ITU

sudacad سوداكاد
أكاديمية سوداتل للاتصالات
SUDATEL TELECOMMUNICATIONS ACADEMY

ITUWTDC
BUENOS AIRES 2017
9-20 October

ITU-SUDACAD Regional Forum

IoT for Development of Smart Sustainable Cities

Khartoum, Sudan

13-14 December 2017

Session 6

Interoperability, Integration, and Interconnection

of Internet of Things Systems

Prof. Mustapha Benjillali
INPT, Morocco
benjillali@ieee.org

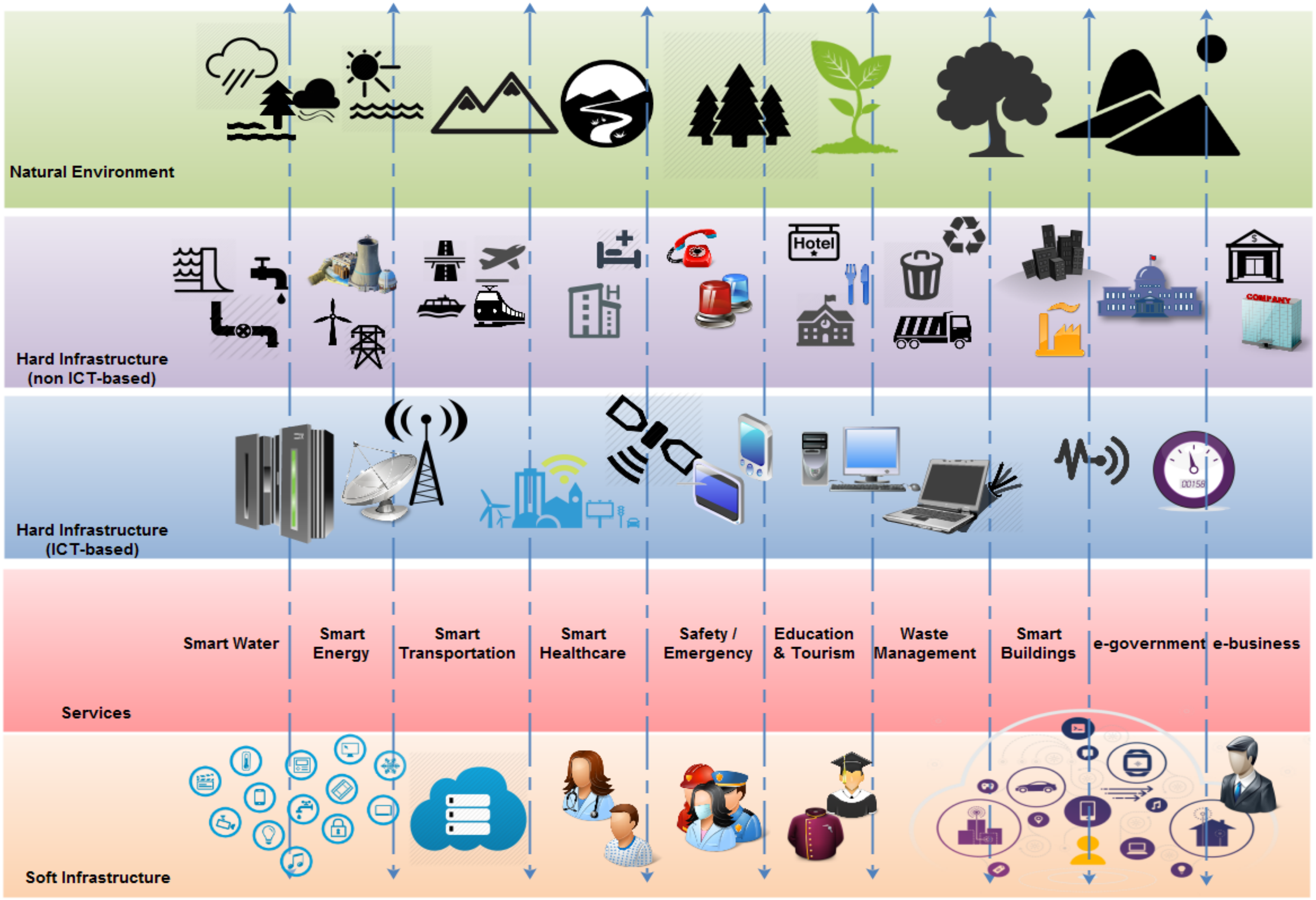
ITU-D
1992
2017
CELEBRATING
25YEARS
OF ACHIEVEMENTS

ITU WTDC BUENOS AIRES 2017 9-20 October

IoT and Multi-layer Interoperability Challenges

ITU-D 1992 2017 CELEBRATING 25YEARS OF ACHIEVEMENTS

Real Life IoT Layers



Natural Environment

Hard Infrastructure (non ICT-based)

Hard Infrastructure (ICT-based)

Services

Soft Infrastructure

Smart Water

Smart Energy

Smart Transportation

Smart Healthcare

Safety / Emergency

Education & Tourism

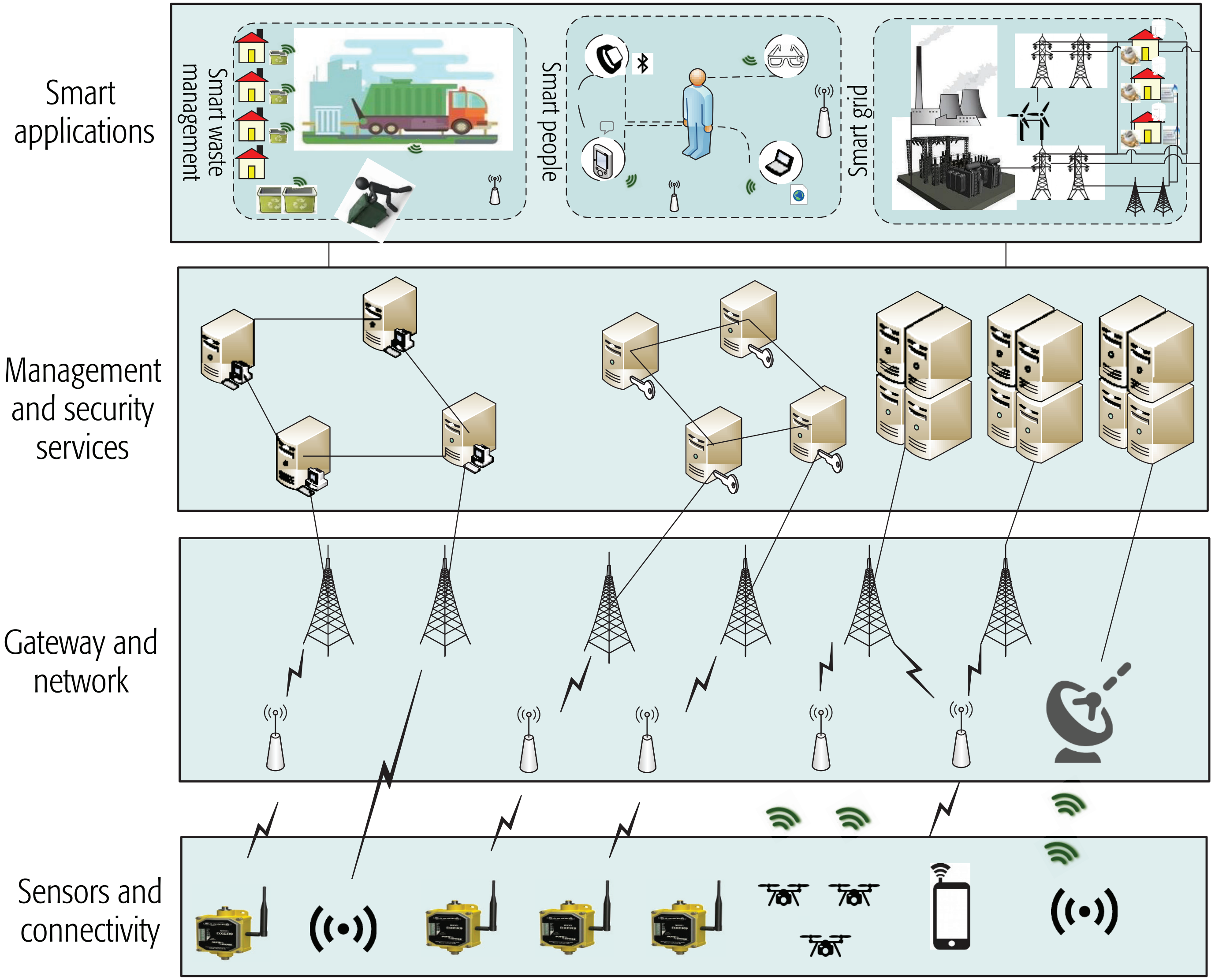
Waste Management

Smart Buildings

e-government

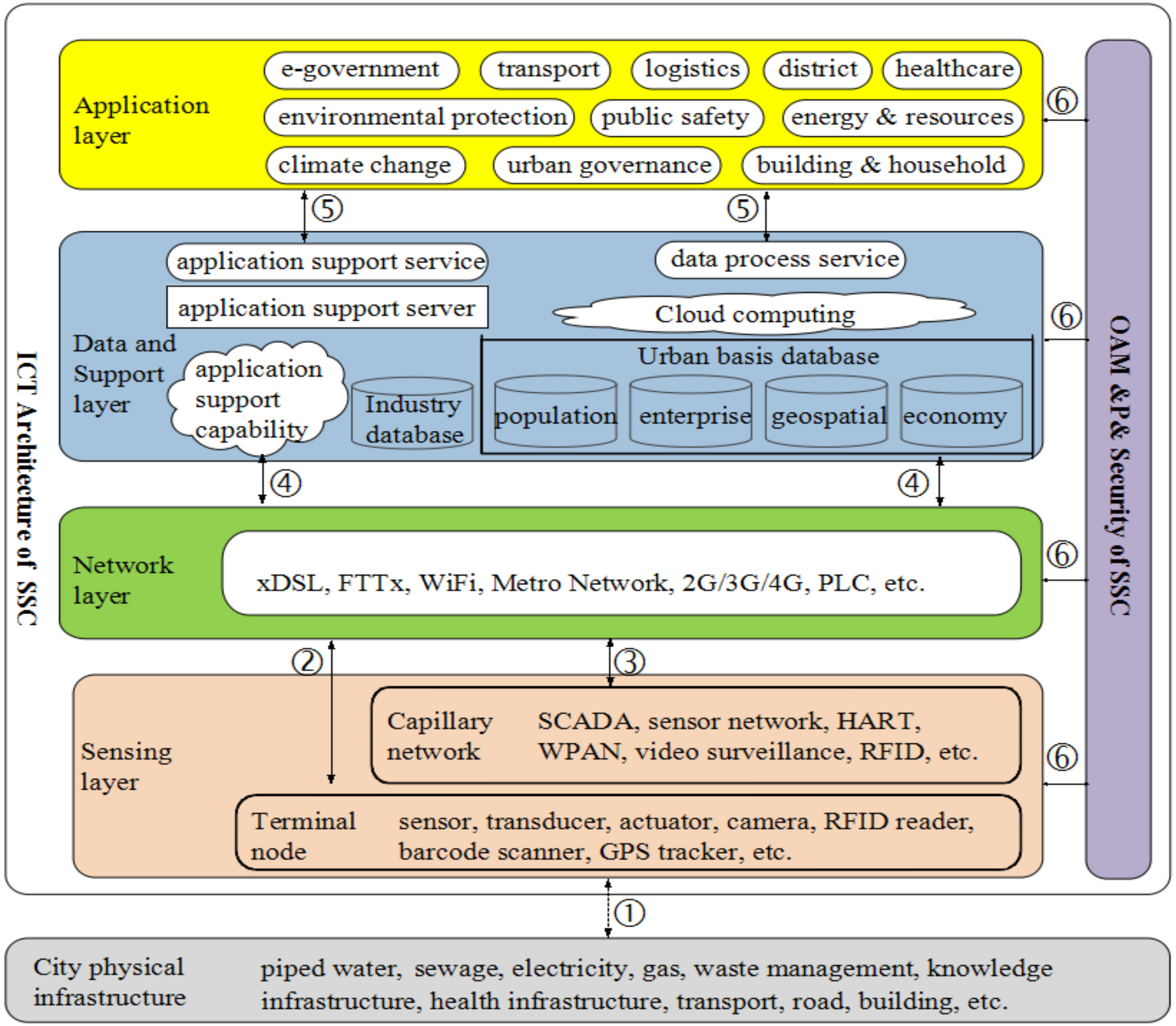
e-business

Multi-Layer Model



Source: I. Yaqoob et al., "Internet of thIngs ArchItecture: recent AdvAnces, tAxonomy, requIrements, And open chAllenges", IEEE Wireless Communications, June 2017.

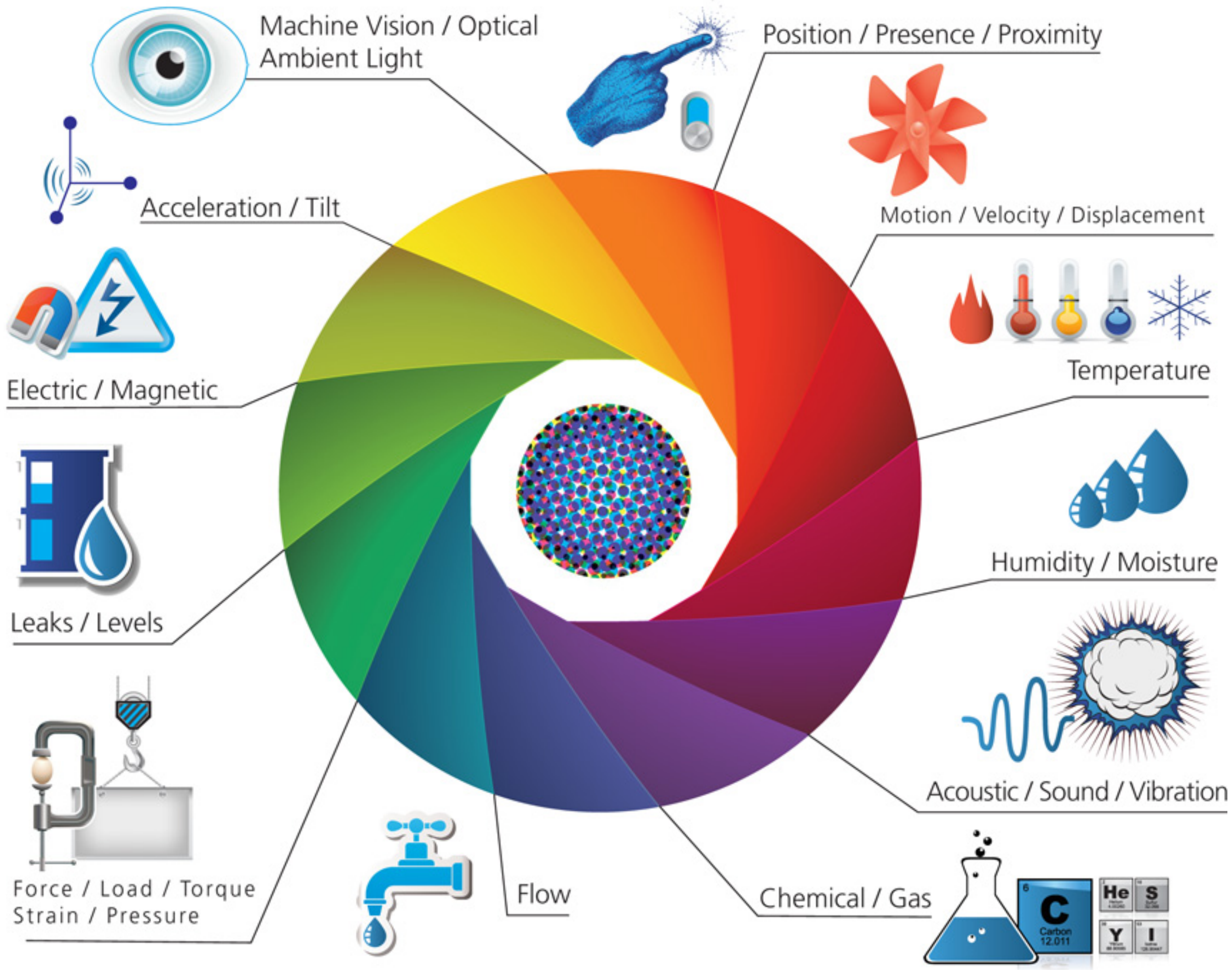
Multi-Layered View


Application layer
e-government
transport
logistics
district
healthcare
environmental protection
public safety
energy & resources
climate change
urban governance
building & household
⑤
⑤
Data and Support layer
application support service
application support server
data process service
Cloud computing
application support capability
Industry database
Urban basis database
population
enterprise
geospatial
economy
④
④
Network layer
xDSL, FTTx, WiFi, Metro Network, 2G/3G/4G, PLC, etc.
②
③
Sensing layer
Capillary network
SCADA, sensor network, HART, WPAN, video surveillance, RFID, etc.
Terminal node
sensor, transducer, actuator, camera, RFID reader, barcode scanner, GPS tracker, etc.
①
City physical infrastructure
piped water, sewage, electricity, gas, waste management, knowledge infrastructure, health infrastructure, transport, road, building, etc.
ICT Architecture of SSC
OAM &P& Security of SSC
⑥
⑥
⑥
⑥

Source: ITU-T FG-SSC, May 2016

ITUWTDC
BUENOS AIRES 2017
9-20 October

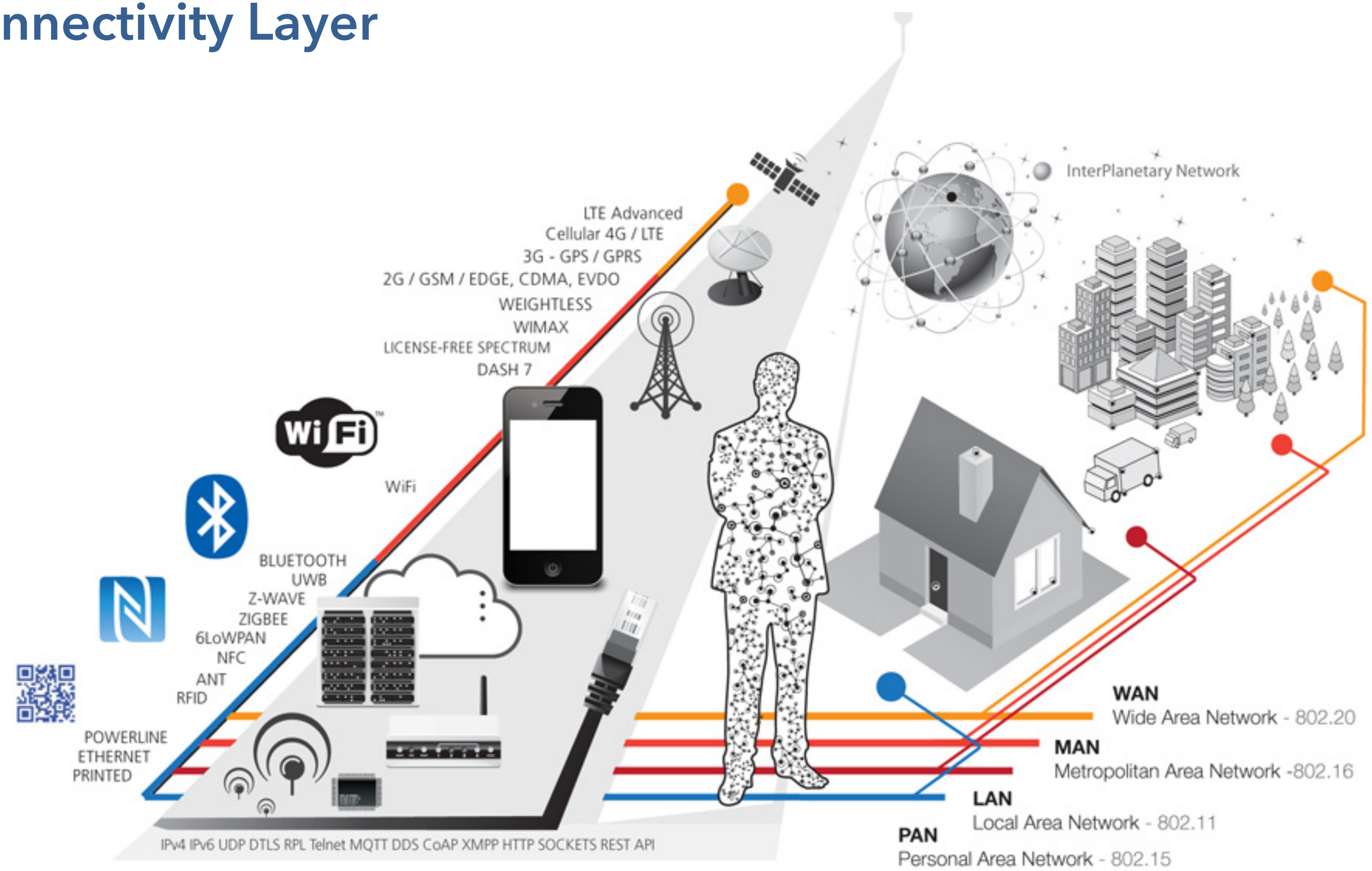
Sensors Layer



Source: Harbor Research.

CELEBRATING
25YEARS
OF ACHIEVEMENTS
ITU-D
1992
2017

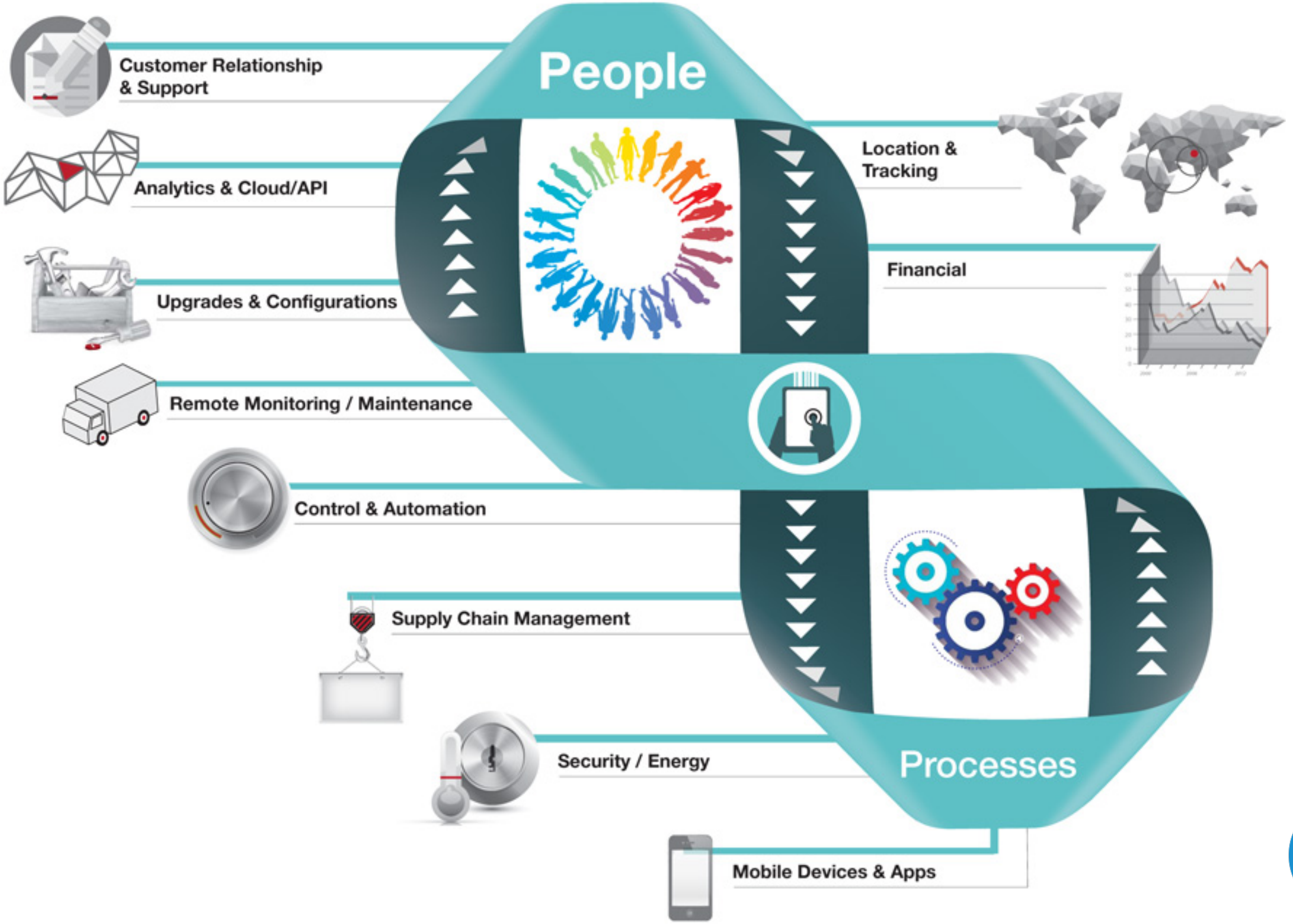
Connectivity Layer


InterPlanetary Network
LTE Advanced
Cellular 4G / LTE
3G - GPS / GPRS
2G / GSM / EDGE, CDMA, EVDO
WEIGHTLESS
WIMAX
LICENSE-FREE SPECTRUM
DASH 7
Wi Fi
WiFi
BLUETOOTH
UWB
Z-WAVE
ZIGBEE
6LoWPAN
NFC
ANT
RFID
POWERLINE
ETHERNET
PRINTED
IPv4 IPv6 UDP DTLS RPL Telnet MQTT DDS CoAP XMPP HTTP SOCKETS REST API
WAN
Wide Area Network - 802.20
MAN
Metropolitan Area Network -802.16
LAN
Local Area Network - 802.11
PAN
Personal Area Network - 802.15

Source: *Harbor Research.*

Upper Layers

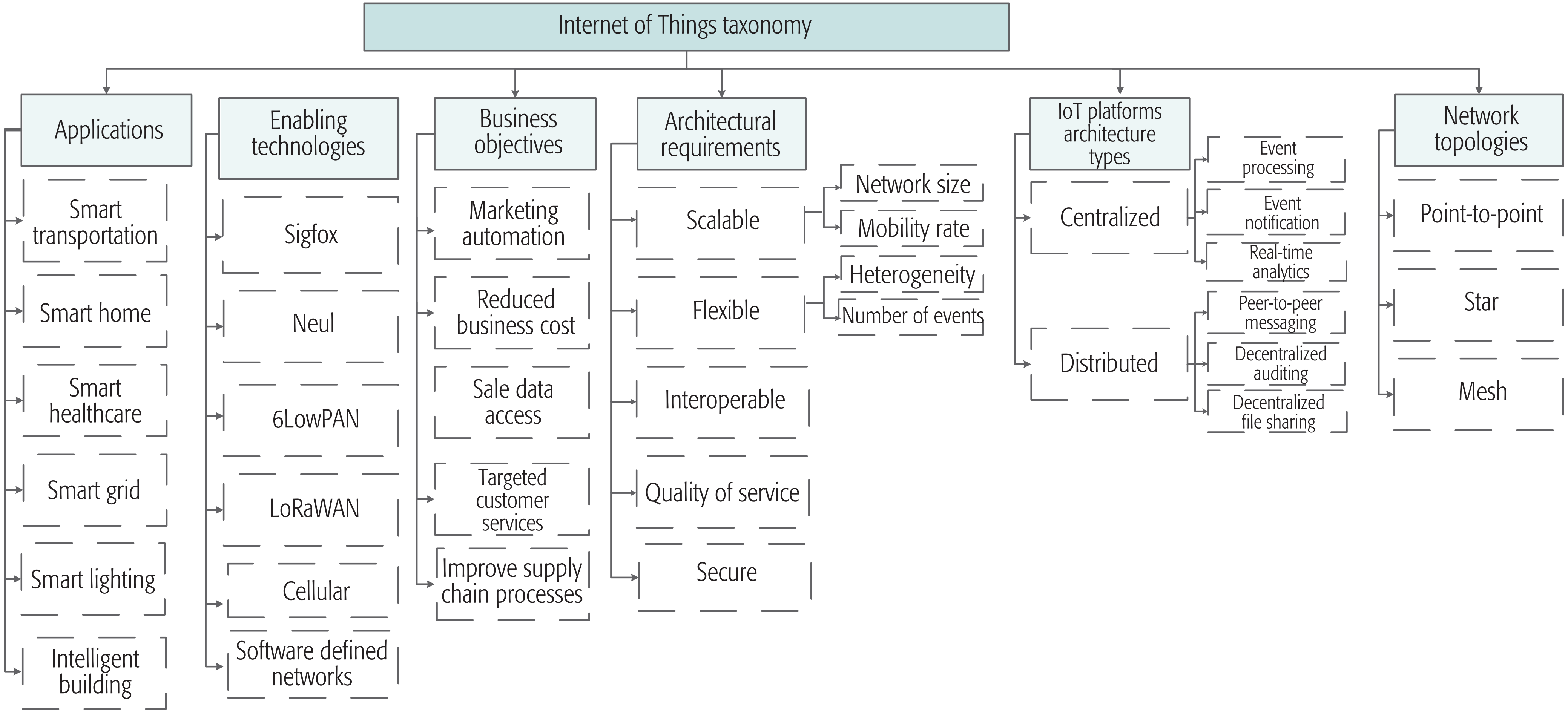
ITUWTDC BUENOS AIRES 2017
9-20 October



Source: Harbor Research.

ITU-D 1992 2017 CELEBRATING 25YEARS OF ACHIEVEMENTS

Taxonomic Classification



- Internet of Things taxonomy
  - Applications
    - Smart transportation
    - Smart home
    - Smart healthcare
    - Smart grid
    - Smart lighting
    - Intelligent building
  - Enabling technologies
    - Sigfox
    - Neul
    - 6LowPAN
    - LoRaWAN
    - Cellular
    - Software defined networks
  - Business objectives
    - Marketing automation
    - Reduced business cost
    - Sale data access
    - Targeted customer services
    - Improve supply chain processes
  - Architectural requirements
    - Scalable
      - Network size
      - Mobility rate
    - Flexible
      - Heterogeneity
      - Number of events
    - Interoperable
    - Quality of service
    - Secure
  - IoT platforms architecture types
    - Centralized
      - Event processing
      - Event notification
      - Real-time analytics
    - Distributed
      - Peer-to-peer messaging
      - Decentralized auditing
      - Decentralized file sharing
  - Network topologies
    - Point-to-point
    - Star
    - Mesh

Source: I. Yaqoob et al., “Internet of thIngs ArchItecture: recent AdvAnces, tAxonomy, requIrements, And open chAllenges”, IEEE Wireless Communications, June 2017.

Consumer IoT (cIoT) versus Industrial IoT (iIoT)

Rough distinction cIoT and iIoT, with implications on underlying technologies and business models.

cIoT:

- Improving the quality of people's life by saving time and money.
- Interconnection of consumer electronic devices, as well as of (virtually) anything belonging to user environments such as homes, offices, and cities.

iIoT:

- Integrating Operational Technology (OT) and Information Technology (IT).
- Smart machines, networked sensors, and data analytics to improve business-to-business services across a wide variety of market sectors and activities.
- Generally implying machine-to-machine (M2M) interactions, distributed control not requiring human intervention.

Consumer IoT (cIoT) versus Industrial IoT (iIoT)

Common communication requirements:

- Scalability
- Need for lean protocol stack implementations in constrained devices
- Friendliness to IP ecosystem …

Specific communication requirements are very different:

- Reliability
- QoS (latency, throughput, etc)
- Privacy …

In cIoT, desirable features: *(e.g. quantified self)*

- Low power consumption,
- Ease of installation,
- Integration and maintenance,

In iIoT, other concerns:

- Evolves from large base of systems
- Result of the integration of disconnected islands,
- Semi-proprietary protocols and architectures

Modern IoT Connectivity Landscape

- Diversity of available connectivity solutions — Need for harmonization across industries — Combination to meet IoT Key Performance Indicators (KPIs).

- First forms of IoT connectivity dated back to the 80s (Legacy Radio Frequency Identification (RFID) technologies) — in the 90s Wireless Sensor Networks (WSNs) gained a lot of momentum due to their attractive application scenarios, both in business and consumer market.

- First decade of 21st century, industrial alliances and Standards Developing Organizations (SDOs) put lot of effort in developing standardized low power IoT solutions:
  - First, mainly proprietary solutions, such as WirelessHART, and Z-Wave. They actually delayed the initial take off of the IoT, due to interoperability issues, among different vendors.
  - Then, more generic connectivity technologies by SDOs (IEEE, ETSI, 3GPP, and IETF), easing interconnection and Internet-connection of constrained devices. Bluetooth, IEEE802.15.4 among low power short range solutions available today, which have played an important role in the IoT evolution.
  - Recently the IEEE802.15.4 physical (PHY) and medium access control (MAC) layers have been complemented by an IP-enabled IETF protocol stack. The IETF 6LoWPAN (today 6lo) and IETF ROLL WGs have played a key role in facilitating the integration of low-power wireless networks into the Internet, by proposing mainly distributed solutions for address assignment and routing.
  - At the same time, the 3rd Generation Partnership Project (3GPP) has been working toward supporting M2M applications on 4G broadband mobile networks, such as UMTS, and LTE, with the final aim of embedding M2M communications in the 5G systems.

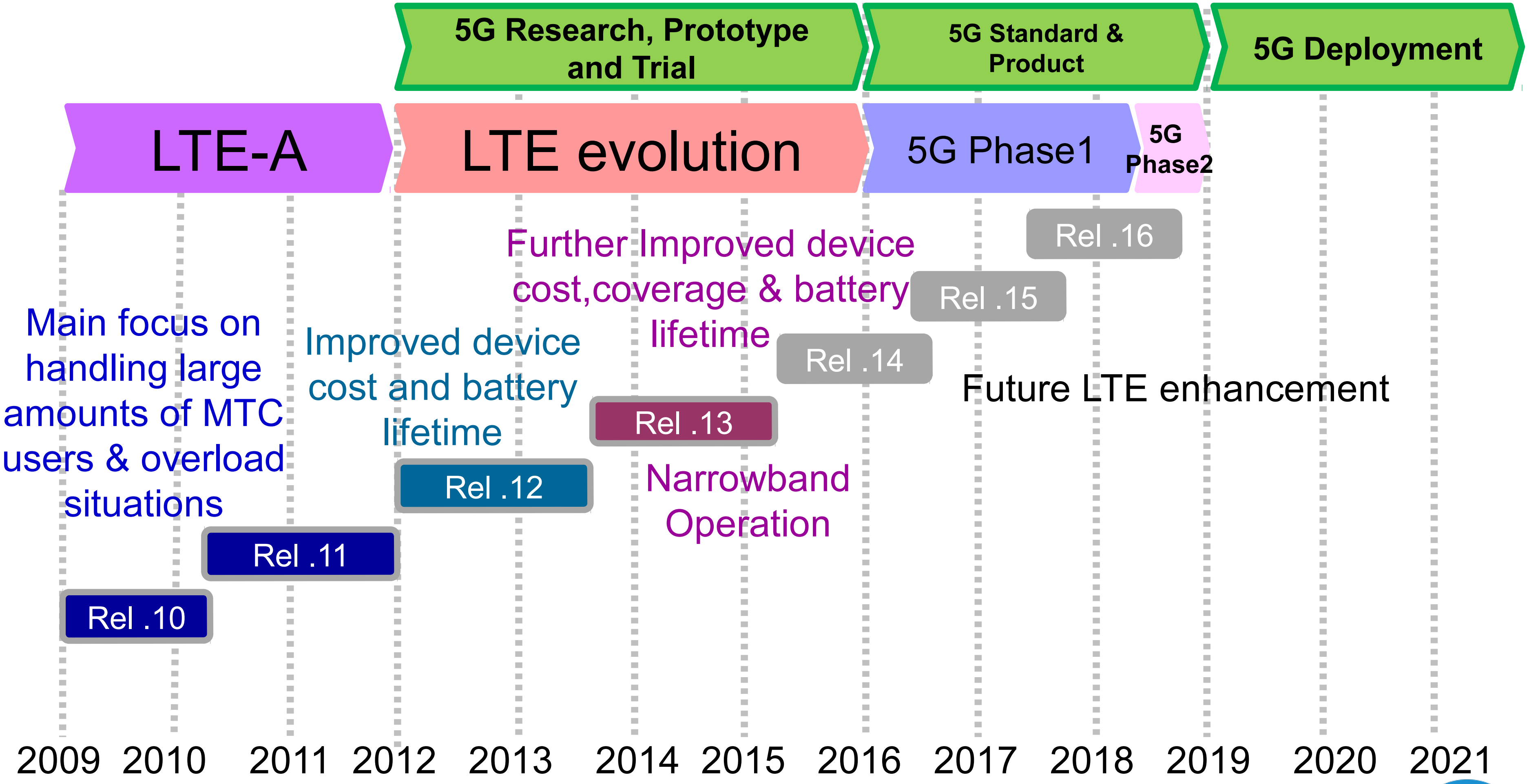
- No one of these aforementioned technologies has emerged as a market leader, mainly because of technology shortcoming, and business model uncertainties.

- Now, the IoT connectivity field is at a turning point with many promising radio technologies emerging as true M2M connectivity contenders:
  - Low-Power WiFi,
  - Low-Power Wide Area (LPWA) networks
  - Several improvements for cellular M2M systems.

Modern IoT Connectivity Comparative Landscape

	ZigBee	BLE	LP-Wifi	LPWA	3GPP Rel8	LTE Rel13 & NB-IoT
Scalability	✗	✗	✓	✗	✓	✓
Reliability	✗	✓	✓	✗	✓	✓
Low Power	✓	✓	✓	✓	✗	✓
Low Latency	✗	✓	✓	✗	✓	✓
Large Coverage	✗	✗	✓	✓	✓	✓
Low module cost	✓	✓	✓	✓	✗	✓
Mobility support	✗	✗	✗	✗	✓	✓
Roaming support	✗	✗	✗	✗	✓	✓
SLA support	✗	✗	✗	✗	✓	✓

3GPP Schedule



Source: M. R. Palattella et al., “Internet of Things in the 5G Era: Enablers, Architecture and Business Models”, IEEE JSAC, 2015.

Ubiquitous Connectivity Enablers

- Many more features and functionalities will need to be added to the currently predominantly broadband approach.
- Strong heterogeneous networking (HetNet) paradigm (with different MAC/PHY, coverage, backhaul connectivity, QoS design parameters, ...).
- Seamless connectivity for the emerging IoT through a complex set of mechanisms for coordination and management.
- Evolved 4G and emerging 5G networks will thus be characterized by interoperability and integration between multiple radio access networks

Ubiquitous Connectivity Enablers (4G-Evolution & 5G)

RAT Enablers

- Relaying for Increased Coverage
- Millimeter Wave Technologies
- Device-to-Device Communications

RAN Enablers

- Decoupled Down/Uplinks
- License Assisted Access
- Radio Access Network as a Service

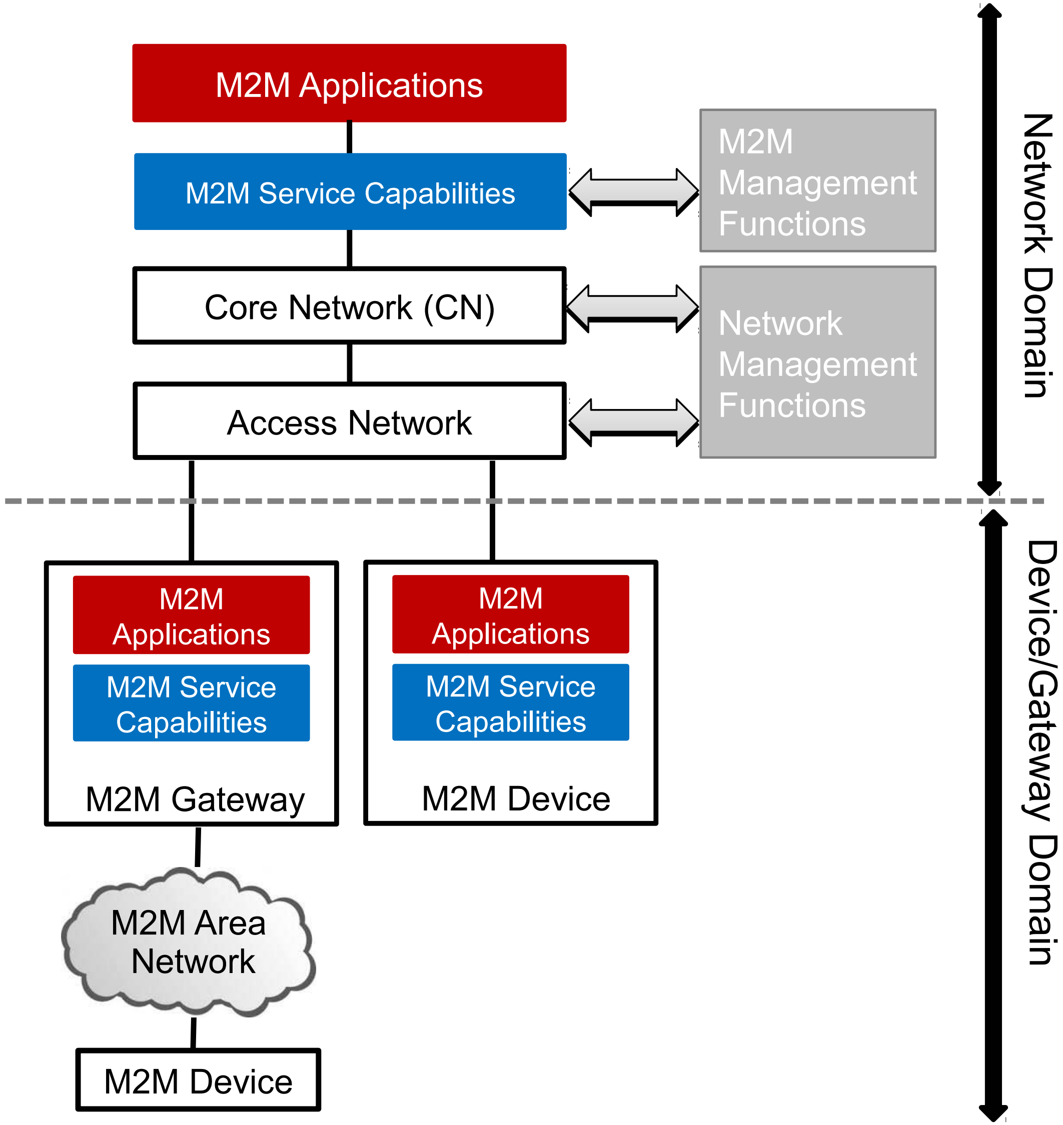
Network Enablers

- Software Defined Networking
- Network Function Virtualization

MTC ARCHITECTURE IN 5G

- M2M architectures allow the different actors of an IoT system to:
  - exchange data, check the availability of resources,
  - discover how to compose complex services,
  - handle device registration,
  - and offer a standardized output to any vertical application.
- Main challenge with M2M architectures is the vertical fragmentation of the IoT market
- Recently, two noticeably international standardization projects (i.e., ESTI SmartM2M and oneM2M) have been formulated to resolve fragmentation issues in M2M systems
- Definition of an horizontal service layer that is able to embrace different existing communication technologies and to include future extensions to 5G systems.
  - ETSI SmartM2M
  - SmartM2M to oneM2M

M2M Architecture



Source: *M. R. Palattella et al., "Internet of Things in the 5G Era: Enablers, Architecture and Business Models", IEEE JSAC, 2015.*

Thank You

شكراً

sudacad سوداكاد
أكاديمية سوداتل للإتصالات
SUDATEL TELECOMMUNICATIONS ACADEMY

ITUWTDC
BUENOS AIRES 2017
9-20 October

ITU-SUDACAD Regional Forum

IoT for Development of Smart Sustainable Cities

Khartoum, Sudan

13-14 December 2017

Session 6

Interoperability, Integration, and Interconnection

of Internet of Things Systems

Prof. Mustapha Benjillali
INPT, Morocco
benjillali@ieee.org

ITU-D 1992 2017
CELEBRATING 25YEARS OF ACHIEVEMENTS

IoT4SSC Open Problems and Challenges

Requirements for future IoT Architectures

Resource Control:

The smart devices participating in an IoT environment must be accessible and configurable in a remote manner. In some situations, when the administrators are not available at their particular places, controlling the resources from outside can help resolve the matter. More- over, IoT systems must be able to balance the load in case of redundant resource availability, which can lead toward appropriate resource utilization.

Energy Awareness:

The incorporation of energy awareness in the IoT paradigm, where most of the devices are resource constrained, can help avoid unnecessary energy consumption. In some cases, when the load is not too heavy, devices should put themselves into sleep mode. More- over, the formation of lightweight communication protocols can help save the energy of smart devices. Thus, the future IoT architecture must be designed in such a way that it can minimize energy consumption.

Quality of Service:

One of the requirements of IoT architectures is that they shall be able to provide quality services to users. QoS in IoT can be ensured by prioritizing the services and retrieval. Applications that require real-time processing must be given high priority to improve their performance. Moreover, in response to a query, only the required information should be retrieved. Incorporation of these suggestions in the the future IoT architecture can make it a huge success.

Requirements for future IoT Architectures

Interoperability:

In the IoT paradigm, enabling communication among devices from different vendors is a key requirement. The future IoT architecture must be able to support internet- working and seamless communication between all kinds of applications such as business, desktop, and mobile applications. In addition, to enable the communication between constrained and unconstrained devices of an IoT system, adaptation between networking protocols must be required.

Interference Management:

IoT architecture must be able to handle the interference problem. In the future, when trillions of smart devices that have multi-radio capabilities will be connected to the Inter- net, interference will become a real problem. Therefore, the future IoT architecture must be designed in such a way that it can incorporate radio awareness. Flawless connectivity can only be ensured by address- ing the interference problem. In order to achieve reliable services in the IoT environment, interference-free solutions must be developed.

Security:

Strengthening security in the IoT environment has become an essential requirement. The future IoT architecture must be secure enough to prevent devices being activated by unauthorized means. In addition, the securi- ty mechanisms must be lightweight as most of the devices are resource constrained. Moreover, ensuring the freshness of data is also very import- ant. The lack of strong security support in IoT can undermine the trust of IoT users, which can lead to the failure of the technology.

Open Challenges

Interoperability:

IoT has three main types of interoperability challenges, namely technical, semantic, and pragmatic. The technical challenges have a concern with device capabilities, protocols, and relevant standards to coexist and interoperate in the same computing paradigm, whereas semantic have a concern with the capabilities of various IoT components that are responsible for process- ing and interpreting the exchanged data. However, pragmatic have a concern with the capabilities of the system components to observe the parties intentions. Achievement of technical interoperability can be gained by offering agent-based mediation between IoT devices and standards. Semantic interoperability is a requirement to the machine computable logic, knowledge discovery, and data federation between information systems. Pragmatic interoperability can be achieved through the creative design of predefined specifications of the components behavior. In the future, cross-lay- er interoperability solutions are required.

Scalability:

IoT are expected to face many challenges related to the potential unbounded number of interacting entities and substantial differences in the interaction patterns and behavior. The existing IoT architectures need to be scaled up to accommodate the trillion of smart devices. IoT systems scalability management can be summarized into two points. First, the rapid growth has been witnessed in the IoT devices. However, current management protocols do not scale well to accommodate the requirements of IoT devices due to their limited capabilities. Second, social relationships between the owners of the devices need to be considered, where some of IoT system entities are human portable devices. In the future, scalability management protocols are expected to track social relationships between devices in order to enable ad hoc based computing services by providing some incentives.

Flexibility:

Since there are numerous applications of IoT, service provisioning to the different IoT applications according to their demands has become very challenging. IoT users usually need dynamically configured, customized, value-add- ed, and autonomous on-the-move services. More- over, personalized, customized, autonomous, and dynamic services can be supported by construct- ing and utilizing the adaptive, context-aware, and reconfigurable multiple service network architecture. In the future, models of service declarative specifications are required for the construction of future network service architectures.

Open Challenges

Energy Efficiency:

Tiny devices are the back- bone of IoT. However, these devices have limit- ed processing capabilities, memory, and battery power. Consequently, compute-intensive applications and routing processes cannot run on IoT devices, as these devices are very lightweight. Consideration of energy awareness in routing protocols is still lacking. Although some protocol supports low-power communication, these protocols are in an early stage of development. In the future, energy harvesting techniques can be promising solutions to full the energy requirements in IoT.

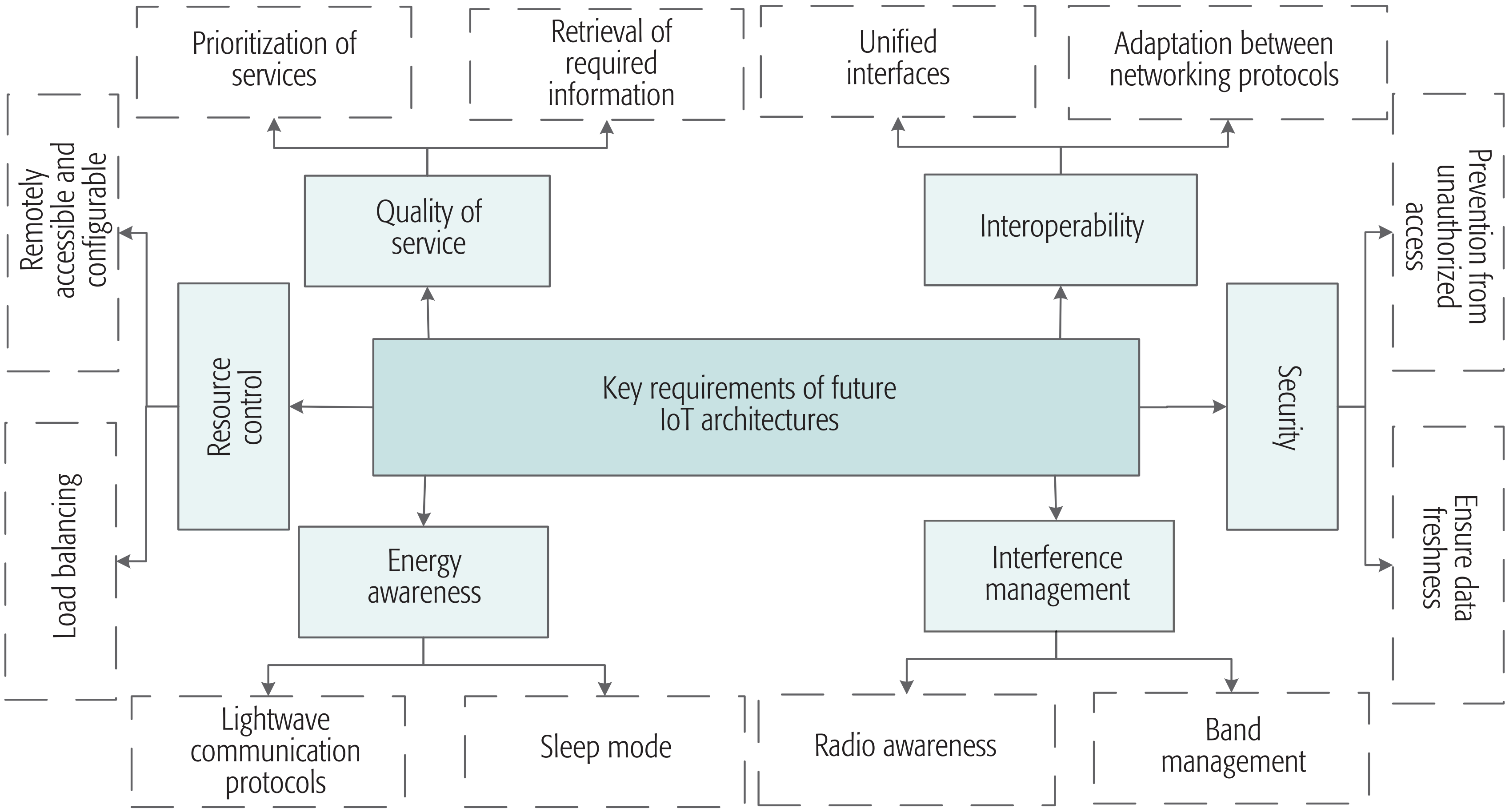
Mobility Management:

Node mobility can create various challenges in terms of IoT network and protocol efficiency. The current mobility protocols of vehicular ad hoc networks (VANETs), mobile ad hoc networks (MANETs), and sensor networks cannot deal well with typical IoT devices due to severe energy and processing constraints. Mobility management is a crucial task, and has two stages. First, movement detection is needed in order to be aware of the device movement, which requires linking to a new region of a network. Second, the signaling and control messages require to be incorporated in such a way that it can help in knowing nodes' locations in a network. Movement detection can be achieved through frequent scans, via either passive messages from participating proto- cols or a beacon from the mobility protocol. Mobility management is one of the key issues in the IoT paradigm. Consequently, it must be considered in the future IoT architecture.

Security:

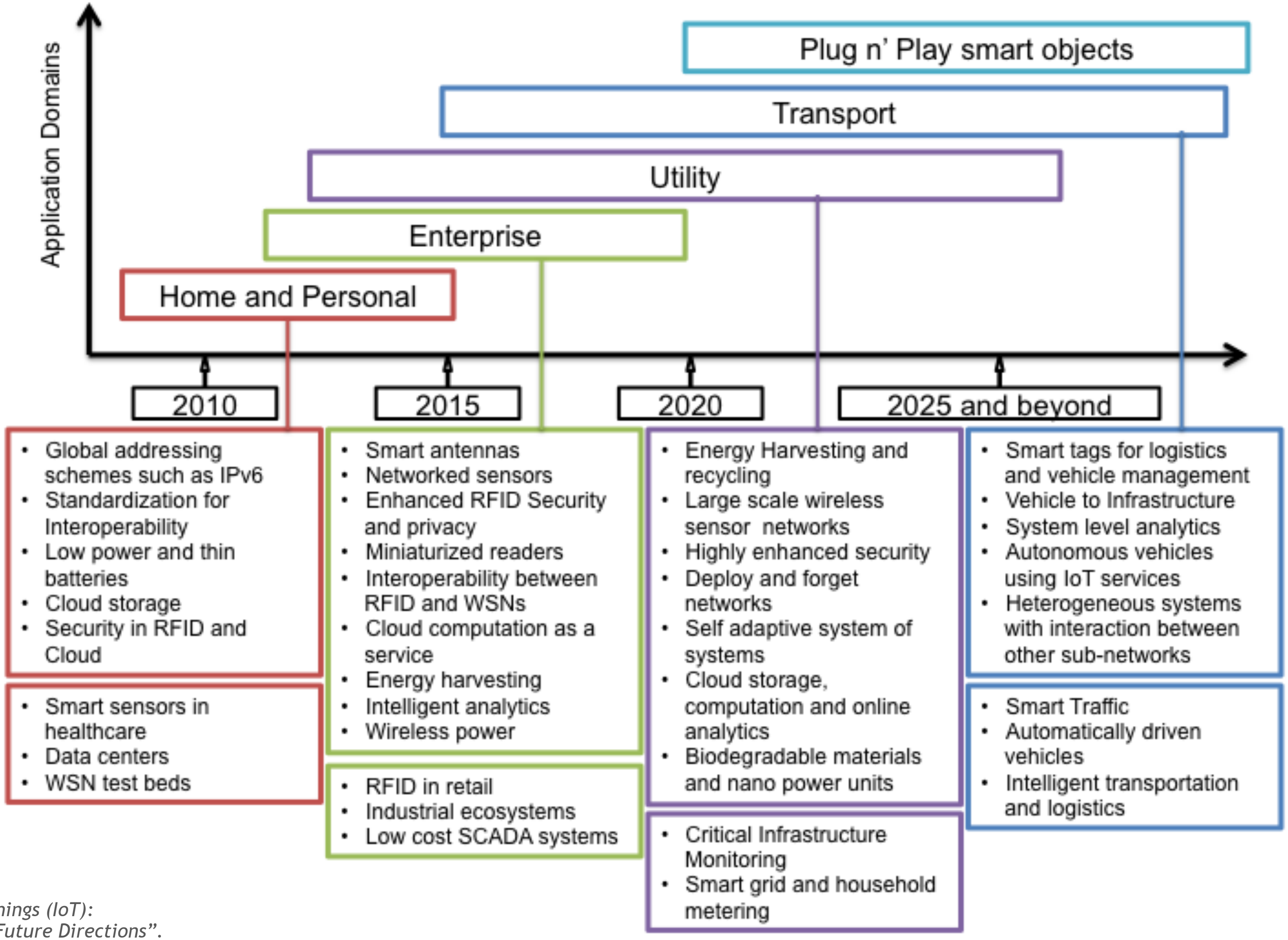
The diversity of IoT applications and heterogeneity of IoT communication infrastructures results in an equally numerous variety of security challenges. In IoT, security can be provided in bottom-up fashion. In a bottom-up way, the system must follow a secure booting process, access control rules, device authentication procedures, and must be able to accept updates and patches of security software in a non-disruptive way. Since the security is a key concern in IoT, suitable security mechanisms must be applied at both the device and network levels (physically and non-physically). IoT devices must have some sort of intelligence to recognize and counteract potential threats. Fortunately, this does not require a revolutionary approach; rather, an evolution of measures that have proven successful in other networks must be adapted in the IoT paradigm by considering the processing capabilities of smart devices.

Key Future Requirements


Prioritization of services
Retrieval of required information
Unified interfaces
Adaptation between networking protocols
Remotely accessible and configurable
Quality of service
Interoperability
Prevention from unauthorized access
Resource control
Key requirements of future IoT architectures
Security
Load balancing
Energy awareness
Interference management
Ensure data freshness
Lightwave communication protocols
Sleep mode
Radio awareness
Band management

Source: I. Yaqoob et al., "Internet of thIngs ArchItecture: recent AdvAnces, tAxonomy, requIrements, And open chAllenges", IEEE Wireless Communications, June 2017.

Applications/Enablers Vision and Timetable



2010

- Global addressing schemes such as IPv6
- Standardization for Interoperability
- Low power and thin batteries
- Cloud storage
- Security in RFID and Cloud

- Smart sensors in healthcare
- Data centers
- WSN test beds

2015

- Smart antennas
- Networked sensors
- Enhanced RFID Security and privacy
- Miniaturized readers
- Interoperability between RFID and WSNs
- Cloud computation as a service
- Energy harvesting
- Intelligent analytics
- Wireless power

- RFID in retail
- Industrial ecosystems
- Low cost SCADA systems

2020

- Energy Harvesting and recycling
- Large scale wireless sensor networks
- Highly enhanced security
- Deploy and forget networks
- Self adaptive system of systems
- Cloud storage, computation and online analytics
- Biodegradable materials and nano power units

- Critical Infrastructure Monitoring
- Smart grid and household metering

2025 and beyond

- Smart tags for logistics and vehicle management
- Vehicle to Infrastructure
- System level analytics
- Autonomous vehicles using IoT services
- Heterogeneous systems with interaction between other sub-networks

- Smart Traffic
- Automatically driven vehicles
- Intelligent transportation and logistics

Source: J. Gubbi et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions".

Summary of Open challenges

- Architecture
- New protocols
- Quality of service
- Energy efficient sensing
- Data processing
- GIS based visualization
- Cloud computing
- Secure reprogrammable networks and Privacy
- Participatory sensing
- International activities

Thank You

شكراً