Challenges Introduced by 5G in IoT Middleware

Technological Requirements of 5G Systems

5G is a promising technology that has been considered the next step for a long term worldwide evolution of mobile communication. 5G is intended to be the major component of the networked or IoT/M2M-oriented society, and will help to realize the IoT vision toward unlimited access to information and sharing of pervasive data (anywhere and anytime) for anyone (human-centric approach) and anything (device/things-oriented approach) The aim of 5G is not only about mobile

connectivity for people, but also mobile and ubiquitous connectivity for any kind of computing device and application that may benefit from being connected to the Internet (IoT) and also to the Web (WoT—Web of Things).

In order to enable massive connectivity for a very wide range of heterogeneous IoT applications and devices, the capabilities of 5G mobile networks must extend far beyond those of previous generations of mobile communication (e.g., 3G and 4G).

A. *Massive System Capacity*

Massive system capacity is related to higher data traffic demands and higher number of IoT devices and applications that will be connected to the Internet in the 5G Era. Data traffic demands for mobile communication in IoT systems are predicted to increase dramatically in the coming years. To support such demand, 5G network technologies must be able to deliver data with much lower cost per bit compared with the current and available networks. Furthermore, in order to be able to operate with the same or preferably even lower overall energy consumption compared with today mobile technologies, 5G must enable radically lower energy consumption per delivered bit.

Another aspect of 5G-system capacity is the capability to support a much larger number of IoT devices and applications compared with today. The new use cases envisioned for 5G-based IoT applications include, for example, the deployment of billions of wirelessly connected sensors, actuators, and other mobile devices, but allowing that each device will be associated with very little traffic, implying that, even jointly, they will have a limited impact on the overall traffic volume of the network.

B. *Higher Ubiquitous Data Rates for Real-life Conditions Situations*

Every generation of mobile communication technology has been associated with higher data rates compared with the previous one. In the past, much focus has been taken on the peak data rate that can be supported by a wireless-access technology under ideal conditions. However, a more interesting requirement regarding capability is the data rate that can actually be provided under real-life conditions in different IoT scenarios. In this way, the intended data rates requirements for 5G must be:

- 10 Gbps in specific scenarios such as indoor and dense outdoor environments;
- 100 Mbps should be generally achievable in urban and sub-urban environments;
- (At least) 10 Mbps should be achievable essentially everywhere, including sparsely populated rural areas in both developed and developing countries.

C. *Very Low Latency for Next-generation Networks*

Lower latency network has been a key target for both 4G and the evolution of 3G, driven mainly by the continuous quest for higher achievable data rates. As envisioned IoT applications (e.g., traffic safety and control of critical infrastructure and industry processes) may require much lower latency compared with what is possible with the mobile communication systems of today, the 5G research community is targeting higher data rates, which itself, will drive a need for very lower latency. To support such latency-critical applications, 5G should allow for an end-to-end application, a latency of 1ms or less.

D. *Ultra-high Reliability and Availability for Mobile Connectivity*

In addition to very low latency, 5Gshould also enable mobile connectivity with ultrahigh reliability and availability. For critical services, such as Healthcare monitoring systems and Traffic Safety, connectivity with certain guarantees, such as specific maximum latency, should not only be “typically available”. Rather, ensuring connectivity with specific requirements should be always available (i.e., with “availability”) and essentially with no deviation (i.e., with “reliability”).

E. *Very Low Cost and Energy Consumption for Mobile Devices*

The possibility for low cost and low energy consumption for mobile devices has been a key requirement since the early days of mobile communication. However, in order to enable the vision of billions of wirelessly connected devices, a further step has to be taken in terms of hardware cost and energy consumption. It should be possible for such IoT/5G devices to be available at very low cost and with a battery life of several years without recharging.

F. *Virtualized Network Technology Support*

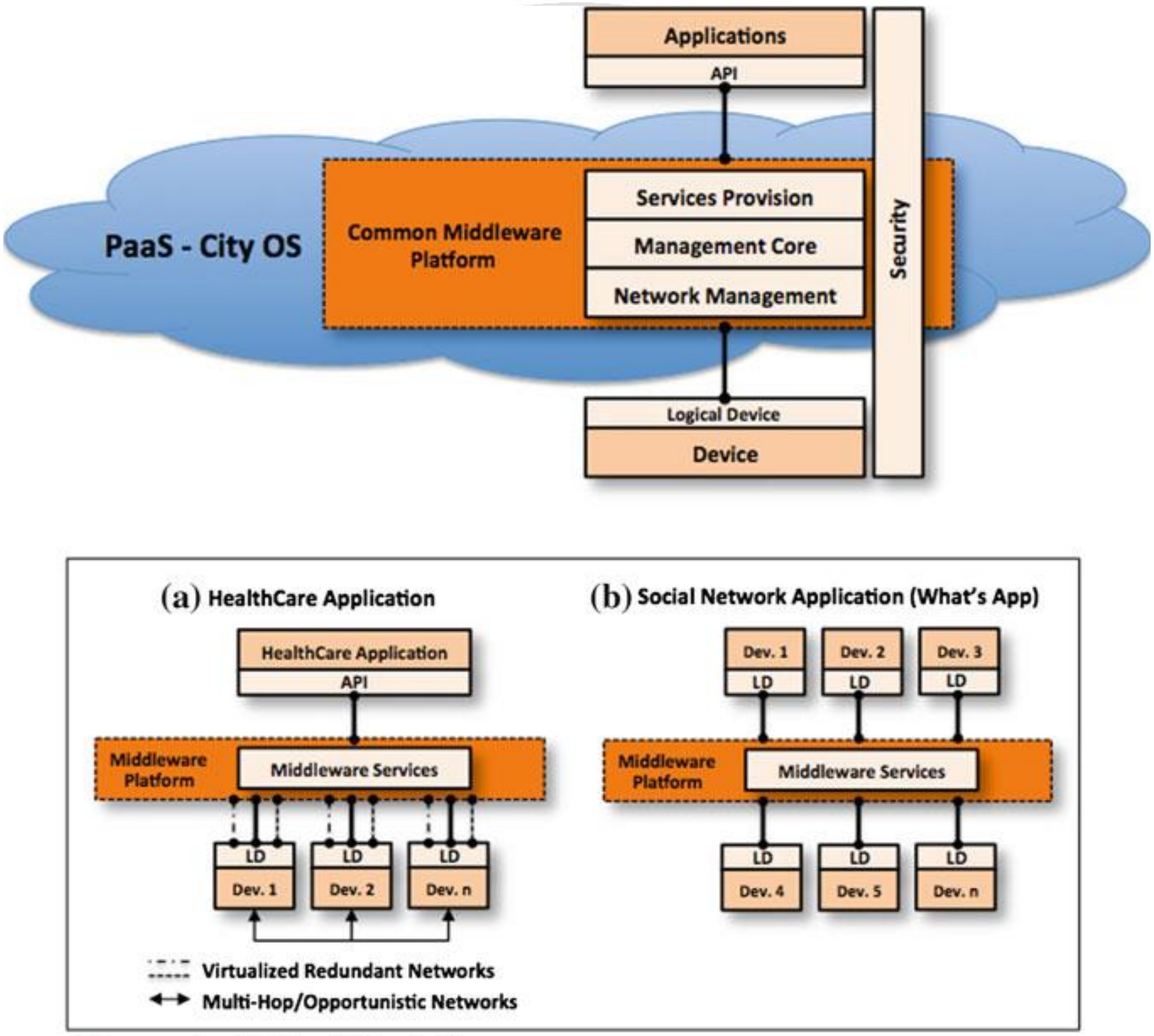
Cost and deployment flexibility will also be important factors in 5G networks, requiring a shift toward software-based implementations and virtualization technologies. In particular, 5Gsystems will be able to create multiple virtual core networks tailored to the specialized requirements of particular applications. For example, the system could create a virtual core network to support M2M, a separate virtual core network to support the Internet content, and another virtual core network to support operator differentiated media services, all of which can be configured by dynamically utilizing the network resources from the same or different networks.

Perspectives and a Middleware Approach Toward 5G (COMPaaS Middleware)

IoT middleware systems will have to support the requirements imposed by 5G which will result in specific changes to allow the applications requirements demanded by 5G.

Figure 2.6 illustrates a possible system architecture for 5G-based IoT Middleware with two application examples: (a) a “Healthcare Monitoring application” oriented to mission-critical services in a hospital (i.e., a group of medical devices and sensors for patients monitoring that continuously route data through redundant networks to guarantee delivery of priority data), and

(b) a non-critical example focused on “Social Networks” as WhatsApp Messenger (i.e., a set of smart phones interacting through the Internet with the middleware which acts as a topic-based pub/sub server notifying users with appropriated data).



• Two examples of 5G-based IoT applications

Fig.2.6 IoT middleware as a common platform for city OS

[Ref: L.A. Amaral et al. Middleware Technology for IoT Systems: Challenges and Perspectives Toward 5G,2016]

In case of disaster relief operations or EMS, an ambulance-to-hospital based e- Health system is a good example of how 5G-based IoT technology can help save lives. In this case, by providing real-time patient information to the hospital via wireless communications, this e-Health system enables remote diagnoses and primary care, and reducing rescue response time.

In both cited cases we can use IoT middleware systems to abstract the devices or medical equipment's integration from a house or an ambulance, and also to allow the interaction with hospital systems In EMS, for example, the IoT Middleware can locate the ambulance and provide the shortest path routing, so patients can be carried to the hospital as quickly as possible. In this sense, it is also important to have an effective middleware system to ensure that the response time between send and interpret data is fast enough to guarantee that all decisions of a doctor are based on the current health condition of the patient.

Regarding the core architecture illustrated in Fig. 2.6, one of the necessary changes is related to the "potential processing in cloud", since 5G network will be able to transmit data in a reliable and fast manner. In this perspective, the middleware would be involved in the provision of reliable and elastic services to interact with the physical devices, allowing to abstract both the integration and interoperability of data, which potentially can be embedded in the cloud, but performing the same tasks as it does outside the cloud.

In 5G environments, the communication between objects will be faster than today. IoT middleware systems will have also to be widely more scalable than they are today in order to ensure more connections from devices and applications allowing them to communicate. To cope with this, a more interoperable middleware system will be necessary to interact with other middleware systems, and also to understand the different data types. "Interoperability and scalability" are two essential requirements that will ensure the IoT consolidation through the 5G evolution.

As the number of devices will increase drastically, IoT middleware systems will need to host "context-aware lookup services" that enable discovery and management of thousands of devices. The use of these services will ensure the context provision for applications beyond the proper management of devices. In addition, a requirement that will be present to ensure the provision of lookup services is "context awareness".Context is extremely important to allow the composition of services with relevant and appropriate information to the user at anytime and anyplace. Moreover, context will be used to give sense to the devices connected to the network in order to be used in the best possible way.

Finally, all middleware perspectives aimed to 5G will need a "security architecture" that should be lightweight in order to provide security in all the middleware layers, as well as to contemplate all security requirements necessary to ensure system protection against various threats that will arise, especially in communication networks.

COMPaaS Middleware

COMPaaS (Cooperative Middleware Platform as a Service) is an IoT middleware system that has been tailored to support the 5G technology integration. Basically, the goals of the COMPaaS can be summarized as follows:

- Abstraction of the integration and interoperation between applications and physical devices through the provision of hierarchical system services according to device profiles (i.e., a set of functional characteristics describing each physical device).
- Abstraction of the collection and management of data provided by physical devices through the provision of application-level services.
- Provision of high-level services to facilitate the development and integration of IoT applications.
- Provision of a software architecture based on IoT/M2M andWoT (Web of Things) standards.

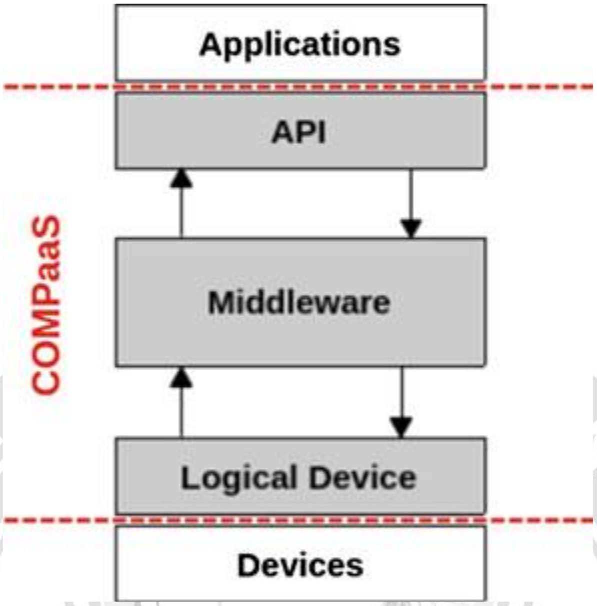


Fig.2.6 IoT middleware as a common platform for city OS

[Ref: L.A. Amaral et al. Middleware Technology for IoT Systems: Challenges and Perspectives Toward 5G,2016]

COMPaaS architecture is based on SOA approach and is composed of two main systems as shown in Fig. 2.6: “Middleware” and “Logical Device”. Logical Device is the system responsible for hiding all the complexity of physical devices and abstracts the functionality of these devices to the upper layer.

Middleware: Middleware is the system responsible for abstracting the interaction between applications and devices and also for hiding all the complexity involved in these activities. It provides an API to be used by applications in order to use the services of the COMPaaS. The main functions of the middleware range from data management to device integration and address the provision of high-level services to applications. Figure 2.7 presents the organization of the modules of the middleware. All services are part of the middleware API available to applications, except the communication service, which is used for both applications and logical devices. The rest of the modules (Resource Manager, Resource Handler, and Event Handler) allows the integration with logical device(s).

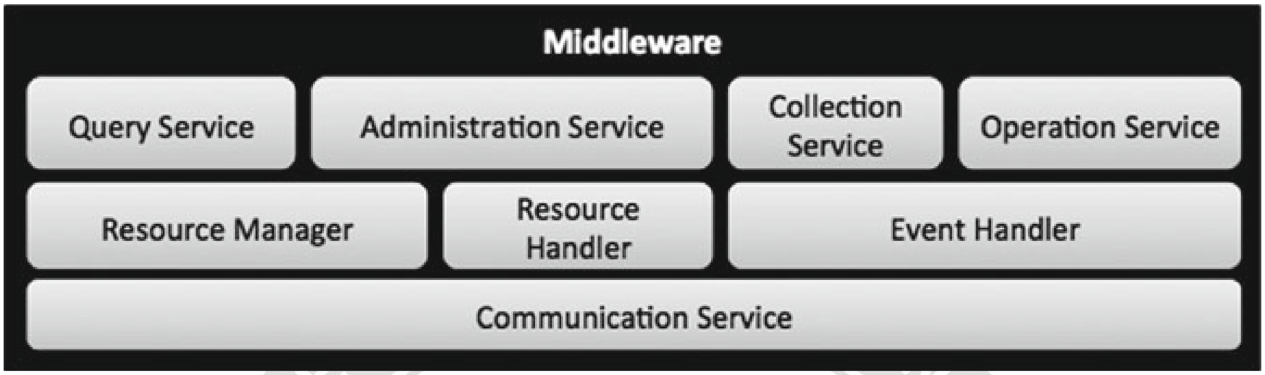


Fig.2.7 Modules of the COMPaaS

[Ref: L.A. Amaral et al. Middleware Technology for IoT Systems: Challenges and Perspectives Toward 5G,2016]

Logical Device: This is the middleware abstraction for the physical devices that are relevant to the applications and that must be accessible to provide some benefit. Logical Devices are described through system profiles. Each system profile contains attributes to characterize the physical device, such as: name, manufacturer, function, model, data type, URI, etc. These attributes are used by applications to find the desired devices. Besides the profile, logical device also contains two more system elements: ***communication module and service module***. The communication module is not only responsible for the publication of the resource (the registration of the resource in the middleware), but also for the provision of the features for data communication and for notification of the operational status of the resource to the middleware. On the other hand, the service module is responsible to expose the interfaces and features of the resource to the middleware.