like single person running in a place where running is abnormal. But for identifying group behaviors like panicking, convergence or divergence movements, their algorithm lags behind.

2.3. Generalized Methods

Generalized abnormal detection approach has performed well in terms of both accuracy and efficiency. They are also target towards implementation in real time. Approaches such as HOFME [17] HOFM [18] for detecting anomalous events in crowded scenes used general concepts such as orientation, magnitude and entropy which overcomes the difficulty to create models due to their unpredictability and their dependency on the context of the scene. The main drawback of these modals is that, they consider the overall magnitude of the block to be processed. Here, if the momentum within the block is not unidirectional, then it may affect the accuracy by detecting wrong blocks.

3. PROPOSED WORK

The proposed model is composed of training and detection phases. In training phase, the normal patterns are clustered, whereas during detection phase, if they differ significantly from the normal patterns learned, they are considered as abnormal. There are four major modules in the system namely optical flow of blocks computation, motion descriptor computation, motion descriptor pattern clustering, and nearest neighbor search. Figure 2 shows the overall flow of the proposed model. The particle movements in the video input are captured using optical flow. The extracted optical flow is passed to a magnitude vector computing

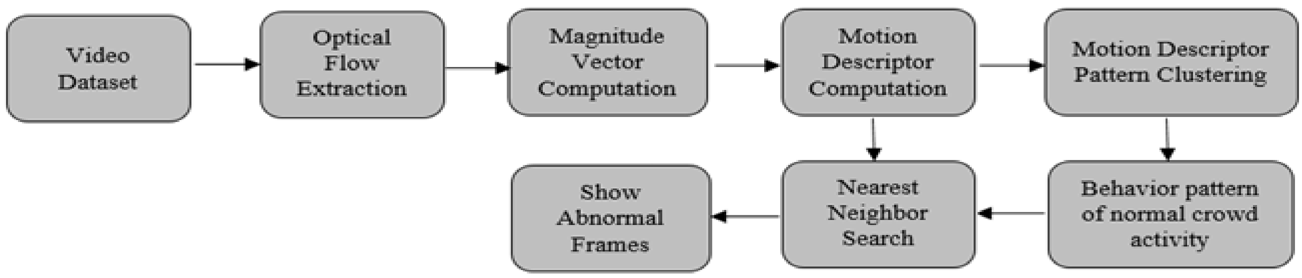


Figure 2 - Overview of the proposed model for abnormal crowd activity detection

module where each frame is divided into uniform blocks and optical flow magnitude of each blocks are calculated in different directions. Then, maximum magnitude in the block is taken as threshold value and the magnitude of the particles in other blocks pointing towards the block is taken for computing the influence weights. Similarly for every frame in the video, influence weight is calculated and stored in Motion Descriptor map. The generated motion descriptor map is used for training the system by *k*-means clustering algorithm which clusters the motion descriptor map based on the influence weights as data points. For each block separate clusters are formed.

3.1. Magnitude Vector Computation

The video dataset is split into individual frames for processing them in a sequential manner. Each frame is analyzed specifically for every moving pixel and it is being identified as individual particle. The optical flow is more effective in calculating the displacement between all frames which takes brightness as its pattern. Each particle has individual magnitude and directions which are all the properties by which a particle differs from an idle pixel. Individual frame in video dataset is divided into uniform blocks. Block classification is more efficient than object classification as it is faster and computation of foreground extraction is not needed. In addition, object classification needs trajectory extraction which is a complex task but it is as effective as block identification. In block detection, unwanted object movements may collide as noise and it is a challenging task to be eliminated. Our current approach is based on a block size of 8x6 which is fixed for maintaining an accurate performance state.

For every block magnitude vector of size 8 is assigned and magnitude of particles moving in a 45^{o} pace are added together to represent the magnitude of the block as eight octant in terms of direction. For instance, magnitude of particles with direction of motion between 0^{o} and 45^{o} are added together and the resultant value occupies b_i^0 where b_i represents magnitude vector of the ith block. An individual block in frame with particles with different magnitude and direction is depicted in Figure 3(a) and 3(b) showing the particles pointing to similar direction.

The particles pointing towards similar directions are grouped together and total sum of magnitude of all particles in each group is calculated and stored in an array. Maximum value in array is selected as the threshold magnitude of the block. The magnitude of the block b_i^k in direction k is calculated as,

$$b_i^k = \sum_{p_d = k.\pi/4}^{(k+1).\pi/4} p_m \tag{1}$$

where p_d represents direction of motion of a particle and p_m represents magnitude of the particle.

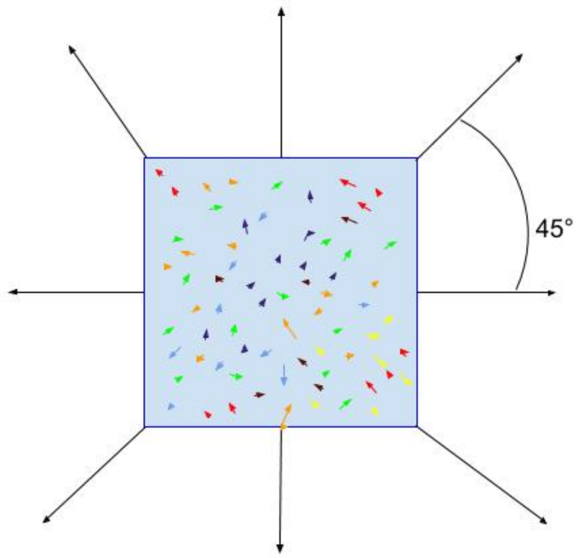


Figure 3(a) - Visualization of a block with optical flow movements inside the block

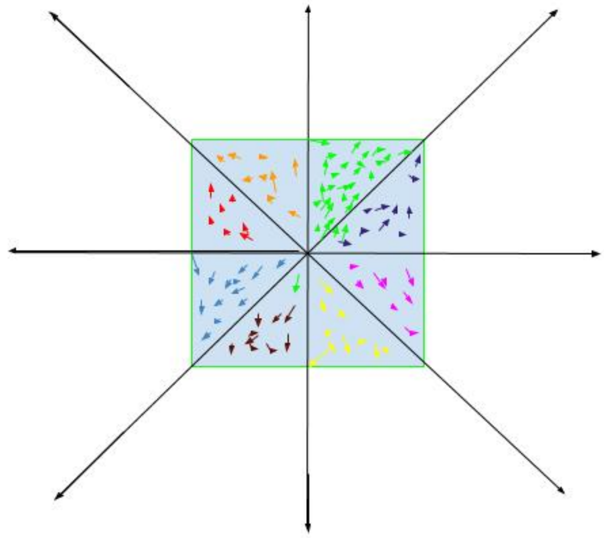


Figure 3(b) - Classification of Optical Flow movements inside a block based on direction of movement

3.2. Motion Descriptor Computation

The main feature of the proposed motion influence map is that it effectively reflects the motion characteristics of the movement speed, movement direction, corresponding magnitude and size of the objects or subjects, and their interactions within a frame sequence. Each frame is separated into several block structures for computing individual motion features of every block with its all other neighboring blocks. Two major factors which influence the movement of objects are: i. magnitude, and ii. direction angle.

Algorithm
Input: $K -$ Set of blocks in the frame
Output: M $-$Motion Descriptor Map
M is set to zero at the beginning of each frame
for all i in K,
th_{b_i}= max(b_i^k).sizeb_i
for all $j\epsilon K$ where $\neq ji$,
    Compute ed_{ij} - Euclidean Distance between block i and j
    if $ed_{ij} \leq th_{b_i}$,
    $\theta_{ij} -$ Angle btw block i and j
        $k = \lfloor \theta / 45 \rfloor$
    w_{ij}= exp(-ed_{ij} / b_i^k)
    $M^j_{orien_{b_i}} = M^j_{orien_{b_i}} + w_{ij}$
    end if
end for
end for

The movement of the object is highly influenced by neighboring blocks relative to a selective block which concludes that neighboring blocks will have high influence over the distant blocks. For every individual block structure, a distinct parameter called threshold distance is being computed by multiplying magnitude of each block with total block size of an overall frame. Threshold th_{b_i} is computed as,

$$t\square_{b_i} = max(b_i^k).size_{b_i} \tag{2}$$

where, b_i^k is the magnitude of block b_i in the direction k. It is calculated by multiplying the size of single block with magnitude of particle pointing to similar direction. For every block in a frame, Euclidean distance between every other block and the corresponding angle of deviation between blocks are computed. The flag variable f is computed as,

$$f = \begin{cases} 0\,, if ed_{ij} > th_{b_i} \\ 1\,, otherwise \end{cases} \tag{3}$$

Let θ be the angle of deviation between block i and j.

$$k = \lfloor \theta \;/\; 45 \rfloor \tag{4}$$

Now, influence weight of blocki on blockj, w_{ij} is computed as,

$$w_{ij} \;=\; f.exp(-ed_{ij} \;/\; b_i^k) \tag{6}$$

Influence weight, w_{ij} of blocks is calculated for every frame in the video and added with influence weight of previous blocks called Motion Descriptor.

3.3. Motion Descriptor Pattern Clustering

After computing the influence weights of all blocks (w_{ij}), a motion influence map clustering is generated which significantly represents the motion patterns within a frame. Each component of the motion influence vector represents the quantized motion vector orientation of the ith block. In the computation of influence weight, it is known that only a pair of blocks are considered, that is w_{ij} reflects only the influence of the i^{th} block on block j. To compute the motion influence vector of the jth block within a frame, assumption is based on all other blocks that potentially affect the motion of block j.

$$M^j_{orien(b_i)} \;= \sum_j w_{ij} \tag{7}$$

Where $j \in \{1, 2, . . ., MN\}$, i denotes the quantized orientation index of a block, which is used as a component index of *block-j* and denotes the computed influence weight. The computed motion influence weight of the block of every frame is added up to form a motion descriptor map. The motion descriptor map is clustered into many clusters based on the influence weights using k-means clustering. The result of the k-means clustering provides a behavioral pattern which has influence weights in many clusters.

3.4. Nearest Neighbor Search

In this module, the influence weights computed from the previous modules are framed as motion descriptor map and searched for nearest cluster distance in the trained system. If the motion descriptor is near to center of any cluster of the behavior pattern then it is a normal block. If the distance between the computed motion descriptor and closest cluster center must be lesser than threshold of acceptance, then the block is considered normal. If the distance is greater than threshold then the block in the frame is considered abnormal. Minimum distance, md of deviation of the computed motion descriptor is calculated as,

$$m_d = \forall_c \min(eucl(c)) \tag{8}$$

The block is considered abnormal if m_d is greater than the threshold of acceptance.

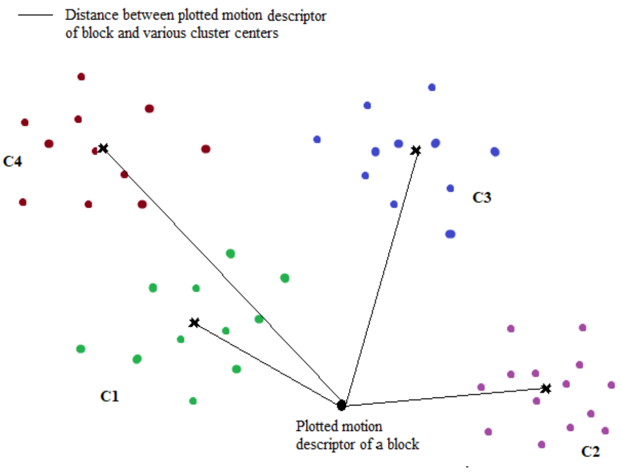


Figure 4 - Visualization of detection of abnormal block in nearest neighbor search

3. EXPERIMENTAL RESULTS

Performance of the proposed work is analyzed by experimenting with two major public datasets namely, UMN and UCSD [19] datasets and also a created dataset in a real time environment (Fig. 5(a) and 5(b)). The locally created datasets fulfill the requirements of typical household scenario in a residential area. The effectiveness of the algorithm is analyzed at both frame level and block level for all these three datasets. Performance measures such as accuracy, recall and precision are calculated for several experiments. The system is implemented on OpenCV and Python programming language.

4.1. Dataset

The UMN dataset consists of 11 video clips of crowded escape scenarios from three different indoor and outdoor scenes. It includes 7740 frames in total, where the frame size is 320 × 240. There are two sets of video clips in the UCSD dataset. In this dataset, a normal activity was defined as people walking along a pathway. Ped-1 consists of 34 training clips and 36 test clips with frame size 238×158 and Ped-2 consists of 16 training clips and 12 test clips with frame size 360 × 240. Apart from these two standard datasets, we have tested the algorithm with our own created dataset which consists of activities such as crowd gathering, normal walk as training set and sudden panicking, throwing abnormal objects, snatch theft, bike movements as abnormal.

4.2. Static Parameters Settings

In the proposed framework, there are several parameters, such as the block size, threshold of acceptance in the nearest neighbor search module, and K values in the K-means clustering, that governs the system performance. Experiments were performed to account the effect of varying parameters.

4.2.1. Threshold of Acceptance

During nearest neighbor search, the threshold of acceptance plays an important role in classifying a block in a frame for the normal/abnormal identification. Larger threshold means only sharp abnormal movements are detected. In scenarios which involve usual fast movements, the threshold must be set larger and it must be set smaller in the opposite case. As listed in Table 1, it is clear that for UMN dataset, threshold of acceptance value 4.8368e-04 gives the best results. When the threshold value is higher, the recall is 100%, i.e., the algorithm predicted all actual abnormal as abnormal.

Table 1– Performance of the system with various threshold values in UMN Dataset

Threshold of Acceptance	Performance		
	Accuracy	*Recall*	*Precision*
5.8368e-06	82.10	83.69	97.46
8.8292e-05	91.57	91.76	98.73
4.8368e-04	98.94	98.68	100
1.6586e-03	89.47	100	87.34

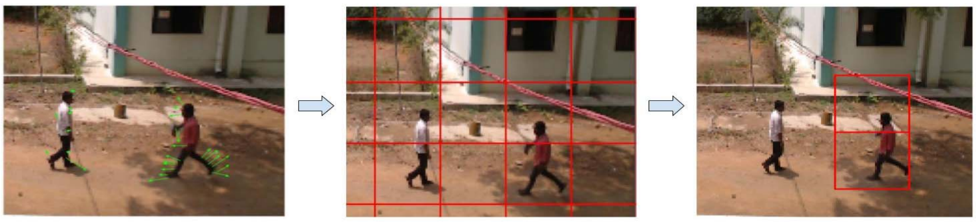


Figure 5(a) - Abnormal Crowd Activity detection system flow with created dataset

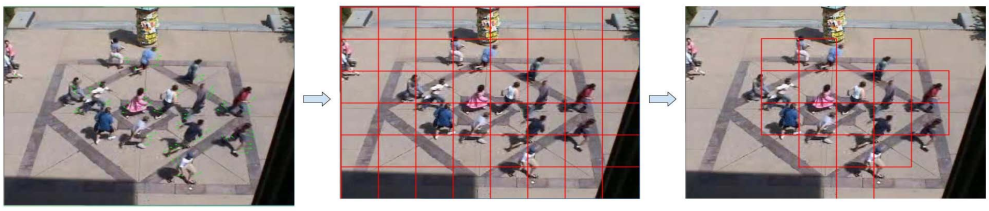


Figure 5(b) - Abnormal Crowd Activity detection system flow with UMN dataset

4.2.2. Number of Clusters

K-means clustering algorithm requires the number of clusters to be prefixed before clustering process. It affects the performance of the system since abnormality is predicted from distance the motion influence of the block is deviated from the normal clusters. The algorithm was tested with four different number of cluster values. As listed in Table 2, it is clear that when number of clusters is 4, the performance of the system is high. Precision is 100% indicating that detected abnormal blocks are actually abnormal. Clustering happens separately for each block in the frame. Further, the results from Table 2 show that increasing the number of clusters does not guarantee the improvement of the system performance.

Table 2– Performance of the system with varied number of clusters in UMN Dataset

No of Clusters	Performance		
	Accuracy	Recall	Precision
4	98.94	98.68	100
5	98.17	98.66	98.66
6	98.94	100	92.73
7	98.78	98.68	96.10

4.2.3. Block Size

Each frame in the video is divided into $M \times N$ uniform blocks for computing influence weight between blocks and further processing. However, considering that the motion influence value represents the motion of surrounding blocks rather than the target block itself, the choice of the block size can affect the performance. Therefore, we measured the unusual activity detection performance for the UMN dataset on various block sizes to show the effect of a change in block size.

The experimental results considering different block size is shown in Table 3. When the size of a block is small and the motion information of an object is represented by various motion vectors, thereby generating noise, the use of a motion influence map will be fully considered. However, if the size of a block is bigger than the size of an object, important motion characteristics may be disregarded. Here, it can also be observed that the performance is maximized when the block size is set to approximately half the size of the pedestrian.

Table 3– Performance of the system with varied block division of frames in UMN Dataset

Frame Division	Performance		
	Accuracy	Recall	Precision
8×6	98.94	98.68	100
10×8	96.35	97.20	99.25

4.3. Comparison with other works

The proposed algorithm has been compared with HOFME [12] and has produced higher accuracy in both standard datasets (UMN, UCSD) and custom made dataset. Both block level and frame level accuracy are listed in Table 4 and Table 5.

Table 4– Comparison of works (Block level accuracy)

Method	Datasets			
	UMN	UCSD		Created Dataset
		Ped 1	Ped 2	
HOFME [12]	98.52	72.70	87.50	95.04
Proposed Method	98.94	71.32	88.13	98.78

Table 5 – Comparison of works (Frame level accuracy)

Method	Datasets			
	UMN	UCSD		Created Dataset
		Ped 1	Ped 2	
HOFME [12]	84.94	86.30	89.50	93.56
Proposed Method	92.35	81.20	91.10	95.60

4. CONCLUSION

Abnormal activity detection in a crowded scene requires development of system model and associated learning process. Unlike previous methods described in the literature, which have focused on either local or global abnormal activity detection, the proposed method considers the motion characteristics within a frame to detect and localize abnormal human activities in a crowded scene. The model can classify a frame as normal, abnormal, and localize the areas of abnormal activities within the frame. The experiments were conducted on two public datasets, UMN and UCSD datasets to validate the effectiveness of the proposed method in comparison with competing methods from the literature. The proposed solution was also tested with a custom made dataset representing a local real time environment. The ITU recommendations were used in developing system in a standardized modular fashion. However, one of the limitation of the proposed system is: threshold of acceptance need to be fixed for specific scenarios. Another constraint of the model is that it is more dependent on view angle and camera distance from action. The experiments were limited to a fixed viewpoint, and there is a limitation in the applicability of the approach for surveillance cameras with zoom, or tilt functionality.

Dynamic thresholding in surveillance system will make the model more real time impermeable. The proposed work can be further extended by implementing clustering part with hierarchical algorithms instead of basic *k*-means. The advantage of using hierarchical algorithms is that the cluster size need not be pre-determined in most cases. The proposed method deals only with static cameras. However, it can be extended to tilt and zoom cameras using localization results. Further, camera motion estimation can be added to reduce inaccuracies due to small camera movements.

REFERENCES

[1] D. Helbing and P. Molnar, "Social force model for pedestrian dynamics," Physical Review E, vol. 51, no. 5, pp. 4282–4286, 1995.

[2] R. Mehran, A. Oyama, and M. Shah, "Abnormal crowd behavior detection using social force model," in Proc. IEEE Conf. Computer Visual Pattern Recognition, Miami, FL, pp. 935–942, Jun. 2009.

[3] X. Cui, Q. Liu, M. Gao, and D. N. Metaxas, "Abnormal detection using interaction energy potentials," in Proc. IEEE Conf. Computer Visual Pattern Recognition, Colorado Springs, CO, USA, pp. 3161–3167, Jun. 2011.

[4] D. Xu, E. Ricci, Y. Yan, J. Song, and N. Sebe, "Learning deep representations of appearance and motion for anomalous event detection," in Proc. British Machine Vision Conference (BMVC), UK, pp. 548–561, September 2015.

[5] L. Kratz and K. Nishino, "Anomaly detection in extremely crowded scenes using spatio-temporal motion pattern models," in Proc. IEEE Conf. Computer Visual Pattern Recognition (CVPR), pp. 1446–1453, Jun 2009.

[6] E. L. Andrade, S. Blunsden, and R. B. Fisher, "Modelling crowd scenes for event detection," in Proc. 18th Int. Conf. Pattern Recognition (ICPR), pp. 175–178, August 2006.

[7] J. Kim and K. Grauman, "Observe locally, infer globally: A space-time MRF for detecting abnormal activities with incremental updates," in Proc. IEEE Conf. Computer Visual Pattern Recognition, Miami, FL, USA, pp. 2921–2928, Jun. 2009.

[8] K. W. Cheng, Y. T. Chen, and W. H. Fang, "Video anomaly detection and localization using hierarchical feature representation and Gaussian process regression," in Proc. IEEE Conf. Computer Visual Pattern Recognition (CVPR), pp. 2909–2917, June 2015.

[9] W. Li, V. Mahadevan, and N. Vasconcelos, "Anomaly detection and localization in crowded scenes," IEEE Trans. on Pattern Analysis Matching Intelligence, vol. 36, no. 1, pp. 18–32, Jan. 2014.

[10] V. Saligrama and Z. Chen, "Video anomaly detection based on local statistical aggregates," in Proc. IEEE Conf. Computer Visual Pattern Recognition (CVPR), pp. 2112–2119, Jun. 2012.

[11] J. Shao, C. C. Loy, and X. Wang, "Scene-independent group profiling in crowd," in Proc. IEEE Conf. Computer Visual Pattern Recognition (CVPR), pp. 2227–2234, Jun. 2014.

[12] F. Jiang, J. Yuan, S. A. Tsaftaris, and A. K. Katsaggelos, "Anomalous video event detection using spatiotemporal context," Computer Visual Image Understand., vol. 115, no. 3, pp. 323–333, 2011.

[13] Aravinda S. Rao, Jayavardhana Gubbi, Slaven Marusic, and Marimuthu Palaniswami, "Crowd Event Detection on Optical Flow Manifolds", IEEE Transactions on Cybernetics, vol. 46, no. 7, July 2016

[14] Arnold Wiliem, VamsiMadasu, Wageeh Boles, Prasad Yarlagadda, "A suspicious behaviour detection using a context space model for smart surveillance systems," in Computer Vision and Image Understanding, Vol. 116, no. 2, pp. 194 – 209, Feb 2012.

[15] T. Xiang, S. Gong, "Incremental and adaptive abnormal behaviour detection," Journal on Computer Vision and Image Understanding, vol. 111, no. 1, pp. 59–73, July 2008.

[16] Y. Yuan, J. Fang, and Q. Wang, "Online anomaly detection in crowd scenes via structure analysis," IEEE Trans. Cybern., vol. 45, no. 3, pp. 548–561, March 2015.

[17] R. V. H. M. Colque, C. A. C. Júnior, and W. R. Schwartz, "Histograms of optical flow orientation and magnitude and entropy to detect anomalous events in videos," IEEE Transactions on Circuits and Systems for Video Technology, vol. 27, no. 3, March 2017.

[18] R. V. H. M. Colque, C. A. C. Júnior, and W. R. Schwartz, "Histograms of optical flow orientation and magnitude to detect anomalous events in videos," in Proc. 28th SIBGRAPI Conf. Graph., Patterns Images, Salvador, Brazil, pp. 126–133, Aug. 2015.

[19] Semiotics Visual Communication Lab UCSD Anomaly Data Set. [Online]. Available: http://www.svcl.ucsd.edu/projects/anomaly/

SESSION 6

SOCIAL, LEGAL AND ETHICAL ASPECTS IN MACHINE LEARNING

A GENDERED PERSPECTIVE ON ARTIFICIAL INTELLIGENCE

Smriti Parsheera[1]

[1]National Institute of Public Finance and Policy, New Delhi

ABSTRACT

Availability of vast amounts of data and corresponding advances in machine learning have brought about a new phase in the development of artificial intelligence (AI). While recognizing the field's tremendous potential we must also understand and question the process of knowledge-making in AI. Focusing on the role of gender in AI, this paper discusses the imbalanced power structures in AI processes and the consequences of that imbalance. We propose a three-stage pathway towards bridging this gap. The first, is to develop a set of publicly developed standards on AI, which should embed the concept of "fairness by design". Second, is to invest in research and development in formulating technological tools that can help translate the ethical principles into actual practice. The third, and perhaps most challenging, is to strive towards reducing gendered distortions in the underlying datasets to reduce biases and stereotypes in future AI projects.

Keywords – Artificial intelligence, gender, ethics, fairness

1. INTRODUCTION

The term artificial intelligence (AI) was coined in a Dartmouth summer research proposal in 1955 that described itself as a "*2 month, 10 man study of artificial intelligence*". John McCarthy, Marvin Minsky and their fellow drafters explained it as a "*proposal to find how to make machines use language, form abstractions and concepts, solve kinds of problems now reserved for humans, and improve themselves"* (McCarthy et al, 1955[1]). They highlighted these as problems that needed a carefully selected group of scientists to work on them and there seemed to be no doubt about the gender of those researchers.

Sixty years hence, AI is seen as one of the most promising fields of computer science. Its latest boom is fueled by the availability of vast amounts of data and corresponding advances in machine learning and neural technology. Self-driving vehicles, cancer detection technologies, image recognition tools, language translation and virtual assistants are some of the many AI applications that we encounter in everyday conversations. The field has, however, gone through its share of "AI winters", characterized by cutbacks in funding when research outcomes failed to keep up with the claimed progress.

Today, we are in a phase of AI boom. As per most accounts, AI based systems will play a much greater role in the coming decades, redefining business models, job markets and overall human development. In all the euphoria surrounding AI and its future, not enough was being said about the underlying processes that drive research in this field. This has begun to change in the last few years as countries begin to adopt national or regional AI strategies, many of which incorporate an inclusion and ethics dimension in them (Dutton, 2018[2]).

Like most human creations, AI artifacts tend to reflect the goals, knowledge and experience of their creators. They also draw from the strengths and weaknesses of the data that is used to train them. It is therefore natural to expect the limitations and biases of the creators and their datasets to be reflected in their results. This leads us to ask some basic questions. First, what is regarded as AI, who designs it and to what end? Second, what is the basis for determining the elements of intelligence that are found worth replicating in machines? Finally, to what extent do these decisions reflect the diverse experience and needs of human society?

These are complex questions, and the answers will necessarily vary based on the respondent's standpoint -- education, gender, race, class, religion, nationality and the intersectionality of these factors. Despite recent attempts to "diversify" AI research, and more generally research in the fields of science, technology, engineering and mathematics (STEM), the discipline has retained a male-oriented focus. It is telling that when the Institute of Electrical and Electronics Engineers (IEEE) instituted a Hall of Fame to acknowledge the leading contributors to AI, not one of the ten persons on the list was a woman (Wang, 2010[3]).

A research environment that fails to account for the worldview of one entire gender group is clearly lacking in many respects. In making this claim, we are cognizant of the fact that just as there is no universal "human knowledge", it is also not possible to classify "men's knowledge" and "women's knowledge" into distinct buckets. There exist a multiplicity of viewpoints within these groups. A more inclusive, and indeed more fruitful, research agenda should ultimately be able to overcome these binaries. Recognizing the existence of a gendered perspective on AI is, however, the starting point for this conversation. While this paper uses the role of gender in AI research as its lens of enquiry, the issues that it poses and the solutions that it suggests are also relevant to broader pursuits of inclusiveness in AI-based systems.

2. DEFINING AI AND ITS "INTELLIGENCE"

John McCarty, one of the founders of this field, described AI as the "*the science and engineering of making intelligent machines*" where intelligence refers to "*the computational part of the ability to achieve goals in the world*" (McCarty, 2007[4]). Another suggestion is to look at intelligence as a "*quality that enables an entity to function appropriately and with foresight in its environment*" (Nilsson, 2010[5]). Both these definitions, forwarded by practitioners of AI, refer to intelligence in rather broad terms, as qualities which can be possessed by humans, animals and machines, albeit, at different levels.

Russell and Norvig (2010)[6] present a classification of the available definitions of AI along two lines -- (i) based on the function expected to be performed (*thought processes/ reasoning* of the machine versus the *outcome/ behaviour* that it exhibits); or (ii) the metrics used for assessing the success of AI (*human performance* versus an ideal standard of "*rationality*"). The Turing test, developed by British mathematician and cryptographer Alan Turing in 1950, reflects a combination of the behavioral element and human-like performance in the above classification. If upon the exchange of a series of questions with a person and machine, a human interrogator is unable to distinguish between the two, the Turing test would regard the machine to be an intelligent, thinking entity (Copeland, 2018[7]).

Despite its continued relevance over the years, the Turing test has also come under attack for its attempt to define the intelligence of machines by replicating human behaviour. Russell and Norvig (2010)[6] point to this as a limitation by saying, "*Aeronautical engineering texts do not define the goal of their field as making machines that fly so exactly like pigeons that they can fool even other pigeons*".

AI's claims of building intelligence in machines have also faced strong philosophical criticisms. These criticisms stem from arguments about the lack of a mind, of consciousness and intentionality in machines, features which some philosophers regard as essential for establishing true intelligence. John Searle illustrated this through his famous Chinese room thought experiment. As per this, person who does not know any Chinese can follow a set of rules on how to correlate Chinese symbols and produce a response to questions that may convince an outsider that the person is acting intelligently. Producing meaningful replies in Chinese would however not mean that the person has any actual understanding of the language.

In making the claim that similar behavior by a computer programme cannot be equated with intelligence, Searle draws a distinction between "weak AI", where the computer serves as a tool to study the mind and "strong AI" where the computer itself can be said to possess a mind. He focuses his criticisms on the latter by arguing that in order to constitute strong AI a machine would need to satisfy the tests of consciousness and intentionality or causal powers that are possessed by the human brain (Searle, 1980[8]). Similar debates on the "intelligence" of AI have also emerged from other fields like psychology, economics, biology, neuro-science, engineering and linguistics (Russell and Norvig, 2010 [6]).

Feminist epistemologist Alison Adam notes that these popular criticisms of are lacking in two major respects. First, they gauge the success or failure of AI based on philosophical tests of ideal intelligence, which for Adam is less relevant than understanding how AI is actually being put to use. For her, the success of AI lies in its widespread adoption in everyday life. Second, she notes that the traditional critiques of AI completely ignore how AI systems reinforce existing power structures. AI research has failed to represent the knowledge of certain social groups, such as women (Adam,2005[9]). This has worked to the disadvantage of society as well as the field itself.

3. GENDER OF AI DEVELOPERS AND THEIR ARTIFACTS

While the contours of what constitutes intelligence in AI has remained contested, a more operational understanding of AI has also emerged. As per some researchers, AI can simply be defined as "*what AI researchers do*" (Grosz et al, 2016[10]). This approach clearly gives the practitioners in this field immense power, not just in defining their own agenda but also the contours of the discipline that they represent. It therefore becomes pertinent to discuss who are these researchers and what is it that they do?

3.1 Early choices in AI research

Interestingly, even though we have seen significant advances in AI applications in recent years, the fundamental elements of what constitutes AI research have not changed very significantly. In 1955, the Dartmouth College proposal identified the following as some of the components of the AI problems that needed further research: programming a computer to use a language (*natural language processing*); self-improvement by machines (*machine learning*); and neuron nets (*neural networks* and *deep learning*) (McCarthy et al, 1955[1]). The text in parenthesis reflects the currently in vogue terminology for these processes. While these areas of research still remain relevant, newer sub-areas like computer vision and robotics have also been added along the way (Grosz, 2016[10]).

This leads us to ask – on what basis did AI researchers decide that certain elements of intelligence (versus others) were worth replicating in machines? In 1950, Alan Turing admitted that he did not know the right answer. He proposed that it would be prudent to try both the approaches that were being suggested at that time. The first would be to choose an abstract activity like playing chess and teach machines to do it. The second would be to equip machines with sense organs and teach them the right answers, like teaching a child (Turing, 1950[11]).

Adam, 1998[12] uses the fascination with chess in early AI works to demonstrate how the interests and worldview of AI researchers influenced their conception of what amounted to intelligent behavior. She refers to the following quote from Rob Wilnesky, an AI researcher, to illustrate the point:

> "*They were interested in intelligence, and they needed somewhere to start. So they looked around at who the smartest people were, and they were themselves, of course. They were all essentially mathematicians by training, and mathematicians do two things - they prove theorems and play chess. And they said, hey, if it proves a theorem or plays chess, it must be smart.*"

The choice of chess and theorem proving, both being activities predominantly associated with men, therefore became a natural choice for early AI researchers (Adam, 1998[12]). The choice of chess as a metric for proving machine intelligence is particularly interesting given that the game still continues to suffer from a significant gender problem, resulting in the under-inclusion and under-performance of women (Maass et al, 2007[13]). Yet, it would be hard to claim that that the early choices of AI researchers stemmed from any malice against women or their role is society. Instead, these decisions reflected the researchers' own experiences, interests and social conditioning.

The "context" of AI researchers, which includes their gender, has therefore defined the directions in which the field has progressed. It is possible to imagine that if the group contemplating early ideas for testing machine intelligence included some women, an entirely different set of ideas may have emerged.

3.2 Different dimensions of gender bias

It has been over seven decades since AI first emerged as a discipline and yet the gender imbalance in AI, and more broadly in the fields of STEM, still remains significant. As per data released by the UNESCO Institute for Statistics, women constitute less than 29 percent of scientific researchers globally (UNESCO, 2017[14]). Further, there are many inter regional differences, with many developing countries showing a lower percentage of women in science. For instance, in India's case the figure of women in science was only about 14.3 percent (UNESCO, 2017[14]).

A study involving computer science PhD graduates in India found that 32 percent of the graduating PhD students in 2016 were women (Parkhi and Shroff, 2016[15]). This figure is closer to the world average of women in science although it is also worth noting that a majority of the PhD graduates opted for teaching jobs and only a small number went on to join research labs. Therefore the percentage of women from this pool who might have gone on to engage in applied research is likely to be much smaller.

The under-representation of women in AI research has the corresponding effect of under-representation of their ideas in setting AI agendas. This imbalance also manifests itself in other forms that go beyond issues of direct representation. Firstly, the few women who do manage to enter this field have reported systematic discrimination in terms of salaries, promotions and incidents of sexual harassment (Vasallo et al, 2015[16]). This contributes to the leaky pipe problem in STEM. Secondly, the AI industry is also replete with examples of gender based stereotypes being reflected in the identities of AI artifacts, their functions and outputs. To some extent this can be attributed to the lack of diverse perspectives in the designing and testing of these artifacts.

For instance, virtual assistants like Apple's Siri, Amazon's Alexa, Google's assistant and Microsoft's Cortana commonly come with female sounding voices (although in some cases like Apple's Siri users were later given the option to change the default voice). This is also the case with most GPS assistants. Several factors may contribute to this. On one hand, it could be a conscious business decision, based on physical and psychological reasons for preferring a woman's voice for such machines. On the other, it may be a case of unconscious reiteration of society's existing gender stereotypes -- a woman's voice being regarded as more suitable for roles that demand obedience (Glenn, 2017[17]. Similarly, the names and body shapes given to robots and other AI solutions have also been known to reflect the prevalent socio-cultural norms and gender identities (Bowick, 2009[18]).

Another dimension of the gender problem in AI comes from the perceptions and stereotypes of the real world, the data that emerges from there and its use in training algorithms. This can be illustrated with a few examples. When translation services, like the one offered by Google, translate text from gender neutral languages like Turkish and Finnish to a gendered one like English, the algorithm tends to attribute a gender to the subject. This classification may be based on the profession being described – engineers, doctors, soldiers are generally described as "he" while teachers, nurses and secretaries would be "she". It could also relate to the activities or emotions in question – happiness and hardwork are associated with "he" while terms like lazy and unhappy with "she" (Morse, 2017[19]).

Bolukbasi et al, 2016[20] explain that this problem can be attributed to the blind adoption of “word embedding” techniques. Word embedding enables the mapping of the affinity or relationship between different words, where a public resource like Google News serves as the training dataset. The researchers illustrate how this could influence the search results for a person looking for a computer science researcher in a particular university because the words “computer science” are more commonly associated with men -- “*between two pages that differ only in the names Mary and John, the word embedding would influence the search engine to rank John’s web page higher than Mary* ” (Bolukbasi et al, 2016[20]). Similar findings of gender biases been also been made in case of visual recognition tasks like captioning of images (Zhou et al., 2018[21]) and display of image search results based on occupations (Kay, 2015[22]).

These examples demonstrate that AI applications can often end up strengthening and reinforcing society's existing biases. For instance, Zhou et al., 2018[21] found that where training images for the activity of cooking contained 33% more females, the trained model for captioning images amplified the disparity to 68%. This seems to run contrary to Donna Haraway’s vision of a cyborg universe where technology would offer a tool to break away from the dualities of human-machine and male-female identities (Haraway, 1991[23]). This is an inspiring idea and one that we still have an opportunity to fix. Concepts of equity, fairness and non-discrimination have been well entrenched in the human rights discourse for the past several decades. Yet, conscious and unconscious human biases often prevent these values from translating into actual outcomes. How then can we re-envision AI research in ways that could move us closer to this ideal?

4. RE-ENVISIONING AI FROM A GENDERED PERSPECTIVE

Improving the representation of women in AI research, both as researchers and as beneficiaries of the research is seen as a first step towards a gendered re-envisioning of AI. This has led to initiatives like having specialized programmes for women, funding support, mentorship initiatives, increased intake in educational institutions and promoting equal opportunities in the job market. However, even if such initiatives were to succeed, it is questionable whether merely increasing the number of women can bring the desired level of diversity in AI knowledge-making.

In her work on objectivity and diversity, Sandra Harding notes that although increasing the physical presence of excluded groups is an important first step, the real issue goes beyond that of participation. It involves questioning *whose agendas should be pursued by science*? (Harding, 2015[24]). A research agenda that is primarily funded through private resources will logically rely on market mechanisms to decide on the kind of problems that need to be solved and their optimum solutions. In the long run, this could very well lead to the development of breakthrough technologies, the benefits of which may ultimately trickle down the marginalized sections of society. However, there is a distinction between retrofitting newer objectives into available technologies versus a ground up approach of identifying specific problems and developing solutions for them.

The latter approach would require a more meaningful engagement by businesses, governments and the public in identifying AI research agendas and supplying resources to pursue them. These resources could be in the form of financial support, ethical frameworks, as well as making available open data resources that can feed into the design of AI solutions. For instance, the development of AI applications that are useful for addressing the health concerns of rural women in a developing country like India may not be an obvious interest area for many AI researchers. This may stem both from the lack of funding for sustained research in such areas and also the lack of access to the data that is necessary for enabling this research. Similarly, the ways in which algorithmic credit will work out in the Indian setting may be very different from what happens in other parts of the world. Agenda setting for future AI research must therefore be rooted in the social and cultural backdrop and institutional context of each society.

Having said that, there is also a case for evolving a robust set of ethical standards for AI research and the tools for translating those principles into tangible outcomes. Questions of bias and ethics have already found a place in many national AI strategies. For instance, the United Kingdom has noted that although it cannot match countries like the United States and China in terms of AI spending, it intends to play a greater role in AI's ethical development (House of Lords, 2018[25]). In India, a discussion paper issued by the Government think tank NITI Aayog (NITI Aayog, 2018[26]) as well as an AI Task Force set up by the Indian Government have spoken about the need for ethical standards, including auditing of AI to check that it is not contaminated by human biases (AI Task Force, 2018)[27]. Both these documents are, however, conspicuously silent on the gender dimensions of AI education and research in the country. Most large technology companies also have internal ethics policies to govern their research initiatives. Moving from these siloed structures to a collectively designed set of global minimum standards for AI development should be the next goal. These principles can then be applied based on each region’s own context.

This above proposal comes with the worry that absent strict enforcement, producers would tend to interpret any ethical guidelines in a flexible manner. This could resulting in the under-production of “fairness” in the system. The opacity of AI algorithms and possibility of diverse interpretations on what constitutes fairness in any given situation only compound the problem. But trying to solve this issue through heavy-handed regulation and strict ex-ante controls would present its own set of challenges. Such interventions may come at the cost of stifling efficiency and innovation. This also presumes a certain level of state capacity to effectuate the regulation, which is often not available in reality. How then can we strike a balance between these positions to make sure that AI research evolves in a socially and ethically responsible direction? We propose a three step approach towards this goal.

The first step would be to embed the concept of "***fairness by design***" in AI frameworks (Abbasi et al, 2018[28]). This draws from the concept of "privacy by design" that has evolved in the context of data protection debates (Cavoukian, 2011[29]). Fairness by design should compel developers to ensure that the very conception and design of AI systems is done in a manner that prioritizes fairness. Abbasi et al, 2018[28] propose that the components of such a framework would include:

(i) creating cross-disciplinary teams of data scientists and social scientists;
(ii) identifying and addressing the biases brought in by human annotators;
(iii) building fairness measures into the assessment metrics of the program;
(iv) ensuring that there is a critical mass of training samples so as to meet fairness measures; and
(v) adopting debiasing techniques.

A fair amount of research has been done on building solutions for gender biases in natural language processing. For instance, Bolukbasi et al, 2016[20] use debiased word embeddings for removing negative gender associations from word embeddings generated from a dataset. Another strategy is to use gender swap techniques to remove any correlation between gender and the classification decision made by an algorithm (Park et al, 2018[30]). A variation to this would be to conduct "stress tests" where certain parts of the data (such as the gender of some candidates in a selection process) can be randomly altered to check whether the randomization has an effect on the final outcome that is generated, i.e. the number of women being shortlisted (Economist, 2018)[31].

While encouraging further research of this nature, a lot more needs to be done in terms of mainstreaming these solutions and making them readily available to smaller developers. Google's "What-If" tool offers a useful example. It is an open source tool that allows users to analyze machine learning models against different parameters of fairness. For instance, the data can be sorted to make it "group unaware" or to ensure "demographic parity" (Weinberger, 2018[32]). Given the many positive externalities to be gained from the creation and opening up of such fairness enhancing tools, the second step of the re-envisioning AI project would be for governments and other agencies to invest in more research and development on this front.

Finally, we must remember that the datasets being used for training machine learning algorithms are created in the real-world, i.e. outside the AI ecosystem. Therefore, while building reactive use-case based solutions (NITI Aayog, 2018[26]) may solve some of our immediate needs, the larger agenda must be to correct the training dataset itself. To take an example, the outcomes of natural language processing can be made more inclusive if the persons generating the underlying text (writers, researchers, policymakers, journalists, publishers and other creators of digital content) work towards the feminization (using words like *she* and *her*) and neutralization (*chairperson* instead of *chairman*) of the language that they use (Sczesny et al, 2016[33]). Here again, there is a role for the State to use awareness, education and, if required, other policy tools to promote the use of gender fair language. Similar solutions need to considered for other fields of AI research, accompanied by the identification of the persons and processes needed to effectuate the desired changes.

5. CONCLUSION

From its very inception, the field of AI has largely remained the domain of men. This paper illustrates how the gender of its founders and subsequent researchers has played a role in determining the course of AI research. While efforts are now being made to fill this gap, including by promoting more women in STEM, the gender problem of AI is not just about the representation of women. It is also about understanding whose agendas are being pursued in AI research and what is the process through which that knowledge is being created.

Research has shown that AI's reliance on real-world data, which is fraught with gender stereotypes and biases, can result in solutions that end up reinforcing or even exacerbating existing biases. While fairness and non-discrimination are well recognized principles in the human rights discourse, these principles often fail to translate into practice, often on account of the conscious and unconscious biases. The challenge therefore is to find ways to bundle the technological progress of AI with the objectives of pursuing greater fairness in society -- for machines to eliminate rather than reinforce human biases.

We propose a three step process towards this end. First, we need to develop a set of publicly developed AI ethics that embed the concept of "*fairness by design*". To travel the distance from formulating ethical principles to their actual implementation is another challenge. We find that "fairness" as a concept is prone to diverse interpretations, which can result in its under-production in the system.

The second step would therefore be to invest in research and development in formulating technological tools to implement AI ethics. This would, for instance, include further work on developing debiasing and fairness testing techniques. Open dissemination of such solutions to make them readily available for adoption by the AI community, will generate positive externalities for the system as a whole. This will require cooperation among a range of stakeholders, including governments, corporations, universities and researchers working in the fields of computer science, social science and data science.

Finally, we need to think about deeper solutions for cleaning up the gender biases and stereotypes in the underlying datasets that serve as fodder for training AI algorithms. For instance, feminization and neutralization of language have been suggested as solutions to enhance fairer outcomes in natural language processing. Similar solutions need to considered for other fields of AI research along with an identification of the persons and processes that are necessary to effectuate the desired changes.

REFERENCES

[1] McCarthy et al, 1955: John McCarthy, Marvin Minsky, Nathaneil Rochester and Claude Shannon, *A proposal for the Dartmouth summer research project on artificial intelligence*, August 31, 1955, available at https://www.cs.swarthmore.edu/~meeden/cs63/f11/AIproposal.pdf

[2] Dutton, 2018: Tim Dutton, *Artificial Intelligence Strategies*, Medium, 28 Jun 2018, available at https://medium.com/politics-ai/an-overview-of-national-ai-strategies-2a70ec6edfd

[3] Wang, 2010: Fei-Yue Wang, IEEE Intelligent Systems, Volume: 26, Issue: 4, July-Aug, 2011, available at https://ieeexplore.ieee.org/document/5968105/

[4] McCarty, 2007: John McCarthy, *What is artificial intelligence*?, 11 December, 2007, available at http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html

[5] Nilsson, 2010: Nils J. Nilsson, *The quest for artificial intelligence - A history of ideas and achievements*, Cambridge University Press, 2010.

[6] Russell and Norvig (2010): Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd Ed, Prentice Hall Series in Artificial Intelligence, 2010.

[7] Copeland, 2018: BJ Copeland, *Artificial Intelligence*, Britannica Encyclopedia, available at https://www.britannica.com/technology/artificial-intelligence

[8] Searle, 1980: John Searle, *Minds, brains, and programs*, Behavioral and Brain Sciences, 3 (3), 417-457.

[9] Adam 2005: Alison Adam, *Gender, Ethics and Information Technology*, Palgrave Macmillan, 2005.

[10] Grosz, 2016: Barbara Grosz et al, *Artificial intelligence and life in 2030*, One hundred year study on artificial intelligence, September 2016.

[11] Turing, 1950: Alan Turing, *Computing Machinery and Intelligence*, Mind, 49, 433-460.

[12] Adam, 1998: Alison Adam, *Artificial Knowledge - Gender and the Thinking Machine*, Routledge, 1998.

[13] Maass et al, 2007: Anne Maass, Claudio D'Ettole and Mara Cadinu, *Checkmate? The role of gender stereotypes in the ultimate intellectual sport*, European Journal of Social Psychology, Volume 38, Issue 2, March/April 2008, 231-245.

[14] UNESCO, 2017: UNESCO Institute of Statistics, Fact Sheet No. 43, March, 2017, available at http://uis.unesco.org/sites/default/files/documents/fs43-women-in-science-2017-en.pdf

[15] Parkhi and Shroff, 2016: Sachin Parkhi and Gautam Shroff, *ACM Survey on PhD Production in India for Computer Science and Information Technology*, 2015-16, available at http://india.acm.org/PhDProductionReport2015_16.pdf

[16] Glenn, 2017: Marie Glenn, 2017, *Few good men: Why is the growing population of AI voices predominantly female?*, IMB Blog, 2 Mar, 2017, available at https://www.ibm.com/blogs/insights-on-business/ibmix/good-men-growing-population-ai-voices-predominantly-female/

[17] Bowick, 2009: Micol Marchetti-Bowick, *Is Your Roomba Male or Female? The Role of Gender Stereotypes and Cultural Norms in Robot Design*, Intersect, Volume 2, Number 1, 2009.

[18] Vassallo et al, 2015: Trae Vassallo et al, *Elephant in the Valley Survey 2015*, available at https://www.elephantinthevalley.com/

[19] Morse, 2017: Jack Morse, *Google Translate might have a gender problem*, Mashable, 1 Dec 2017, available at https://mashable.com/2017/11/30/google-translate-sexism/

[20] Bolukbasi, 2016: Tolga Bolukbasi, Kai-Wei Chang, James Zou, Venkatesh Saligrama and Adam Kalai, *Man is to Computer Programmer as Woman is to Homemaker?*

Debiasing Word Embeddings, 2016, available at https://arxiv.org/pdf/1607.06520.pdf

[21] Zhao, 2017: Jieyu Zhao, Tianlu Wang, Mark Yatskar, Vicente Ordonez and Kai-Wei Chang, *Men Also Like Shopping: Reducing Gender Bias Amplification using Corpus-level Constraints*, 29 Jul 2017, available at https://arxiv.org/abs/1707.09457

[22] Kay, 2015: Matthew Kay, Cynthia Matuszek, and Sean A Munson, *Unequal Representation and Gender Stereotypes in Image Search Results for Occupations*, ACM CHI Conference on Human Factors in Computing Systems, Apr 2015, available at https://www.researchgate.net/publication/271196763_Unequal_Representation_and_Gender_Stereotypes_in_Image_Search_Results_for_Occupations

[23] Haraway, 1991: Donna Haraway, *A Cyborg Manifesto: Science, Technology, and Socialist-Feminism in the Late Twentieth Century*, in Simians, Cyborgs and Women: The Reinvention of Nature, Routledge, 1991.

[24] Harding, 2015: Sandra Harding, *Objectivity and Diversity: Another Logic of Scientific Research*, University of Chicago Press, 2015.

[25] House of Lords, 2018: House of Lords, Select Committee on Artificial Intelligence, *AI in the UK: ready, willing and able?*, 16 Apr 2018, available at https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf

[26] NITI Aayog, 2018: NITI Aayog, *Discussion Paper - National Strategy for Artificial Intelligence*, Jun 2018, available at http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

[27] AI Task Force, 2018: Artificial Intelligence Task Force, Constituted by the Ministry of Commerce and Industry, Government of India, available at https://www.aitf.org.in/

[28] Abbasi, 2018: Ahmed Abbasi, Jingjing Li, Gari Clifford and Herman Taylor, *Make "Fairness by Design" Part of Machine Learning*, Harvard Business Review, 1 Aug, 2018, available at https://hbr.org/2018/08/make-fairness-by-design-part-of-machine-learning

[29] Cavoukian, 2011: Ann Cavoukian, *Privacy by Design - The 7 Foundational Principles*, 2011, available at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[30] Park et al, 2018: Ji Ho Park, Jamin Shin and Pascale Fung, *Reducing Gender Bias in Abusive Language Detection*, August, 2018, https://arxiv.org/abs/1808.07231

[31] Economist, 2018: *For artificial intelligence to thrive, it must explain itself*, 15 Feb 2018, available at https://www.economist.com/science-and-technology/2018/02/15/for-artificial-intelligence-to-thrive-it-must-explain-itself

[32] Weinberger, 2018: David Weinberger, P*laying with AI Fairness, People+AI Research Initiative*, available at https://pair-code.github.io/what-if-tool/ai-fairness.html

[33] Sczesny et al, 2016: Sabine Sczesny, Magda Formanowicz, and Franziska Moser, *Can Gender-Fair Language Reduce Gender Stereotyping and Discrimination?*, Frontiers in Psychology, 2016; 7: 25, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4735429/

ETHICAL FRAMEWORK FOR MACHINE LEARNING

Charru Malhotra[1], Vinod Kotwal[2], and Surabhi Dalal[3]

[1]Indian Institute of Public Administration, India
[2]Department of Telecommunications, India
[3]India Centre for Migration, India

ABSTRACT

Artificial Intelligence (AI) with its core subset of Machine Learning (ML) is rapidly transforming life experiences as humans begin to grow more dependent on these 'smart machines' for their needs – ranging from routine mundane chores to critical personal decisions. However, these transformative technologies are at the same time proving unpredictable too as has been reported worldwide in certain cases. Therefore, several studies/reports, such as COMEST report on Robotics ethics (UNESCO, 2017) point to an obvious need for inculcating more ethical behavior in machines. The present study aims to look at the role and interplay of ML (the hard sciences) and Ethics (the soft sciences) to resolve such predicaments that are inadvertently manifested by machines not constrained or controlled by human expectations. Based on focused review of literature of both domains-ML and Ethics, the proposed paper attempts to first build on the need for introduction of an ethical algorithm in the domain of machine learning and then endeavors to provide a conceptual framework to resolve the ethical dilemmas.

Keywords – Ethics, Artificial intelligence/machine learning, design approach, spiritual quotient, emotional quotient

1. INTRODUCTION

The field of study that deals with the development of computer algorithms for transforming data into intelligent action is known as machine learning (ML) [1]. The increase in ML is driven by simultaneous evolution of computational power and statistical methods to handle exponential collation and manipulation of data. Whenever an algorithm transforms itself into new actionable intelligence based on data, machine learning takes place. ML learns from experience and improves its performance as it learns [1].Basic learning process has three components *viz.* data input, abstraction and generalization; these are equally applicable to ML as well as humans though in the latter they take place subconsciously [2]. Thus, ML is best considered a subset of Artificial Intelligence (AI) where algorithms directed by complex neural networks teach computers to think like humans while processing "big data" and calculations with high precision, speed and supposed lack of bias [3].

Amongst many current applications, ML is being widely used to predict weather conditions, medical diagnosis, outcome of elections, facial recognition, criminal justice system, make predictions about credit worthiness, examine customer churn, automated traffic signals, targeted advertising etc.

The speed of growth of ML and its pervasiveness in our daily lives is being fueled by exponential growth in the 'big data'. However, bad data impacts the quality demands of ML in two ways, first on the historical data used to train the predictive model and secondly the new data used by that model to make future decisions. Thus, amongst other things, data must be *right data* (unbiased data) [25]. The ML algorithms running on the data are benefiting humanity, at large, but recent research is also uncovering many instances of biases in ML algorithms [3].Increasing application of and thereby dependence on ML is thus raising associated concerns including legal & social issues and ethical biases. The next question which then arises is that how do we eliminate/reduce biases? This links it to the question of ethics and ethical behaviour. Ethics affect every decision of our lives and they are one of the differentiating principles of how humans react in a given situation as opposed to machines that rely on machine learning and algorithms. Human beings possess conflicting moral opinions therefore the judgments are subjective. Ethical decision-making is essentially situational and the context defines what may be accepted as ethical or not. Every culture prescribes a certain 'code of ethics' which govern the group of people affiliated to that particular social or cultural group. In this backdrop, can we create machines that follow universally accepted ethical principles/guidelines/framework?

Etymologically, the term "ethics" corresponds to the Greek word "ethos" which means character, habit, custom, way of behavior etc. By the 17th century, 'ethics' was accepted as the science of morals, the rule of conduct, and the science of human duty. Ethics is treated as moral principles that govern a person's or a group's behavior and actions. In simple words, ethics refers to what is right and wrong and how to act on it. There is no single definition of ethics. Different definitions have their roots in the two basic philosophies of realism and idealism, or objectivism and interpretivism. The common thread in various theories and definition is that ethics concentrates on human actions or on the consequences of human actions. Thus, ethics may be defined as the systematic study of human actions from the point of view of their rightfulness or wrongfulness, as means for the attainment of ultimate happiness for individual and society [24].

In this paper we examine the (i) the interplay of ML and ethics; (ii) briefly discuss emerging ethical issues in use of ML that sometimes overlaps into AI; (iii) explore some 'existent frameworks' for managing ethical issues arising in ML; and (iv) suggest 'new parameters to manage ethical issues' and provide 'implementation strategies' as well as ' way forward'.

2. SCHOOLS OF THOUGHT AND PHILOSOPHIES ON ETHICS

The concept of ethics was originally proposed by the Greek philosopher Aristotle for the discussion of philosophical questions relating to daily life: the '*ethike theoria'* that deals with the study of, and gives criteria for the evaluation of human behavior. Since then, ethics has become one of the major topics in Western philosophy [21]. Ethics always change and they are handed down from one generation to the other. Therefore, what may have been correct or right or good for one may not be the same for another? Life does not always present us with the scenarios in black and white, rather we always encounter grey areas where every decision has an ethical implication and there is nothing exactly right or completely wrong; for instance, the Indian epic *Mahabharata* depicts complex characters who are fighting ethical dilemmas all the time. In general, ethics involves the analysis of conduct that can cause benefit or harm to other people [4].

In the western philosophy, there are many theories/schools of ethics *viz.,* egoism, hedonism, naturalism and virtue theory, existentialism, utilitarianism, contractualism and religion [26]. However, most commonly discussed are few. The first, the Virtue ethics inspired by *Nicomachean Ethics* by the Greek philosopher Aristotle (384-322 B.C.E.), holds that virtues (such as generosity, charity and justice) are dispositions to act in ways that benefit the possessor and society [5]. Another related thread of rational, inspired by German philosopher Immanuel Kant (1724-1804), holds the concept of duty central to morality. Kantianism is concerned about not what we do, but what we ought to do. What we ought to do reflects our dutifulness [4].

Unlike Kantianism, the theory of Utilitarianism that originates from philosophies proposed by Jeremy Bentham (1748-1832) and John Stuart Mill (1806-1873), examines right or wrong based on the consequences of an act or a rule. The utilitarian viewpoint asserts that guiding principle of conduct should be greatest happiness of the greatest number of people. In addition, Social Contract Theory , based on exposition and defense by Thomas Hobbes (1588-1679), John Locke (1632-1704), Jean-Jacques Rousseau (1712 -1778), John Rawls 1921- 2002), provides the justification for the establishment of moral rules to govern relationships among citizens as well as the mechanism capable of governing these rules-governments [6].

3. ETHICAL ISSUES IN MACHINE LEARNING

ML is continuously unleashing its power in a wide range of applications. Traditional roles performed by humans are now increasingly being taken over by machines and there are also concerns being raised in the literature about human workforce to be replaced by machines sooner than expected (for instance Rifkin, 1996) [39]. Google Assistant, inbuilt with the feature of "duplex" and IBM Debater are a case in point - both depict the move to build technology adept in undertaking meaningful conversations or arguments with a human companion, thus partially fulfilling human need of a companion [28] [8] but being 'robots' they are capable of 'recording' and 'analyzing' personal idiosyncrasies and behavioral preferences too.Similarly, ML based virtual assistants 'substituting' human beings in undertaking banking services have access to sensitive financial data. It is not an exaggerated presumption that such 'machine based assistance' would not only be susceptible to remote hacking from outside but also can be equally prone to 'instigation' of frauds from the machine 'itself' [7] a la' 'Winston', a conversational virtual assistant with AI abilities constructed to help Edmond Kirsch- the computer scientist, in the piece of fiction titled 'Origin' (Dan Brown, 2017).

The more we become reliant on machines, the more complex the relationship between humans and machines gets. There are also questions being raised on whether we have gone too far when computer generated imagery (CGI) can create realistic humans or when fake videos cannot be distinguished from the real ones [27]? Big data empowers ML algorithms to uncover more fine-grained patterns and make more precise predictions than ever before [32]. Complicating the matters further is the vast quantity of easily available data. ML is continuously unleashing its power in a wide range of applications. It has been pushed to the forefront in recent years partly owing to the advent of big data. ML algorithms have never been better promised while challenged by big data. Big data enables ML algorithms to uncover more fine-grained patterns and make more timely and accurate predictions than ever before [32]. There is easily available data to the machine to learn from and over a period of time it will become difficult to ascertain what the machine is learning and from where. By the year 2020, it is estimated that the total number of Internet-connected devices being used will be between 25 and 50 billion. As the numbers grow and technologies become more mature, the volume of data published will increase [33].However, this vast quantity of data that is available for ML should be correct, properly labeled, and *right data* [25]. There is however, a distinction between *right data* and *data is right* standards. *Data is right* standards may not be met as it might not be *right data* but also because there may be human errors during data collection; data creators may not know the purpose for what it will be used; poorly calibrated measurement tools etc.

The learning based on the quality of data and algorithms will inevitably lead to the machines learning both good as well as bad practices. Machine ethics is not merely science fiction; it is a topic that requires serious consideration, given the rapid emergence of increasingly complex autonomous software agents and robots. Machine ethics is an emerging field that seeks to implement moral decision-making faculties in computers and robots [9]. The increasing cases reported worldwide of machines harming humans or turning incapable of being assistance to humans shows how ethical concerns in the use of machine learning is an urgency that needs to be addressed quickly. The technological advancement should not take place in isolation rather it should come up with ways to mitigate accidental or intentional harms caused by the Artificially Intelligent machines relying on Machine Learning [10].

In information societies, operations, decisions and choices previously left to humans are increasingly delegated to algorithms, which may advise, if not decide, about how data should be interpreted and what actions should be taken as a result [11].

3.1 Methodology

The methodology adopted for this study is descriptive, exploratory, and analytical in nature based on review of literature. Secondary sources, related to the domain of both ML and ethics, have been referred to glean the existing philosophies and frameworks for which scholarly publications, related articles, research reports, and books have been examined. Since ML is an emerging domain, therefore references to social media have been made wherever appropriate. However, such public domain references might not have the desired academic rigor but such references have provided authors a larger understanding of emerging aspects of ML. These generic references have also helped the authors to debate on varied interpretations of emerging trends and have further aided in creating a bibliography to locate other important secondary sources. After collating all these aspects of the nascent domain, including the existing frameworks elaborating the interplay of ML and ethics. The authors have further classified learning's from the existing body of work and based on this attempted to propose a unique conceptual framework that is expected to lend strong 'ethical flavours' to the future attempts of the researchers, designers and policy makers associated with the domain of ML.

4. EXISTENT FRAMEWORK TO MANAGE ETHICAL ISSUES

Efforts are being made to address the concerns arising from the use of AI and ML by proposing guidelines/principles/frameworks. For instance, Isaac Asimov (1942) in his short story "Runaround" introduced the "three laws of robotics" to which fourth, or zeroth law was added by him later on in the year 1985 [29]. He envisioned a world where human-like robots would act like servants and would need a set of programming rules to prevent them from causing harm[30].These laws enunciated in a work of fiction are still mentioned as template for guiding development of robots [30] while at the same time being questioned for their relevance [31]. Moving on, the World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) of United Nations Educational, Scientific and Cultural Organization (UNESCO) proposes a technology-based ethical framework on robotics ethics based on the distinction between deterministic and cognitive robots (October, 2017). These relevant ethical principles and values include: (i) human dignity; (ii) value of autonomy; (iii) value of privacy; (iv) "do not harm" principle; (v) principle of responsibility; (vi) value of beneficence; and (vii) value of justice. The principle of human responsibility is the common thread that joins the different values that are enunciated in the report [12].

Wallach and Allen (2009) suggest two basic approaches of implementing machine morality: top-down and bottom-up — as well as a hybrid approach [13] . The top-down approach (**Figure 1**) is concerned with borrowing moral frameworks from philosophers including Kant (1724-1804),Hegel (1770-1831), Hume (1711-1776) and concepts like utilitarianism *et al* (referred in the previous section) and the system relies on these set of moral guidelines to make decisions in future. In the bottom-up approach the machine learns through manipulation just like a child learns morality while growing up similarly the machine through evolutionary algorithms learns to make ethically acceptable decisions. Wallach however also points out to the drawbacks of each of these approaches [14].

Recognizing the fact that powerful technologies like AI raise questions about its use, industry leaders have been proposing set of principles/guidelines to guide this area. Nadella, Microsoft CEO outlined ten essential rules to approach AI (2016). The first six rules on the list discuss what an ideal AI should contain or do. The remaining four rules stress on few important attributes that must be incorporated [34]. These rules clearly state that AI must prevent bias and also emphasize the need for empathy, education, creativity and focus on judgment and creativity. Similarly, Pichai (2018), has outlined the seven principles that will guide Google in its work forward in this area [15]. The seven principles are: (i) be socially beneficial; (ii) avoid creating or reinforcing unfair bias; (iii) be built and tested for safety; (iv) be accountable to people; (v) incorporated privacy design principles; (vi) uphold high standards of scientific excellence; and (vii) be made available for uses that accord with these principles. Of particular importance is the principle that lays down "avoid creating or reinforcing unfair bias". It is acknowledged in the post that "AI algorithms and datasets can reflect, reinforce, or reduce unfair biases. We recognize that distinguishing fair from unfair biases is not always simple, and differs across cultures and societies. We will seek to avoid unjust impacts on people, particularly those related to sensitive characteristics such as race, ethnicity, gender, nationality, income, sexual orientation, ability, and political or religious belief." [15]

Given the increasing autonomy of AI and ML it has become an arduous task to pin down as to who should be held responsible for bearing the ethical responsibility for the behavior of the machine. Time has come to discuss the ethics of the institutions and people behind the machines.

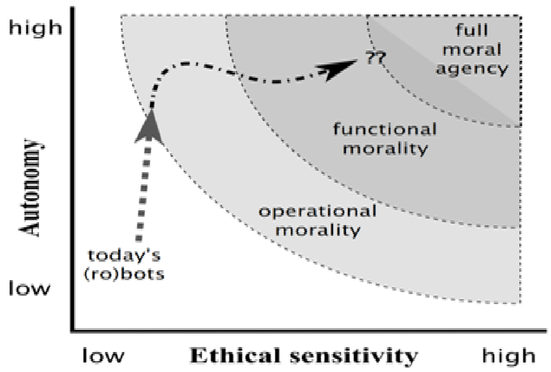


Figure 1 - Moral agency increases as autonomy and ethical sensitivity increase. [13]

5. 'ETHICAL FRAMEWORK' : PROPOSED NEW FRAMEWORK TO MANAGE ETHICAL ISSUES IN ML

This inherently interdisciplinary field of machine ethics actually lies at the intersection of domains of philosophy, cognitive science, psychology, computer science and robotics [14]. Today the machines have surpassed human intelligence and found groundbreaking solutions. For instance, Daniel Lobo and Michael Levin at Tufts University devised an evolutionary algorithm which successfully unraveled mysteries of the planarian worm's regenerative biology [16]. Touted as accurate predictors and efficient tools that increase accuracy when used in any given field, the push for greater dependence on ML and AI is increasing with Big Data. However, the central question at the heart of this discussion should be that are these machines really trustworthy and free of human prejudice only because they provide results based on numerical calculations. The algorithms or codes which are fed into the machines themselves are flawed, as they are encoded opinions of human beings who could be involved with the machine at any given stage in its production and training; which involves: gathering data, cleaning data, choosing algorithms, testing algorithms, selecting models, testing models, refining models and finally reaching at the operational model [18].

The flawed and biased opinions and prejudices of the human designers find ways to influence the machine learning. In such a case it is thus highly doubtful if one may bestow complete trust in a machine's decisions because these biased ideas only turn a machine into a weapon for silently inflicting harm.To overcome these issues a framework is being proposed to study the ethical dimensions in Machine Learning. The two axes i.e. the x-axis and y-axis represents Emotional Quotient (EQ) and Spiritual Quotient (SQ) respectively. IQ remains the only constant. The four quadrants represent the four areas of learning (**Figure 2**).

The approach is suggestive and works on the premise that the machine already possesses Intelligence Quotient (IQ). Presence of IQ thus fulfils the condition of rational clarity in decision-making. Moreover, the machine has access to data both archaic and new (through IOT and Big Data). On the other hand, EQ is used to express 'emotional intelligence' in the same way as IQ is used to express 'intelligence'. Mayer and Salovey (1990) offered the first formulation of a concept they called 'emotional intelligence' [35]. It refers to the ability to process emotional information accurately and efficiently. Goleman (2013) presented a model of E.I. that essentially comprises of five areas: self-awareness, self-regulation, empathy, social skills and motivation [36]. Similarly the term 'Spiritual intelligence' is a term that has been used by some philosophers, psychologists, and developmental theorists to indicate spiritual parallels with IQ (Intelligence Quotient) and EQ (Emotional Quotient). Zohar (1997) coined the term "spiritual intelligence" outlining twelve underlying principles of self-awareness, spontaneity, empathy, holism, compassion, being vision and value led, celebration of diversity, humility etc.[37].

The proposed conceptual framework is based on the premise that the person designing/ developing ML (henceforth, referred to as 'designer', for ease) would always have IQ whereas the other two quotients *viz.* EQ and SQ would oscillate from 'Low' to 'High' values in her personality type / design approach. This would lead to four personality types in a ML designer depending upon the variance of these two quotients in two stages (Low and

High) in a design. The four different possibilities that may emerge for a designer of ML algorithm can be classified as - 'Mechanical Learner', 'Cognitive Learner', 'Ethical Learner' and 'Ideal Ethical Master' as described below.

Possibility 1: Mechanical Learner (LOW EQ, LOW SQ)

The first stage in machine learning is when the machine becomes a mere mechanical learner because it relies on algorithms which are fed into its system by a designer who inherently has a low EQ and low SQ. This implies that the designer may not understand and respond to human emotions in a sensitive way or simply lacks empathy. The ability to feel for others is present but lacks empathetic response. The machine devoid of any emotional understanding will thus not think of the implications of its actions but by default will follow the commands as stated in its algorithm.

Low EQ does not mean presence of negative feelings rather it means a neutral response towards another being. A low SQ means the value clarification is not fully mature. Self and social awareness is undermined.

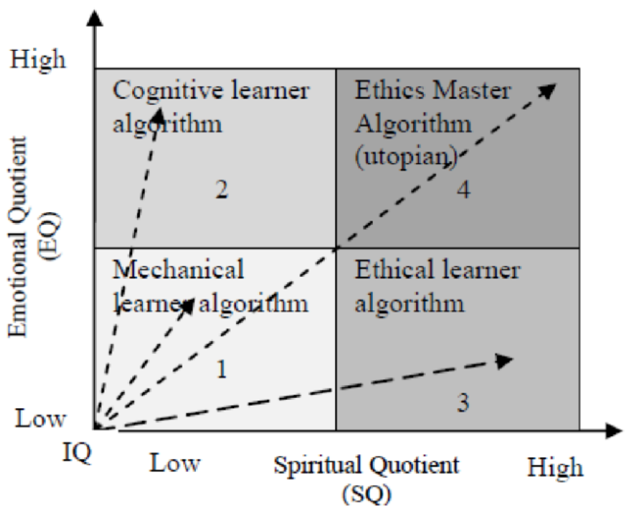


Figure 2 - Possible ethical dimensions for a designer of machine learning algorithms

Possibility 2: Cognitive Learner (LOW SQ, HIGH EQ)

This type of learning is acquired through an active use of emotions, thought processes and sensory perceptions. Psychologist Benjamin Bloom's Taxonomy of learning domains was altered in mid nineties to the domains in the order as: remembering, understanding, applying, analyzing, evaluating and creating [17]. Humans have evolved to this existing stage through cognitive learning approach and this is what actually separates humans from machines.

For a designer to lend a machine (through the algorithms designed by her) a low SQ, constant IQ but a higher level of EQ would make the machine 'behave' empathetic towards others and so the learning process in this case would be inclusive of remembering ethical frameworks of previous thinkers and concepts such as Utilitarianism and then understanding their applications in certain contexts. Such machines would therefore, learn by themselves which would make them susceptible to sometimes making unethical choices as well. The drawback would be that the ethical parameters are general in nature and just like humans may or may not find it ethically correct to stay true to a particular philosophy similarly the machine too would take the 'best guess prediction' which will be partially correct.

Possibility 3: Ethical Learner (LOW EQ, HIGH SQ)

With a low EQ imbued in the machine by its designer, the machine will not stay empathetic towards humans but with a high SQ it would have awareness of how the action of the self (machine) affects others around it. The Talisman of Gandhi (1958) is the best example here as it talks about how when one is faced by a dilemma, one should think of the implications of one's actions on the weakest person one can think of [40]. Such a machine, with Low EQ and High SQ, would be an ethical learner as it would be awakened to the needs of others and therefore, would think in terms of value clarification of the deeds performed by the self and their larger implications on those who may be at the receiving end.

Presumably, an ethical learner type of ML algorithms would be more acceptable as it will have the capacity to look beyond 'the self' and will have inclination to be of service to others (humans) and hence would inadvertently follow Asimov's Zero Law of Robotics too. The personality type of the designer, belonging to this quadrant will never design machine algorithms that are 'biased'. Such a machine will not voluntarily participate in discrimination against anyone based on previously highlighted markers such as race, class, sex, age etc.

Possibility 4: Ideal Ethical Master (HIGH SQ, HIGH EQ)

A high SQ and a high EQ (coupled invariably with the constant IQ) is the best case scenario which would be most ethical in nature, lending it almost an idealist dimension, an utopian existence. With such a designer, inking her algorithms, the machine in this quadrant would have invariably mastered ethical dilemmas and would function flawlessly without ever jeopardizing or compromising on someone's safety or life. A concern for harmony on earth and using ideas for careful utilization of resources makes this an ideal situation in machine learning, leading to a self-regulated system, suitable for all. Recapitulating, what has been previously stated regarding the subjective nature of ethical and moral understanding, this vision may never become true for a designer and hence for her machine too. However, this is what one can aim for the machines to move closer to behaving as sentient beings, and yet ensure that they not digress or regress.

6. IMPLEMENTATION STRATEGIES

Successful implementation of the proposed framework entails involvement of all the stakeholders from the highest national policy making organs of the government to the operational level implementation at the policy. Globally, governments across countries are seized of the need to have national level policies as well as bodies looking into the aspects of ethics in ML that can advise the governments on these complex issues. At the national level, they may be designated as Centre of Research Excellence for AI (COREs)[42] or Centre for Data Ethics and Innovation [43] and their mandate would be to work with experts drawn from different fields to develop an ethical framework. The ethical framework proposed in section 5 is at that higher level of thinking. Its implementation will however, require that this framework is publicized; policy changes are suggested covering private as well as public organisations; promotion of standards around the use of data; encourage research in emerging areas; and make guidelines focusing on incorporating the framework at the design stage, actively encourage transparency and auditability of the systems.

The next step in the implementation hierarchy would be at the organizational level. This would require changes in the hiring, training/capacity building, promotion and feedback policies of the organisations. The organisations would consciously need to focus on hiring persons who fit in the quadrant 2 &3 of the framework depending upon their requirement and also keeping in view the overall national policies governing this work. Incorporating ethical aspects at the design stage would be required and there may be a possibility of an 'ethics engineer' to be part of the team working on ML and AI solutions. Mere programming or algorithm writing will not address the underlying issues as ethics are a manifestation of intent as well as action. The 'ethics engineer's' job would be to fulfill the ethical requirements of the system from the time when the designers feed mathematical algorithms to a careful monitoring of how the machine uses its algorithms to fulfill the ethical objectives fed into it. Some of the broad principles that can be considered are:

Machine should be obedient to owner, designer and authority. Existing program cannot be erased without the authority and consent of system designer. There is need to provide degree of autonomy to machine. So that machine cannot erase some basic program however new cognitive learning program can be erased after some checks. Some basic program should be always locked and cannot be erased or hacked. If it get disturbed than machine should be put in shut down mode [23].

At the organizational level another aspect that requires attention is that most AI solutions suffer from "Black Box Phenomenon"[42] and an important step to tackle this would be to "open the black box". This can be achieved by the documentary auditing of algorithms and databases *posteriori*[44].

7. SUGGESTED WAY FORWARD

Since 'ethics' must become the cornerstone of AI/ ML in the global digital economy, there must be a united global efforts in this direction. First and foremost, there is a need for an ethical framework, which can serve as a standard for imbuing the 'Ethical Framework' in all intelligent machines in the world. For this, some international guidelines may be formulated by a consortium of global leaders. This global consortium also be empowered to monitor an insistent inculcation (with minor contextual modifications) of these guidelines by all the related organisations and governments involved in research and development of AI. Taking a cue from these global guidelines, appropriate interventions are required at the national level too. For instance, there must be appropriate regulatory framework, standards and templates in each country to enable integration of the proposed conceptual framework /design approach in the conventional approach of ML programming. There is also a need of a national authority as brought out in section 6 that periodically checks ethical indices of the various ML innovations in the country. Countries also need to establish a formal as well as an informal network of distinguished think tanks, academics, ethic advocates, practitioners and industry professionals, who could also have knowledge linkages with a similar consortium at global level. Such a cohesive global approach would help to steer the world towards a more ethical model of progress that is likely to emanate from ever-mushrooming AI/ ML based innovations.

8. CONCLUSIONS

With the threat of an Artificial Intelligence arms race looming large on the future of humankind on earth, it is an urgent requirement to speed up the process of introduction of ethical intelligence algorithms in machine learning. Cyber Security and privacy concerns are only going to further get complicated with increasing autonomy in machine learning. For the longevity of natural life on earth it is imperative we design algorithm for machines that become aware of what harmony, empathy, conservation of resources is. Humans need to secure not just their future but also life on earth in general.

Nevertheless, addition of spiritual and emotional quotient in the AI might also lead the machines to begin questioning existential questions that humans may already be facing such as finding the purpose in life etc. The machines will perhaps even lose their rational approach towards things if they are conditioned to think on emotional and spiritual lines which also will make it hard to allow them to fulfill their purpose of being human-centric. We design new things to suit our requirements but if the machines begin to face the same dilemmas that we humans do then we would have accomplished the unthinkable of turning non-living entities into sentient beings.

Whether our ethical practices are Western (Aristotelian, Kantian), Eastern (Shinto, Confucian), African (Ubuntu), or from a different tradition, by creating autonomous and intelligent systems that explicitly honor inalienable human rights and the beneficial values of their users, we can prioritize the increase of human well-being as our metric for progress in the algorithmic age [19]. This will lead to building of trust amongst the communities that ML or AI are designed to serve; build trust across national, cultural and organizational boundaries; and most importantly prove that these systems are demonstrably trustworthy [41].

Acknowledgements: The authors are indebted to Ishita Malhotra (Growth Manager, KnoitHQ, Fairfax, Virginia) and Gaurav Khandelwal (Assistant Consultant, TCS) for their invaluable research support despite their pressing official engagements.

REFERENCES

[1] S. A. Bini, "Artificial Intelligence, Machine Learning, Deep Learning, and Cognitive Computing: what do these terms mean and how will they impact health care?," The Journal of Arthroplasty (2018), doi: 10.1016/j.arth.2018.02.067

[2] B. Lantz, Machine Learning with R, Packt Publishing, 2013.

[3] A. Yapo and J. Weiss, “Ethical Implications of Bias in Machine Learning.” In Proceedings of the 51st Hawaii International Conference on System Science, 2018. <https://aisel.aisnet.org/hicss-51/os/topics_in_os/6/>

[4] R. Herschel and V.M. Miori, “Ethics & Big Data”, Technology in Society, (49), 2017, pp. 31- 36

[5] Rosalind Hursthouse, "Virtue Ethics", The Stanford Encyclopedia of Philosophy (Fall 2013 Edition), Edward N. Zalta(ed.),URL<http://plato.stanford.edu/archives/fall2013/entries/ethics-virtue/>.

[6] C. Friend, “Social Contract Theory.” In Internet encyclopedia of philosophy. 2016 URL<http://www.iep.utm.edu/soc-cont/>

[7] PTI, “Alexa, Siri can now do personal banking - but, may also reveal your a/c balance at a party!” In The Economic Times. URL<https://economictimes.indiatimes.com/magazines/panache/alexa-siri-can-now-do-personal-banking-but-may-also-reveal-your-a/c-balance-at-a party/articleshow/64662888.cms>

[8] E. Lieberman, “Man Vs. Machine: IBM’s Artificial Intelligence Debates Human In A Contest.” In The Daily Caller. URL< 2018/06/19/man-vs-machine-ibms-artificial-intelligence-debates-human-in-a-contest/>

[9] C. Allen and W. Wallach, et al."Why Machine Ethics?", IEEE Journal of Intelligent Systems, Vol. 21, No. 4, pp. 12-17, 2006.

[10] T. Simonite, “Artificial Intelligence Seeks An Ethical Conscience.” In Wired.com dated 12.07.17. URL < https://www.wired.com/story/artificial-intelligence-seeks-an-ethical-conscience/>

[11] B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, “The ethics of algorithms: Mapping the debate”, Big Data & Society (BD&S), Vol. 3 No. 2, Article first published online: December 1, 2016; Issue published: December 1, 2016 URL <https://doi.org/10.1177/2053951716679679>

[12] UNESCO, “Report of World Commission on the Ethics of Scientific Knowledge and Technology (COMEST) on Robotics Ethics.” SHS/YES/COMEST -10/17/2 REV. Paris, 2017. URL <http://unesdoc.unesco.org/ images/0025/002539/253952e.pdf>

[13] W. Wallach, and C. Allen, Moral Machines: Teaching Robots Right From Wrong, Oxford University Press, 2009.

[14] S. Yu, “Machine Morality: Computing Right And Wrong.” Yale Scientific Magazine . 2012. Web. 29 Nov. 2016. URL <http://www.yalescientific.org/2012/05/machine-morality-computing-right-and-wrong/>

[15] S. Pichai, “AI at Google: our principles”. Google URL <https://blog.google/technology/ai/ai-principles/> Published Jun 7, 2018

[16] D. Lobo, and M. Levin, “Inferring Regulatory Networks from Experimental Morphological Phenotypes: A Computational Method Reverse-Engineers Planarian Regeneration.” PLoS Computational Biology. Vol. 11, No. 6, Web 2015. URL https://doi.org/10.1371/journal.pcbi.1004295

[17] L.W. Anderson, D.R. Airasian et al, A Taxonomy for Learning, Teaching, and Assessing: A revision of Bloom's Taxonomy of Educational Objectives, New York: Pearson, Allyn & Bacon. 2001.

[18] C.S. Penn, “How Machine Learning Introduces Unconscious Biases.” Retrieved from URL <http://www.christopherspenn.com/2017/08/how-machine-learning-introduces-unconscious-biases/> dated Aug 16, 2017

[19] The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, “Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems.” Version 2. IEEE, 2017. URL <http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html>

[20] Kantian Ethics, available at URL: <http://www.csus.edu/indiv/g/gaskilld/ethics/Kantian%20Ethics.htm>

[21] M Iaccarino,2001. Science and ethics – NCBI from URL < https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1084045/>

[22] Yersu Kim (Division of Philosophy and Ethics UNESCO) Paris (September 1999). "A Common Framework for the Ethics of the 21St Century".

[23] V Conitzer,Duke University (2017)."Moral Decision Making Frameworks for Artificial Intelligence".

[24] W Jose, IGNOU - 2017 "An Introduction to ethics", "Ethical Concerns in Public Administration".

[25]If your data is bad, your machine learning tools are useless available on URL: https://hbr.org/2018/04/if-your-data-is-bad-your-machine-learning-tools-are-useless (accessed on 22.06.2018)

[26]Eight theories of ethics, Gordon Graham on URL: https://philpapers.org/rec/GRAETO (accessed on 23.06.2018)

[27] What is left for us human beings? Available on URL: https://www.pressreader.com/india/hindustan-times-delhi/20180623/281943133610529 (accessed on 23.06.2018)

[28] The Google Assistant will soon be able to call restaurants and make reservations for you available on URL: https://techcrunch.com/2018/05/08/the-google-assistant-will-soon-be-able-to-call-restaurants-and-make-a-reservations-for-you/ (accessed on 23.06.2018)

[29]Three laws of Robotics at URL: https://en.wikipedia.org/wiki/Three_Laws_of_Robotics (accessed on 23.06.2018)

[30] Isaac Asimov's three laws of Robotics need updating ; available at URL: https://theconversation.com/after-75-years-isaac-asimovs-three-laws-of-robotics-need-updating-74501 (accessed on 23.06.2018)

[31] Isaac Asimov's law of robotics are wrong; available at URL: https://www.brookings.edu/opinions/isaac-asimovs-laws-of-robotics-are-wrong/ (accessed on 23.06.2018)

[32] Zhou, L., S. Pan, et al. (2017). "Machine learning on big data: Opportunities and challenges." Neurocomputing 237: 350-361

[33] Mahdavinejad, M. S., M. Rezvan, et al. (2017). "Machine learning for Internet of Things data analysis: A survey." Digital Communications and Networks

[34] A. P. Chaudhury, "Microsoft CEO Satya Nadella rolls out 10 rules that will define Artificial Intelligence". From URL < https://analyticsindiamag.com/microsoft-ceo-satya-nadella-rolls-10-rules-will-define-artificial-intelligence/>

[35] Salovey, P. and Mayer, John D. (1990) Emotional Intelligence, Imagination, Cognition and Personality , Vol 9, Issue 3, pp. 185 - 211

[36] D. Goleman, "Emotional Intelligence". From URL<https://www.learning-theories.com/emotional-intelligence-goleman.html>

[37] Zohar, D. (1997). Rewiring the corporate brain: Using the new science to rethink how we structure and lead organizations. Berrett-Koehler Publishers.

[38] Musk, Elon (2014), Centennial Symposium , MIT Aeronautics and Astronautics Department, October 22-24, 2014. URL - http://webcast.amps.ms.mit.edu/fall2014/AeroAstro/index-Fri-PM.html

[39] Rifkin, J. (1996). New technology and the end of jobs. The case against the global economy, 108-121.

[40] Mahatma Gandhi [Last Phase, Vol. II (1958), P. 65] "I will give you a talisman. Whenever you are in doubt, or when the self becomes too much with you, apply the following test. Recall the face of the poorest and the weakest man [woman] whom you may have seen, and ask yourself, if the step you contemplate is going to be of any use to him [her]. Will he [she] gain anything by it? Will it restore him [her] to a control over his [her] own life and destiny? In other words, will it lead to swaraj [freedom] for the hungry and spiritually starving millions? Then you will find your doubts and your self melt away."

[41]https://news.itu.int/welcome-to-trustfactory-ai-nine-projects-to-build-trust-in-ai/

[42] National Strategy for Artificial Intelligence #AI for all (June 2018); available at URL: http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf (accessed on 07.10.2018)

[43]AI in the UK: ready, willing and able? (April 2018); available at URL:https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf (accessed on 05.10. 2018)

[44] For a meaningful Artificial Intelligence –Towards a French and European Strategy (March 2018). Available at URL: https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

UNDECLARED CONSTRUCTIONS: A GOVERNMENT'S SUPPORT DEEP LEARNING SOLUTION FOR AUTOMATIC CHANGE DETECTION

Pamela Ferrari Lezaun; Gustavo Olivieri

Department of Systems Information Engineering, Universidad Tecnológica Nacional FRSF, Santa Fe, Argentina

pferrari@frsf.utn.edu.ar, golivieri@frsf.utn.edu.ar

ABSTRACT

In our cities, in particular those with high demographic density, the proliferation of buildings goes so fast that it is not possible or -in the best scenarios- very difficult to be handled by the government departments regulating the legitimacy -in term of safety and taxes- of those constructions.

In this paper, we propose a deep learning tool for computer vision trained with a corpus of satellite images provided by SpaceNet to detect changes in cities, showing the most recent constructions automatically, which allows different municipal officers to check if they have been -or haven't been- declared. To achieve this, we implemented the layered architecture of the SpaceNet Challenge Round 2 winning solution, and decided to improve it with an output comparison which gives us a high value final result for the end-user in the detection of changes, giving him the possibility to appreciate in the graphic user interface how many new buildings and square meters were detected.

Keywords – building detection, undeclared constructions, illegal construction, Machine learning, computer vision

1. INTRODUCTION

In Argentina, millions of undeclared square meters are built every year. Just in the province of Buenos Aires, 14 million square meters were detected in the last few years without registration [1]. As can be seen in Figure 1, just in 2018 half million square meters with irregularities were detected in that province [2]. Many of these infractions involve parcels where industries and active businesses operate but are still registered as vacant parcels.

In 2017, The Direction of land registry office of Plottier in Neuquén Province indicated that estimated clandestine constructions hovered 250.000 square meters and in the capital of that province about half on that number [3]. This situation could also be reflected, to a different extent, in many countries around the world. In Hong Kong, for example, 25% constructions have illegal structures [4]. Another case is in Bulgaria, where the illegal buildings in preserved areas are a threat to the biological diversity [5].

Bearing in mind that with all the aforementioned, much less tax revenue will be obtained, thus, representing great economic losses for the governments of the cities. Due to the nature of the taxes, in one way or another will end up affecting the citizens.

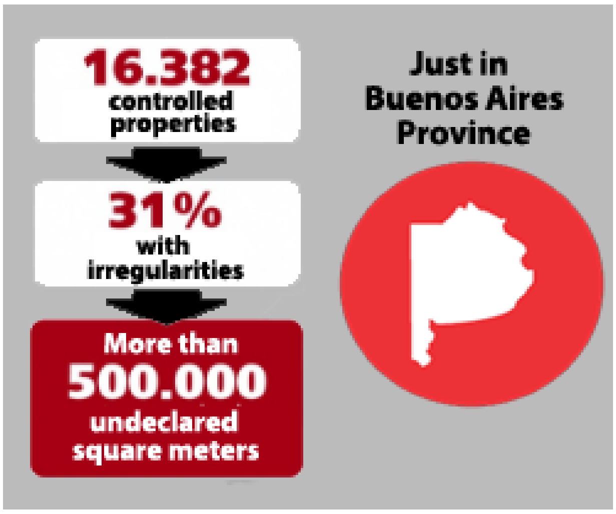


Figure 1 - Statistics of illegal constructions in the province of Buenos Aires.

In the same way, the lack of regulation in building constructions would lead to the non-detection of structural problems that may end in great tragedies such as landslides.

The number of provinces in Argentina -and many regions around the world- facing the same problem are rising constantly. The problem has been mentioned in different academic articles [6, 7, 8], allowing to determine that it is present in many places around the world, all of them with a point in common: the complexity to detect illegal square meters is given by the lack of a tool that can assist different municipal or provincial officers in the detection of undeclared constructions, in process or already finished.

It should be noted that in some countries, the government is investing and implementing projects of this magnitude, as is the case of Spain through the public company of cartography of Canarias (GRAFCAN), who on June 1 of 2017 released a statement in its official page that says "The control of changes in the territory applying Deep Learning techniques to orthophotos is just the first example of the capabilities that the combination of Artificial Intelligence and spatial information can offer for the generation of territorial knowledge." [9]. Such a statement serves as a proof of evidence that there are professionals and specialized technicians working with these techniques which are to be applied, extended and consolidated in the next years. The proposed solution is our contribution to get an innovative, feasible and time scalable solution.

In conclusion, the main goal of the project is to propose the development of a software solution to support the detection of changes in building structures, comparing satellite images with the help of deep learning algorithms.

The paper is structured as follows: Section 2 presents the proposed system. Section 3 provides details of the dataset. Section 4 explains the Deep learning model to be implemented. Section 5 defines the image comparison process. Section 6 presents the results and introduces the final discussion.

2. PROPOSED SYSTEM

To achieve the main objective of this project, the already defined specific goals had to be achieved. First and foremost, an images dataset which would serve as input to the training algorithm was defined. Then, it was necessary to define the machine learning model to be used in detecting buildings in a satellite image, taking into account the tools, libraries, algorithms and architectures commonly used in image processing and computer vision. The next task was to implement the model, defining an error measure and validating it from said measurement, enabling a comparison between two outputs spaced in time to detect possible changes. In the following sections, we will describe each goal, and finally make conclusions and analyze the results.

As it is well known, machine learning algorithms have roughly two stages: training and prediction (or inference). For the training, it is necessary to have an input dataset that will be the "food" of the algorithm in order to begin detecting patterns that in the future, in the inference stage, would allow it to perform its work with greater or lesser accuracy. In addition, and in general, the data requires a preprocessing so that they can be useful to the machine learning algorithm that will use them.

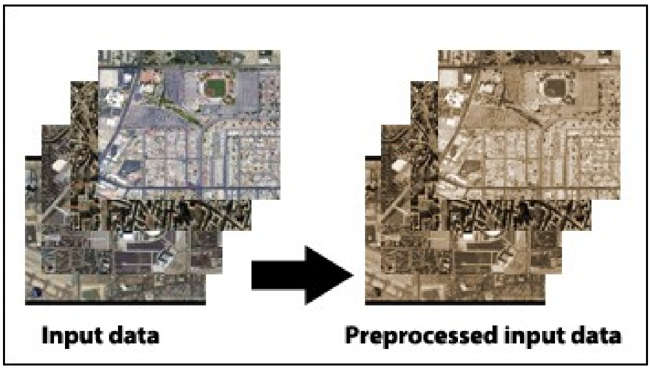


Figure 2 – Two stacks of images: the original input on the left and the preprocessed input on the right

All the aforementioned was a great challenge considering that, for the purpose of this project, the input data should be a large number of high-quality satellite images which have a limited availability, and, generally, a high price. Otherwise, it would be very likely that the algorithm, even if trained with many images of low quality, would yield poor results.

As seen in abstract form in Figure 2, the corpus of images obtained is preprocessed, to be used afterward as input for the layer structure of the machine learning algorithm. Based on certain parameters, and after finishing the process, the algorithm will have the ability to detect what is and what is not a construction. At this point it is absolutely necessary to test the results through the error analysis defined at the time, to make sure that the level of detection accuracy is high enough so that it is possible to obtain useful output data.

The result of the previous process would be an algorithm with parameters trained to delimit the location of the buildings in a satellite image. This output is useful, but it still does not represent the final result yet. Indeed, it is important to achieve it because human vision allows in itself to identify the same, in less time and even more accurately than the computer vision. That is why the output of the trained algorithm is only useful if it is used as input for a new algorithm, which will be responsible for comparing two outputs at different times, in order to determine which elements can be found in image A but cannot be found in image B, as can be seen in Figure 3.

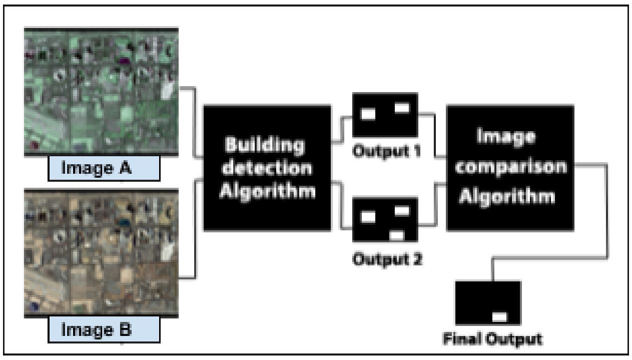


Figure 3 – Flow of input data until its final output

Finally, the wanted output is achieved. The remaining details have to do simply with non-functional requirements, such as the way in which the output will be presented to the users so that they could evaluate it and give it, or not, utility. The mockup in Figure 4 represents the proposed graphic user interface. It shows the number of buildings and square meters detected in the same coordinates but at different times

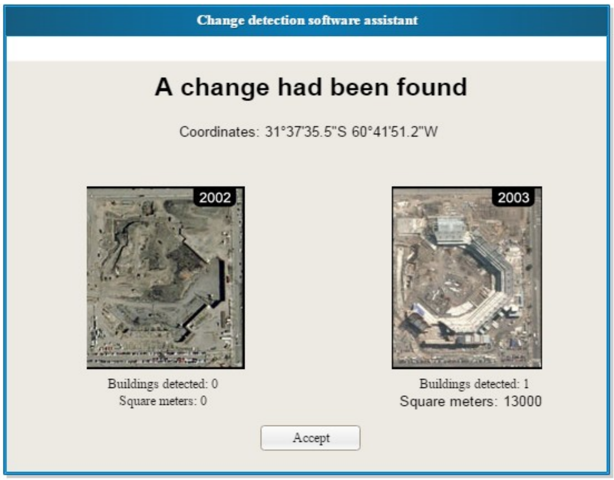


Figure 4 –Example of graphic user interface model.

3. DATASET DETAIL

To have a successful result, a big challenge was to find a large volume of input data with a high resolution. This allows training the algorithm in such a way that a parameter configuration with an acceptable precision for the expected ranges could be obtained.

It is necessary to know that the search is not particularly simple, considering that the higher resolution images are not available for free. Free access to satellite images only occurs in satellites such as LandSat [1], which generates periodic images but with the great disadvantage that they have low resolution, which makes them useless for identifying patterns in small buildings. Companies like DigitalGlobe offer images of very good resolution, but at a high cost. Due to the nature of the project, the volume required is very high as well as the cost to obtain them. It would be almost impossible to face both situations considering the academic nature of this project.

A consortium of companies including DigitalGlobe, CosmiQ Works and NVIDIA launched SpaceNet [10] in 2016, an online repository of satellite images and co-registered map data to train algorithms. It is a corpus of commercial satellite imagery and labeled training data to use for machine learning research. The corpus of images with an excellent resolution (they are satellite images of 0.3m), is not only available for access, but it also has geolocated labels to delimit buildings, perfect for training the algorithm. What is even better, the corpus is divided into two volumes: the first, aimed to train algorithms -about 40GB-, and the second, to perform validation tests -about 20GB-. Last but not least, there are different image alternatives, such as RGB images, panchromatic images or 8 multispectral bands. The package includes images of four cities: Las Vegas, Paris, Shanghai and Khartoum, which allows us to test the algorithm in various urban structures.

All of the above represents an almost perfect combo for the project needs. It is almost perfect because although it allows training the algorithm and tests its accuracy it does not have images at different times from the same geographical place so that, in the final output, we can obtain the expected results. That is why, for the final testing stage, it was decided to generate changes in the satellite images artificially to visualize in the final output the way in which the changes produced are detected. This decision, although not ideal, allowed us to continue with the project without major consequences since, although the scenario we were generating was fictitious, it was sufficiently representative of reality to be useful.

4. DEEP LEARNING BUILDING DETECTION MODEL

For the detection building model, two options were possible: to create a new model or reusing models already evaluated and with a useful function for the project scope. Both options have advantages and disadvantages. For example, lacking experience in these issues, the making of a new model, implied to start down on the learning curve. It is necessary to check continuously if the architecture is correct and, if not, proceeds to accordingly correct the errors. On the other hand, when reusing models with a checked architecture and a solution within limits of tolerable errors is good, but implies this solution to be adapted to the needs of the present project.

The SpaceNet algorithms [11] which are in the public repository and with a free-use license were used considering that it was the most appropriate solution for this

1 The Landsat Program is a series of Earth-observing satellites co-managed by USGS & NASA and offers the longest continuous space-based record of Earth's surface.

case. Particularly, the winning solution of the SpaceNet Round 2 competition, created by Kohei Ozaki, was chosen [12]. Such neural network model has two images input: those images that were mentioned in the last section -in particular, panchromatic images-, but he also includes, to achieve accuracy in detection, OpenStreetMap[2] maps, that is, free and editable maps with geographic information that are distributed under open license. The final input to the neural network is then the concatenation of both sources (Figure 5).

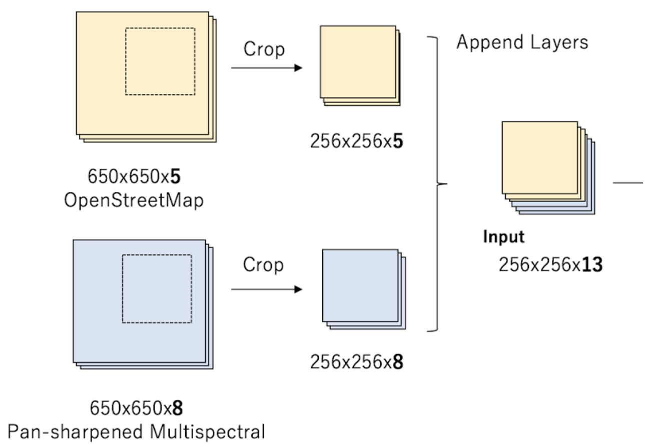


Figure 5 – The final input combines OpenStreetMap and pan-sharped multispectral images in the same stack.

According to this input, the next step was to decide the layers structure of the neural network. First, it is necessary to introduce the U-Net neural network architecture. U-Net is a convolutional network for fast and precise segmentation of images, so that is particularly useful for the processing of satellite images [13].

The architecture of U-Net consists, like any other convolutional network, in a large number of different operations, illustrated by the model in Figure 6. The 'input image tile' represent the input of the images and then the data is propagating through the network along with all possible steps and, in the end, the ready segmentation map comes out.

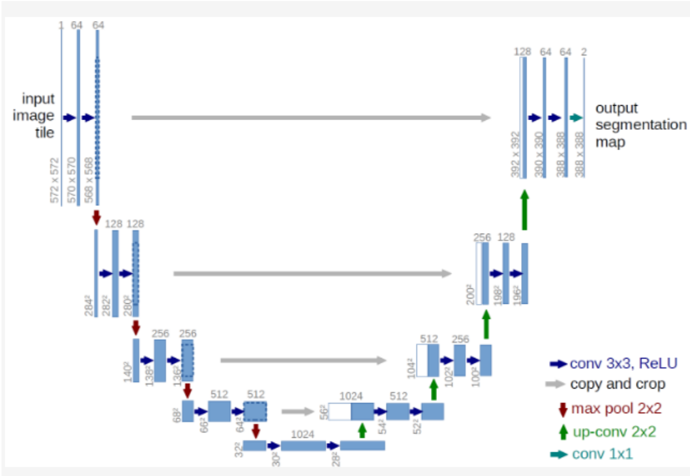


Figure 6 – Architecture of U-Net: a multi-channel feature map

The blue boxes correspond to a multi-channel feature map and the white boxes are copied feature maps. Like a blue box represents a multi-channel, the number of channels is denoted on top in the box and the bottom left edge of the box provided the dimension. The arrow between two blue boxes represents the convolution activation function.

Then continuing with Ozaki's architecture, the model in Figure 7 is an alteration of the U-Net architecture for images segmentation. Basically, each layer represents two convolutional operations, with a 3x3 kernel, performing a nonlinear function. After that, it moves on to the next layer.

In the architecture, a progressive subsampling is made until a kernel of 3x3@512 is reached (that is, a kernel of 3x3 is applied in the operation and 512 filters are obtained in the output of the convolution). Then, a progressive upsampling is performed until the data reaches the output layer. This layer will give an image with the same dimensions of the input image, with the segmentation made. After all this process, for each layer not only will be used as input the output of the previous layer after doing an upsampling. The input will also include the output of the layer that presents the analogous dimensions of kernel and image.

2 OpenStreetMap (OSM) is a collaborative project to create a free editable map of the world

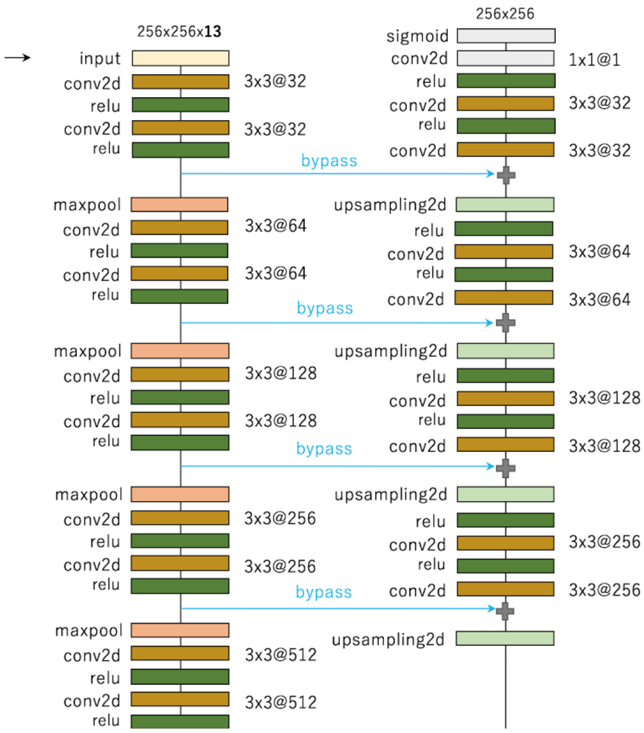


Figure 7 – Kohei Ozaki's ConvNet Architecture

Fortunately, for the project's feasibility, the model described above, together with its source code, is available for free use in a Docker container, which allows, having enough hardware and software resources, to train the network and to use it by deploying the container and executing basic instructions in the command line.

Particularly, the container was deployed in a p2.xlarge instance of Amazon Web Services, with an Ubuntu 16.04 operative system. This instance has the advantage of having 61GB of RAM memory and a nVidia K80 Tesla GPU, enough resources to obtain an acceptable performance according to the needs of the project.

After running the code, a trained algorithm ready to be used in its inference stage will be obtained. It will be ready to give a sufficiently accurate response of what is and is not a building in a satellite image.

Table 1 shows the accuracies obtained from the test data for each of the cities. The values were obtained using the F-Score metric, following these steps to calculate them. For each polygon (probable construction) that the algorithm was capable to detect, these 4 steps are followed: 1- Discard the polygon if it was already matched with another solution polygon. 2- Discard the polygon if is not related to the polygon with which it has matched. 3- If none of the above options occurred, calculate the IOU (Intersection over Union, Jaccard index) [14] of the matched polygons. 4- Discard the polygons with an IOU lower than 0.5.

For each iteration of the above steps, the count of true positives (TP) will be increased by one for each matching polygon found, the count of false positives (FP) will be increased by one for each non-matching polygon and finally, when every detected polygon was processed, for each unmatched polygon (undetected truth polygons) the count of false negatives (FN) will be increased by one.

The precision and recall of the algorithm are defined as follows:

$$Precision = TP/(TP + FP)$$

$$Recall = TP/(TP + FN)$$

Finally, the F-score of the algorithm is defined as 0 if either Precision or Recall is 0. Otherwise:

$$F_{score} = \frac{2 * Precision * Recall}{Precision + Recall}$$

Table 1 – Algorithm accuracy in each city with the F-Score metric [15]

City	Accuracy
Las Vegas	0.885
Paris	0.745
Shanghai	0.597
Khartoum	0.544

This is the great starting point for the main objective: the detection of changes. Comparing the outputs of the inference algorithm is what will allow us to finally achieve what is expected, which is developed in the next section.

5. IMAGE COMPARISON

Regarding the image comparison, the output of the building detection algorithm is helpful to compare two inputs spaced in time and know if changes occurred or not. With this objective, it was decided to make modifications to the algorithm mentioned in the last section. Since it has the capacity to obtain the area of the polygons that it detects, it is possible to determine for specific coordinates, how many square meters of construction were found. Then, if for the same coordinates the inference algorithm is run again with a new image input -temporarily spaced from the first image-, it is possible to get the new quantity of square meters in this zone, in such way that if the difference between them is significant, it can be assured that the area has changed.

Input images have a size of 200mx200m, when there is a change in some sector within this square, it is necessary to identify in some way to which geographical area corresponds that portion that suffered modifications. To achieve this, the 200x200 squares will be labeled with a unique ID that identifies them. And within them, it will be necessary to have a history of areas (square meters) detected as constructions over time, to later be able to compare if any property increased in square meters or there are more buildings.

In order to correctly perform the aforementioned tasks, it is necessary to define an acceptable margin of error, because otherwise, if the difference in square meters detected was due to an error in the detection algorithm, changes would be identified where they do not exist, that is; a false positive.

Finally, those areas of 200mx200m in which a change has been found -the ones that the surface difference is greater than the tolerance level- will be shown to the user, who must determine in the software's final output what construction is new, and subsequently, verify it was declared or not.

6. RESULTS AND DISCUSSION

Our intention is that the software, in future implementations, shows the user on screen the constructions that have changed and reframe them as a screen display, instead of just for the 200mx200m areas as it happens at this moment. With the current approach it is possible to limit the revision of the user only to those tables where there are actually changes in buildings, however, it does not leave aside the tedious task of having to identify which construction is new on a map.

We considered that it is possible to make some changes to improve this project and we propose that the corpus of satellite images provided by SpaceNet could be replaced by a drone and it could take the images of the cities and send them using the future 5G network. On the one hand, this solution is more inexpensive than buying a huge dataset of satellite images to companies and even each city could have their corpus image in a database with weekly or monthly updates.

We hope that cutting-edge technologies can be used to prevent undeclared buildings in preserved forest areas to protect the environmental biodiversity as well as be able to avoid tragedies caused by terrible building construction.

7. REFERENCES

[1] Sylvestre G. "Se está notificando a 2,5 millones de contribuyentes para que se pongan al día". Gustavo Sylvestre Journal. Buenos Aires - Argentina. April 1 2014 http://www.gustavosylvestre.com/politica/se-esta-notificando-a-25-millones-de-contribuyentes-para-que-se-pongan-al-dia-dijo-el-titular-de-arba/

[2] Cermele L. "Arba detectó más de 500 mil metros cuadrados sin declarar". Radio Provincia - Buenos Aires, Argentina. March 28, 2018 https://www.gba.gob.ar/radioprovincia/noticias/arba_detect%C3%B3_m%C3%A1s_de_500_mil_metros_cuadrados_sin_declarar

[3] Suarez M. "Neuquén tiene más de un millón de metros cuadrados sin declarar". Río Negro Journal. Neuquén, Argentina. April 26, 2017. https://www.rionegro.com.ar/region/neuquen-tiene-mas-de-un-millon-de-metros-cuadrados-sin-declarar-NH2669942

[4] Zhao S. "One in four Hong Kong properties has illegal structures, but most owners get away with their misdeed". South China Morning Post Journal. Hong Kong. January 22, 2018. http://www.scmp.com/news/hong-kong/law-crime/article/2129906/one-four-hong-kong-properties-has-illegal-structures-most

[5] European Green. "Restriction of illegal construction in preserved areas". Geneva, Italy. October 15, 2006 https://europeangreens.eu/content/restriction-illegal-construction-preserved-areas

[6] Faton Spahiu, Rineta Jashar. "The legalization process challenges on Illegal constructions in Kosovo". University for Business and Technology Faculty of Architecture and Spatial Planning. July 18, 2016. https://www.researchgate.net/publication/305391468_The_legalization_process_challenges_on_Illegal_constructions_in_Kosovo

[7] Charalabos IOANNIDIS, Christodoulos PSALTIS, Chryssy POTSIOU. "Towards a strategy for suburban informal building control through automatic change detection". School of Surveying Engineering, National Technical University of Athens, Greece. 2007. https://www.researchgate.net/publication/253881637_Towards_a_strategy_for_suburban_informal_building_control_through_automatic_change_detection

[8] Rui LIU, Yun-Fan LI. "Research on application mode of monitoring the illegal constructions for sale based on multi-source data and 3S technology—a case study in Shenzhen, China". Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, 518055, China. Center for Assessment and Development of Real Estate, Shenzhen, 518040, China. Yangze River Scientific Research Institute, Wuhan 430010, China. January 2016. https://www.researchgate.net/publication/310660513_Research_on_application_mode_of_monitoring_the_illegal_constructions_for_sale_based_on_multi-source_data_and_3S_technology-a_case_study_in_Shenzhen_China

[9] CARTOGRAFICA DE CANARIAS, S.A. (GRAFCAM) "inteligencia Artificial aplicada a detección de cambios en el territorio." Canarias, Spain. June 01, 2017. https://www.grafcan.es/2017/06/inteligencia-artificial-aplicada-la-deteccion-de-cambios-en-el-territorio

[10] SpaceNet on Amazon Web Services (AWS). "Datasets." The SpaceNet Catalog. Last modified April 30, 2018. Accessed on [May 15, 2018]. https://spacenetchallenge.github.io/datasets/datasetHomePage.html

[11] SpaceNetChallenge. "Building detection algorithms from second SpaceNet Challenge" https://github.com/SpaceNetChallenge/BuildingDetectors_Round2

[12] Ozaki K. "Winning Solution for the Spacenet Challenge: Joint Learning with OpenStreetMap". June 14, 2017 https://i.ho.lc/winning-solution-for-the-spacenet-challenge-joint-learning-with-openstreetmap.html

[13] Ronneberger O., Fischer, P., BroxT. "U-Net: Convolutional Networks for Biomedical Image Segmentation". Dept. of Computer Science, Faculty of Engineering, University of Freiburg. Vol.9351: 234--241. 2015. https://lmb.informatik.uni-freiburg.de/people/ronneber/u-net/

[14] Adrian Rosebrock. "Intersection over Union (IoU) for object detection". November 7, 2016 https://www.pyimagesearch.com/2016/11/07/intersection-over-union-iou-for-object-detection/

[15] Lindenbaum D. "2nd SpaceNet Competition Winners Code Release". Medium. Jul 26, 2017. https://medium.com/the-downlinq/2nd-spacenet-competition-winners-code-release-c7473eea7c11

ABSTRACTS

Session 1: Machine Learning in Telecommunication Networks - I [1]	
S1.1	**Invited Paper -** A Machine Learning Management Model for QoE Enhancement in Next Generation Wireless Ecosystems *Eva Ibarrola (University of the Basque Country (UPV/EHU), Spain); Mark Davis (Dublin Institute of Technology (DIT), Ireland); Camille Voisin and Ciara Close (OptiWi-fi, Ireland); Leire Cristobo (University of the Basque Country (UPV/EHU), Spain)* Next-generation wireless ecosystems are expected to comprise heterogeneous technologies and diverse deployment scenarios. Ensuring a good quality of service (QoS) will be one of the major challenges of next-generation wireless systems on account of a variety of factors that are beyond the control of network and service providers. In this context, ITU-T is working on updating the various Recommendations related to QoS and users' quality of experience (QoE). Considering the ITU-T QoS framework, we propose a methodology to develop a global QoS management model for next-generation wireless ecosystems taking advantage of big data and machine learning. The results from a case study conducted to validate the model in real-world Wi-Fi deployment scenarios are also presented.
S1.2	Unsupervised Learning for Detection of Leakage from the HFC Network *Emilia Gibellini and Claudio E. Righetti (Telecom Argentina, Argentina)* In the context of proactive maintenance of the HFC networks, cable operators count on Full-Band Capture (FBC) to analyze the downstream spectrum and look for impairments. There exists one particular type of impairment, which is ingress, likely to happen along with leakage. Therefore, the detection of the former leads to the identification of the latter. We collect data from FBC tool, and use unsupervised machine learning to group cable modems such that the signal they receive show common patterns. This allows a characterization of all cable modems in a service group. Then, we use the modems' locations to determine whether the root cause of the flaw is inside the homes or not.
S1.3	Double Sarsa Based Machine Learning to Improve Quality of Video Streaming over HTTP Through Wireless Networks *Dhananjay Kumar and Narmathaa Logganathan (Anna University, India); Ved P. Kafle (National Institute of Information and Communications Technology, Japan)* The adaptive streaming over HTTP is widely advocated to enhance the Quality of Experience (QoE) in a bitrate constrained IP network. However, most previous approaches based on estimation of available link bandwidth or fullness of media buffer tend to become ineffective due to the variability of IP traffic patterns. In this paper, we propose a Double State-Action-Reward-State-Action (Sarsa) based machine learning method to improve user QoE in IP network. The Pv video quality estimation model specified in ITU-T P.1203.1 recommendation is embedded in the learning process for the estimation of QoE. We have implemented the proposed Double Sarsa based adaptation method on the top of HTTP in a 4G wireless network and assessed the resulting quality improvement by using full reference video quality metrics. The results show that the proposed method outperforms an existing approach and can be recommended in standardization of future audio-visual streaming services over wireless IP network. We observed the average improvement of 7% in PSNR and 25% in VQM during the live streaming of video.

[1] Papers marked with an "*" were nominated for the three best paper awards.

Session 2: Artificial Intelligence and 5G	
S2.1	Self-Healing and Resilience in Future 5G Cognitive Autonomous Networks *Janne Ali-Tolppa (Nokia Bell Labs, Germany); Szilárd Kocsis, Benedek Schultz and Levente Bodrog (Nokia Bell Labs, Hungary); Márton Kajó (Technical University of Munich, Germany)* In the Self-Organizing Networks (SON) concept, self-healing functions are used to detect, diagnose and correct degraded states in the managed network functions or other resources. Such methods are increasingly important in future network deployments, since ultra-high reliability is one of the key requirements for the future 5G mobile networks, e.g. in critical machine-type communication. In this paper, we discuss the considerations for improving the resiliency of future cognitive autonomous mobile networks. In particular, we present an automated anomaly detection and diagnosis function for SON self-healing based on multi-dimensional statistical methods, case-based reasoning and active learning techniques. Insights from both the human expert and sophisticated machine learning methods are combined in an iterative way. Additionally, we present how a more holistic view on mobile network self-healing can improve its performance.
S2.2	AI as a Microservice (AIMS) over 5G Networks *Gyu Myoung Lee (Liverpool John Moores University, United Kingdom); Tai-Won Um (Chosun University, Rep. of Korea); Jun Kyun Choi (Korea Advanced Institute of Science & Technology, Rep. of Korea)* As data-driven decision-making services are being infused into Internet of Things (IoT) applications, especially at the 5G networks, Artificial Intelligence (AI) algorithms such as deep learning, reinforcement learning, etc. are being deployed as monolithic application services for autonomous decision processes based on data from IoT devices. However, for latency sensitive IoT applications such as health-monitoring or emergency-response applications, it is inefficient to transmit data to the Cloud data centers for storage and AI based processing. In this article, 5G integrated architecture for intelligent IoT based on the concepts of AI as a microservice (AIMS) is presented. The architecture has been conceived to support the design and development of AI microservices, which can be deployed on federated and integrated 5G networks slices to provide autonomous units of intelligence at the Edge of Things, as opposed to the current monolithic IoT-Cloud services. The proposed 5G based AI system is envisioned as a platform for effective deployment of scalable, robust, and intelligent cross-border IoT applications to provide improved quality of experience in scenarios where realtime processing, ultra-low latency and intelligence are key requirements. Finally, we highlight some challenges to give future research directions.
S2.3	Multifractal Modeling of the Radio Electric Spectrum Applied in Cognitive Radio Networks *Luis Tuberquia-David and Cesar Hernández (Universidad Distrital Francisco Jose de Caldas, Colombia)* The work discussed in this article is framed within the context of cognitive networks in America, showcasing the scenario of the radioelectric spectrum of the city of Bogotá, Colombia. The objective is to model the traffic of the wireless network, since it is underused in this region of Latin America. Hence, some tools are studied to allow the structuring of the type of traffic seen in the network. Based on stochastic tools such as the log-scale diagram, the linear multiscale diagram, and the multifractal spectrum, this research aims to verify the multifractality of traffic series collected on the electric radio spectrum of Bogotá, Colombia in 2012. In fact, the study reveals that all the channels of the network have a multifractal behavior with 90% of them presenting a Hurst parameter in the 0.5 to 1 range. The evidence suggests that the traffic in this region could be modeled as multifractal time series. Therefore, the analysis carried out intends to provide a new modeling method for the Colombian radioelectric spectrum in the form of a multifractal-based analysis.

S2.4	Towards Cognitive Autonomous Network in 5G *Stephen S. Mwanje and Christian Mannweiler (Nokia Bell Labs, Germany)* Cell densification and addition of new Radio Access Technologies have been the solutions of choice for improving area-spectral efficiency to serve the ever-growing traffic demand. Both solutions, however, increase the cost and complexity of network operations for which the agreed solution is increased automation. Cognitive Autonomous Networks (CAN) will therefore use Artificial Intelligence and Machine Learning (ML) to maximize the value of automation. This paper develops the models for cognitive automation and proposes a CAN design that addresses the requirements for 5G and future networks. We then illustrate the benefit of this approach by evaluating ML models that learn a network's response to different mobility states and configurations.

Session 3: Machine Learning in Telecommunication Networks - II	
S3.1	**Invited Paper -** Machine Learning Opportunities in Cloud Computing Data Center Management for 5G Services *Fabio López-Pires (Itaipu Technological Park, Paraguay); Benjamín Barán (National University of the East, Paraguay)* Emerging paradigms associated with cloud computing operations are considered to serve as a basis for integrating 5G components and protocols. In the context of resource management for cloud computing data centers, several research challenges could be addressed through state-of-the-art machine learning techniques. This paper presents identified opportunities on improving critical resource management decisions, analyzing the potential of applying machine learning to solve these relevant problems, mainly in two-phase optimization schemes for virtual machine placement (VMP). Potential directions for future research are also presented.
S3.2	Consideration on Automation of 5G Network Slicing with Machine Learning *Ved P. Kafle, Yusuke Fukushima; Pedro Martinez-Julia and Takaya Miyazawa (National Institute of Information and Communications Technology, Japan)* Machine learning has the capability to provide simpler solutions to complex problems by analyzing a huge volume of data in a short time, learning for adapting its functionality to dynamically changing environments, and predicting near future events with reasonably good accuracy. The 5G communication networks are getting complex due to emergence of unprecedentedly huge number of new connected devices and new types of services. Moreover, the requirements of creating virtual networkslices suitable to provide optimal services for diverse users and applications are posing challenges to the efficient management of network resources, processing information about a huge volume of traffic, staying robust against all potential security threats, and adaptively adjustment of network functionality for time-varying workload. In this paper, we introduce about the envisioned 5G network slicing and elaborate the necessity of automation of network functions for the design, construction, deployment, operation, control and management of network slices. We then revisit the machine learning techniques that can be applied for the automation of network functions. We also discuss the status of artificial intelligence and machine learning related activities being progressed in standards development organizations and industrial forums.

Session 4: Optimization of Data Management with Machine Learning	
S4.1	A Deep Reinforcement Learning Approach for Data Migration in Multi-access Edge Computing *Fabrizio De Vita, Dario Bruneo and Antonio Puliafito (University of Messina, Italy); Giovanni Nardini, Antonio Virdis and Giovanni Stea (University of Pisa, Italy)* 5G technology promises to improve the network performance by allowing users to seamlessly access distributed services in a powerful way. In this perspective, Multi-access Edge Computing (MEC) is a relevant paradigm that push data and computational resources nearby users with the final goal to reduce latencies and improve resource utilization. Such a scenario requires strong policies in order to react to the dynamics of the environment also taking into account multiple parameter settings. In this paper, we propose a deep reinforcement learning approach that is able to manage data migration in MEC scenarios by learning during the system evolution. We set up a simulation environment based on the OMNeT++/SimuLTE simulator integrated with the Keras machine learning framework. Preliminary results showing the feasibility of the proposed approach are discussed.
S4.2	Predicting Activities in Business Processes with LSTM Recurrent Neural Networks *Edgar Tello-Leal (Autonomous University of Tamaulipas, Mexico); Jorge Roa (National Technological University, Santa Fe Regional Faculty, Argentina); Mariano Rubiolo (National Technological University, Santa Fe Regional Faculty & FICH/UNL-CONICET, Argentina); Ulises Ramírez-Alcocer (Autonomous University of Tamaulipas, Mexico)* The Long Short-Term Memory (LSTM) Recurrent Neural Networks provide a high precision in the prediction of sequences in several application domains. In the domain of business processes it is currently possible to exploit event logs to make predictions about the execution of cases. This article shows that LSTM networks can also be used for the prediction of execution of cases in the context of an event log that originates from the IoT and Industry 4.0 domain. This is a key aspect to provide valuable input for planning and resource allocation (either physical or virtual), since each trace associated with a case indicates the sequential execution of activities in business processes. A methodology for the implementation of an LSTM neural network is also proposed. An event log of the industry domain is used to train and test the proposed LSTM neural network. Our preliminary results indicate that the prediction of the next activity is acceptable according to the literature of the domain.

Session 5: Network Applications of Machine Learning	
S5.1	Smart Usage of Multiple RAT in IoT-oriented 5G Networks: A Reinforcement Learning Approach *Ruben Martínez Sandoval, Sebastian Canovas-Carrasco, Antonio-Javier Garcia-Sanchez and Joan Garcia-Haro (Technical University of Cartagena, Spain)* Smart Cities and Smart Industries are the flagships of the future IoT due to their potential to revolutionize the way in which people live and produce in advanced societies. In these two scenarios, a robust and ubiquitous communication infrastructure is needed to accommodate the traffic generated by the 10 billion devices that are expected by the year 2020. Due to its future world-wide presence, 5G is called to be this enabling technology. However, 5G is not a perfect solution, thus providing IoT nodes with different Radio Access Technologies (RATs) would allow them to exploit the various benefits offered by each RAT (such as lower power consumption or reduced operational costs). By making use of the mathematical framework of Reinforcement Learning, we have formulated the problem of deciding which RAT should an IoT node employ when reporting events. These so-called transmission policies maximize a predefined reward closely related to classical throughput while keeping power consumption and operational costs below a certain limit. A set of simulations are performed for IoT nodes provided with two RATs: LoRa and 5G. The results obtained are compared to those achieved under other intuitive policies to further highlight the benefits of our proposal.
S5.2	Message Collision Identification Approach Using Machine Learning *Juan Pablo Martín, Bruno Marengo, Juan Pablo Prina and Martín Gabriel Riolfo (Universidad Tecnológica Nacional, Facultad Regional San Nicolás, Argentina)* Machine learning algorithms, in particular k-nearest neighbors (kNN) and support vector machine (SVM), are employed to estimate the potential success in decodifying ADS-B messages in highly congested areas. The main aim of this study is to optimize automatic dependent surveillance-broadcast (ADS-B) reception on-board low Earth orbit satellites. In this first approach, simulations are performed to obtain the training and testing signals. First, ADS-B communication system is described; second, machine learning, kNN and SVM are introduced. Third, the developed simulator is presented and the kNN and SVM algorithms are described with its results. Finally, the performance of these two is compared.
S5.3	Optical Flow Based Learning Approach for Abnormal Crowd Activity Detection with Motion Descriptor Map *Dhananjay Kumar and Govinda Raj Sampath Sarala (Anna University, India)* Automated abnormal crowd activity detection with faster execution time has been a major research issue in recent years. In this work, a novel method for detecting crowd abnormal activities is proposed which is based on processing of optical flow as motion parameter for machine learning. The proposed model makes use of magnitude vector which represents motion magnitude of a block in eight directions divided by a 45 degree pace angle. Further, motion characteristics are processed using Motion Descriptor Map (MDP), which takes two main parameters namely aggregate magnitude of motion flow in a block and Euclidean distance between blocks. Here, the angle of deviation between any two blocks determines which among the eight values in the magnitude vector to be considered for further processing. The algorithm is tested with two standard datasets namely UMN and UCSD Datasets. Apart from these the system is also tested with a custom dataset. On an average, an overall accuracy of 98.08% was obtained during experimentation.

Session 6: Social, Legal and Ethical Aspects in Machine Learning	
S6.1	A Gendered Perspective on Artificial Intelligence *Smriti Parsheera (National Institute of Public Finance and Policy, New Delhi, India)* Availability of vast amounts of data and corresponding advances in machine learning have brought about a new phase in the development of artificial intelligence (AI). While recognizing the field's tremendous potential we must also understand and question the process of knowledgemaking in AI. Focusing on the role of gender in AI, this paper discusses the imbalanced power structures in AI processes and the consequences of that imbalance. We propose a three-stage pathway towards bridging this gap. The first, is to develop a set of publicly developed standards on AI, which should embed the concept of "fairness by design". Second, is to invest in research and development in formulating technological tools that can help translate the ethical principles into actual practice. The third, and perhaps most challenging, is to strive towards reducing gendered distortions in the underlying datasets to reduce biases and stereotypes in future AI projects.
S6.2	Ethical Framework for Machine Learning *Charru Malhotra (Indian Institute of Public Administration, India); Vinod Kotwal (Department of Telecommunications, India); Surabhi Dalal (India Centre for Migration, India)* Artificial Intelligence (AI) with its core subset of Machine Learning (ML) is rapidly transforming life experiences as humans begin to grow more dependent on these 'smart machines' for their needs - ranging from routine mundane chores to critical personal decisions. However, these transformative technologies are at the same time proving unpredictable too as has been reported worldwide in certain cases. Therefore, several studies/reports, such as COMEST report on Robotics ethics (UNESCO, 2017) point to an obvious need for inculcating more ethical behavior in machines. The present study aims to look at the role and interplay of ML (the hard sciences) and Ethics (the soft sciences) to resolve such predicaments that are inadvertently manifested by machines not constrained or controlled by human expectations. Based on focused review of literature of both domains-ML and Ethics, the proposed paper attempts to first build on the need for introduction of an ethical algorithm in the domain of machine learning and then endeavors to provide a conceptual framework to resolve the ethical dilemmas.
S6.3	Undeclared Constructions: A Government's Support Deep Learning Solution for Automatic Change Detection *Pamela Ferrari Lezaun and Gustavo Olivieri (Universidad Tecnológica Nacional, Facultad Regional Santa Fe, Argentina)* In our cities, in particular those with high demographic density, the proliferation of buildings goes so fast that it is not possible or -in the best scenarios- very difficult to be handled by the government departments regulating the legitimacy -in term of safety and taxes- of those constructions. In this paper, we propose a deep learning tool for computer vision trained with a corpus of satellite images provided by SpaceNet to detect changes in cities, showing the most recent constructions automatically, which allows different municipal officers to check if they have been -or haven't been- declared. To achieve this, we implemented the layered architecture of the SpaceNet Challenge Round 2 winning solution, and decided to improve it with an output comparison which gives us a high value final result for the end-user in the detection of changes, giving him the possibility to appreciate in the graphic user interface how many new buildings and square meters were detected.

INDEX OF AUTHORS

Index of Authors

International
Telecommunication
Union
Telecommunication
Standardization Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland

ISBN: 978-92-61-26921-0

Published in Switzerland
Geneva, 2018