Session 6

Interoperability, Integration, and Interconnection
of Internet of Things Systems

Prof. Mustapha Benjillali
INPT, Morocco
benjillali@ieee.org
IoT and Multi-layer Interoperability Challenges
IEEE Wireless Communications • June 2017

A generic IoT architecture consists of three layers: application, transport, and sensing. The application layer employs intelligent computing to extract valuable information from process data. The transport layer deals with voluminous data and provides an interface for communication. The sensing layer is responsible for collecting the information.

Despite advantages such as easier problem identification and reduction of human error, the spontaneous gateways of wireless sensor networks (WSNs) in IoT systems are not fully applicable to provide ideal services. The existing networking architectures were only designed to support sporadic access and were not able to accommodate the increasing number of connected devices. Although the spontaneous gateways can provide automated services and resource discovery, the lack of capabilities can cause interference problems. The existing devices are not energy-aware, and secure network architectures will be required in the future for IoT.

The involvement of energy-aware, and secure network architectures will meet the objectives of IoT in terms of better QoS, reliability, effectiveness, and efficient management in wireless network environments. Although the proposed work can provide many benefits such as scalability, quick and easy deployment of resources, and security, the lack of a software-defined network (SDN)-based architecture for the IoT with the multi-layer model designed by the controller is a major drawback.

Although the Internet of Things (IoT) market is expected to rise to US$1.7 trillion by 2020, the number of connected devices to the Internet will be huge in number. Cisco predicted that the number of connected devices will rise to 50 billion by the end of 2020. Therefore, an efficient IoT architecture should be developed. Gartner estimated that by 2020, 4.9 billion Internet of Things (IoT) connected devices will be there in the market. The Internet of Things (IoT) is becoming a reality; it is here.市区互联网的实施将对物联网产生重大影响。
Sensors Layer

- Machine Vision / Optical Ambient Light
- Position / Presence / Proximity
- Acceleration / Tilt
- Motion / Velocity / Displacement
- Electric / Magnetic
- Temperature
- Leaks / Levels
- Humidity / Moisture
- Force / Load / Torque
- Flow
- Strain / Pressure
- Chemical / Gas
- Acoustic / Sound / Vibration

Source: Harbor Research.
Taxonomic Classification

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

<table>
<thead>
<tr>
<th></th>
<th>ZigBee</th>
<th>BLE</th>
<th>LP-Wifi</th>
<th>LPWA</th>
<th>3GPP Rel8</th>
<th>LTE Rel13 &amp; NB-IoT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scalability</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Reliability</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Low Power</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Low Latency</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Large Coverage</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Low module cost</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
</tr>
<tr>
<td>Mobility support</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Roaming support</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SLA support</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Fig. 1. 3GPP releases and timeline.

and protocol implementation were staged for release 11 and captured in respective TS document of responsible working groups. Furthermore, charging requirements were addressed by SA5 to reuse existing 3GPP functions (e.g. session initiation and control) to the extent possible. 3GPP architecture work on MTC started. In Rel-10 and in Rel-12 SA2 worked on efficient transmission of Small Data Transmissions and Low Power Consumption UEs. Ever since, the amount of study items and technical specifications for MTC have increased steadily and are now a core ingredient of standardization work.

The standardization of a new 5G air interface is foreseen by 3GPP to be divided in phases where the first phase, with a finalization targeted during 2018, is focusing on early commercial deployments and a subset of the 5G requirements. The second phase of the standardization, targeted to be finalized at the end of 2019, targets fulfillment of the full set of 5G requirements.

D. 3GPP Security

The security framework used in 3GPP systems was originally developed for GSM to provide a basic connectivity service for human to human communication. The security features of GSM were encryption of the air interface to avoid eavesdropping and strong authentication mechanism of the users. The main security solution was kept for 3G and 4G, but enhancements were done to enhance the security level such as introducing state of the art encryption algorithms, more elaborate key management systems, integrity protection of signaling and mutual authentication. The 3GPP security framework is based on the tamper resistant SIM card, which holds the credentials of the subscriber. By using the credentials of the SIM card and corresponding credentials stored in the network, the device and the network mutually authenticate each other. The authentication mechanism also produces keys, which are then used for encryption and integrity protection of the communication on the radio interface. Subscriber privacy in 3GPP systems is considered by using randomly assigned temporary identifiers to make tracking of devices and users more difficult.

Recently 3GPP have worked on enhancements specifically aimed at MTC applications. The new requirements emerged due to characteristics of MTC such as reduced signaling and even 10 years battery lifetime are being taken into account in the security work. 3GPP is working on to enhance the security level of GPRS in order to support the so called GPRS-based cellular IoT system [29]. Another work is to develop security solutions for 3GPP systems to support very low complexity and low cost devices targeting 10 years battery lifetime [30]. The challenges of the removable SIM card to meet the requirements of MTC, like remotely changing the subscription and fitting a SIM card into a tiny device, were studied in 3GPP some years ago, but the standardization work was started in GSMA and ETSI, and it still continuing under the name of embedded SIM.

IV. 5G INTELLIGENT SERVICES

In order to enable the ubiquitous connectivity required for many of the IoT applications, many more features and functionalities will need to be added to the currently predominantly broadband approach. This inherently leads to a strong heterogeneous networking (HetNet) paradigm with multiple types of wireless access nodes (with different MAC/PHY, coverage, backhaul connectivity, QoS design parameters, among others). HetNets will offer the required seamless connectivity for the emerging IoT through a complex set of mechanisms for coordination and management [31]–[35]. Evolved 4G and emerging 5G networks will thus be characterized by interoperability and

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
B. From SmartM2M to oneM2M

An SCL resources tree (see also Fig. 4) includes different kinds of resources as follows: sclBase, scls, scl, applications, and contentInstance. The contentInstance resource enhances resources tree operations by acting as a search engine for resources. The discovery request on distributed SCLs.

The group resource allows subscribers to receive asynchronous notification when an event happens such as the reception of new sensor event or the creation, update, or delete of a resource. The contentInstance resource act as a mediator for data buffering to enable data exchange between applications and SCLs.

CSFs can be used by applications and other CSEs. An AE is a logical entity that provides application logic, such as remote monitoring functionalities, for end-to-end M2M solutions. A CSE is a logical entity that is instantiated in an M2M node and comprises a set of service functions called common services functions (CSFs). Nodes consist of at least one common services entity (CSE) or one application entity (AE). A CSE is a logical entity that involves around 270 companies that are actively contributing to technology associations (TTA), Korea. These organizations include the European Telecommunications Standards Institute (ETSI), Europe; and the Telecommunications Technology Association of Radio Industries and Businesses (ARIB) and the China Communications Standards Association (CCSA), China; the European Telecommunications Standards Institute (ETSI) and the Alliance for Telecommunications Industry Solutions (ATIS) from the United States; the China Communications Standards Association (CCSA), China; the European Telecommunications Standards Institute (ETSI), Europe; and the Telecommunications Technology Committee (TTC), Japan. OneM2M has been kicked off by seven telecom standards organizations: the Telecommunication Technology Committee (TTC), Japan; the Alliance for Telecommunications Industry Solutions (ATIS) from the United States; the China Communications Standards Association (CCSA), China; the European Telecommunications Standards Institute (ETSI) and the Telecommunications Technology Committee (TTC), Japan; the Alliance for Telecommunications Industry Solutions (ATIS) from the United States; the China Communications Standards Association (CCSA), China; and the Telecommunication Technology Committee (TTC), Japan.

In contrast to SmartM2M, oneM2M relaxes scalability restraints by adopting a hierarchical name space, and are grounded on the concept of horizontal service layer. In contrast to SmartM2M, oneM2M adopts a RESTful design, name resources over three layers: security functions, security environment abstraction, and secure environment. Security functions include:

- security environment abstraction offers many security primitives, security administration, and sensitive data handling and security administration. Security functions include:
- identification, authentication, authorization, security association, and secure environment. Security functions include:
- monitoring functionalities, for end-to-end M2M solutions.

Security functions include:
- identification, authentication, authorization, security association, and secure environment. Security functions include:
- monitoring functionalities, for end-to-end M2M solutions.

Security functions include:
- identification, authentication, authorization, security association, and secure environment. Security functions include:
- monitoring functionalities, for end-to-end M2M solutions.

Security functions include:
- identification, authentication, authorization, security association, and secure environment. Security functions include:
- monitoring functionalities, for end-to-end M2M solutions.

Security functions include:
- identification, authentication, authorization, security association, and secure environment. Security functions include:
- monitoring functionalities, for end-to-end M2M solutions.
Thank You

شكراً
Session 6

Interoperability, Integration, and Interconnection
of Internet of Things Systems

Prof. Mustapha Benjillali
INPT, Morocco
benjillali@ieee.org
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. Moreover, 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. Moreover, 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 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 Internet, 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 addressing 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 security mechanisms must be lightweight as most of the devices are resource constrained. Moreover, ensuring the freshness of data is also very important. 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 processing 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-layer 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-added, and autonomous on-the-move services. Moreover, personalized, customized, autonomous, and dynamic services can be supported by constructing 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 backbone of IoT. However, these devices have limited 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 protocols 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

7.2. Energy efficient sensing

Effficient heterogeneous sensing of the urban environment needs to simultaneously meet competing demands of multiple sensing modalities. This has implications on network traffic, data storage and energy utilization. Importantly, this encompasses both fixed and mobile sensing infrastructure as well as continuous and random sampling. A generalized framework is required for data collection and modelling that effectively exploits spatial and temporal characteristics of the data, both in the sensing domain as well as the associated transform domains. For example, urban noise mapping needs an uninterrupted collection of noise levels using battery powered nodes using fixed infrastructure and participatory sensing as a key component for health and quality of life services for its inhabitants.

Compressive sensing enables reduced signal measurements without impacting accurate reconstruction of the signal. A signal sparse in one basis may be recovered from a small number of projections onto a second basis that is incoherent with the first. The problem reduces to finding sparse solutions through smallest $l_1$-norm coefficient vector that agrees with the measurements. In the ubiquitous sensing context, this has implications for data compression, network traffic and the distribution of sensors.

Compressive wireless sensing (CWS) utilizes synchronous communication to reduce the transmission power of each sensor; transmitting noisy projections of data samples to a central location for aggregation.

7.3. Secure reprogrammable networks and Privacy

Security will be a major concern wherever networks are deployed at large scale. There can be many ways the system could be attacked - disabling the network availability; pushing erroneous data into the network; accessing personal information; etc. The three physical components of IoT - RFID, WSN and cloud are vulnerable to such attacks. Security is critical to any network and the first line of defence against data corruption is cryptography. Of the three, RFID (particularly passive) seems to be the most vulnerable as it allows person tracking as well as the

---

**Applications/Enablers Vision and Timetable**

**Applications/Enablers**
- Home and Personal
- Enterprise
- Utility
- Transport

**Source**
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