Overview of the Internet of things

Tatiana Kurakova,

International Telecommunication Union
Place des Nations CH-1211 Geneva, Switzerland

Abstract. This article provides an overview of the Internet of things (IoT). It gives ITU definition of IoT, clarifies the concept and scope of the IoT, identifies the fundamental characteristics and high-level requirements of the IoT and describes the IoT reference model. In conclusion, it gives some examples of practical application of the concept of IoT to everyday lives.

Keywords: Device, Internet of things, physical thing, reference model, thing, virtual thing.

1 Introduction of the IoT

1.1 Concept of the IoT

The Internet of things (IoT) can be perceived as a far reaching vision with technological and societal implications [6].

From the perspective of technical standardization, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT) [2].

Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of "things" to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE – The IoT is expected to greatly integrate leading technologies, such as technologies related to advanced machine-to-machine communication, autonomic networking, data mining and decision-making, security and privacy protection and cloud computing, with technologies for advanced sensing and actuation.

As shown in Figure 1, the IoT adds the dimension "Any THING communication" to the information and communication technologies (ICTs) which already provide "any TIME" and "any PLACE" communication.

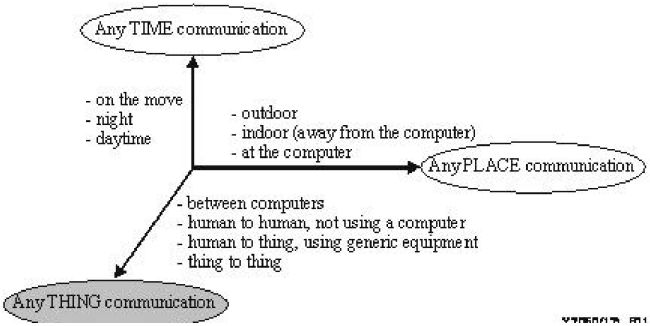

Fig. 1. The new dimension introduced in the Internet of things [1]

Regarding the IoT, things are objects of the physical world (physical things) or of the information world (virtual world) which are capable of being identified and integrated into communication networks. Things have associated information, which can be static and dynamic.

Physical things exist in the physical world and are capable of being sensed, actuated and connected. Examples of physical things include the surrounding environment, industrial robots, goods and electrical equipment.

Virtual things exist in the information world and are capable of being stored, processed and accessed. Examples of virtual things include multimedia content and application software.

1.2 Technical overview of the IoT

Figure 2 shows the technical overview of the IoT.

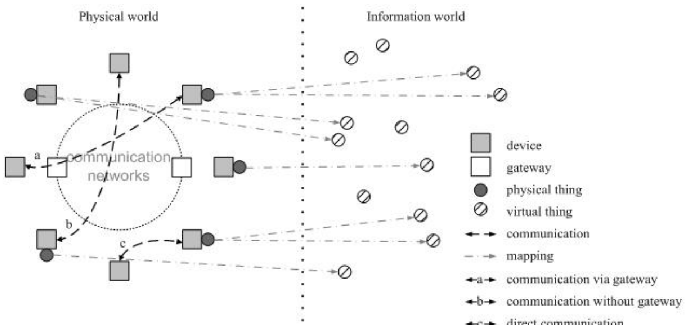

Fig. 2. Technical overview of the IoT [2]

A physical thing may be represented in the information world via one or more virtual things (mapping), but a virtual thing can also exist without any associated physical thing.

A device is a piece of equipment with the mandatory capabilities of communication and optional capabilities of sensing, actuation, data capture, data storage and data processing. The devices collect various kinds of information and provide it to the information and communication networks for further processing. Some devices also execute operations based on information received from the information and communication networks.

Devices communicate with other devices: they communicate through the communication network via a gateway (case a), through the communication network without a gateway (case b) or directly, that is without using the communication network (case c). Also, combinations of cases a and c, and cases b and c are possible; for example, devices can communicate with other devices using direct communication through a local network (i.e., a network providing local connectivity between devices and between devices and a gateway, such as an ad-hoc network) (case c) and then communication through the communication network via a local network gateway (case a).

NOTE 1 – Although Figure 2 shows only interactions taking place in the physical world (communications between devices), interactions also take place in the information world (exchanges between virtual things) and between the physical world and the information world (exchanges between physical things and virtual things).

The IoT applications include various kinds of applications, e.g., "intelligent transportation systems", "smart grid", "e-health" or "smart home". The applications can be based on proprietary application platforms, but can also be built upon common service/application support platform(s) providing generic enabling capabilities, such as authentication, device management, charging and accounting [2].

The communication networks transfer data captured by devices to applications and other devices, as well as instructions from applications to devices. The communication networks provide capabilities for reliable and efficient data transfer. The IoT

network infrastructure may be realized via existing networks, such as conventional TCP/IP-based networks, and/or evolving networks, such as next generation networks (NGN).

Figure 3 shows the different types of devices and the relationship between devices and physical things.

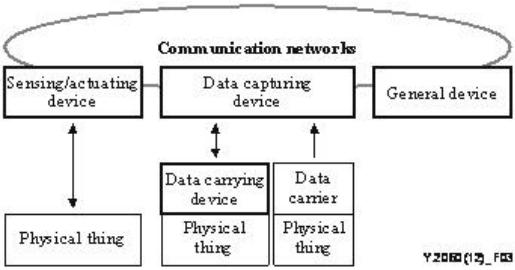

Fig. 3. Types of devices and their relationship with physical things

NOTE 2 – A "general device" is also a (set of) physical thing(s).

The minimum requirement of the devices in the IoT is their support of communication capabilities. Devices are categorized into data-carrying devices, data-capturing devices, sensing and actuating devices and general devices as described as follows:

- Data-carrying device: A data-carrying device is attached to a physical thing to indirectly connect the physical thing with the communication networks.
- Data-capturing device: A data-capturing device refers to a reader/writer device with the capability to interact with physical things. The interaction can happen indirectly via data carrying devices, or directly via data carriers attached to the physical things. In the first case, the data-capturing device reads information on a data-carrying device and can optionally also write information given by the communication networks on the data carrying device.

  NOTE 3 – Technologies used for interaction between data-capturing devices and data-carrying devices or data carriers include radio frequency, infrared, optical and galvanic driving.
- Sensing and actuating device: A sensing and actuating device may detect or measure information related to the surrounding environment and convert it into digital electronic signals. It may also convert digital electronic signals from the information networks into operations. Generally, sensing and actuating devices form local networks communicate with each other using wired or wireless communication technologies and use gateways to connect to the communication networks.
- General device: A general device has embedded processing and communication capabilities and may communicate with the communication networks via wired or wireless technologies. General devices include equipment and appliances for dif-

ferent IoT application domains, such as industrial machines, home electrical appliances and smart phones.

2 Fundamental characteristics and high-level requirements of the IoT

2.1 Fundamental characteristics

The fundamental characteristics of the IoT are as follows:

- Interconnectivity: With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.
- Things-related services: The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.
- Heterogeneity: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.
- Dynamic changes: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.
- Enormous scale: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.

2.2 High-level requirements

The following provide high-level requirements which are relevant for the IoT:

- Identification-based connectivity: The IoT needs to support that the connectivity between a thing and the IoT is established based on the thing's identifier. Also, this includes that possibly heterogeneous identifiers of the different things are processed in a unified way.
- Interoperability: Interoperability needs to be ensured among heterogeneous and distributed systems for provision and consumption of a variety of information and services.
- Autonomic networking: Autonomic networking (including self-management, self configuring, self-healing, self-optimizing and self-protecting techniques and/or mechanisms) needs to be supported in the networking control functions of the IoT,

in order to adapt to different application domains, different communication environments and large numbers and types of devices.

- Autonomic services provisioning: The services need to be able to be provided by capturing, communicating and processing automatically the data of things based on the rules configured by operators or customized by subscribers. Autonomic services may depend on the techniques of automatic data fusion and data mining.
- Location-based capabilities: Location-based capabilities need to be supported in the IoT. Something-related communications and services will depend on the location information of things and/or users. It is needed to sense and track the location information automatically. Location-based communications and services may be constrained by laws and regulations, and should comply with security requirements.
- Security: In the IoT, every 'thing' is connected which results in significant security threats, such as threats towards confidentiality, authenticity and integrity of both data and services. A critical example of security requirements is the need to integrate different security policies and techniques related to the variety of devices and user networks in the IoT.
- Privacy protection: Privacy protection needs to be supported in the IoT. Many things have their owners and users. Sensed data of things may contain private information concerning their owners or users. The IoT needs to support privacy protection during data transmission, aggregation, storage, mining and processing. Privacy protection should not set a barrier to data source authentication.
- High quality and highly secure human body related services: High quality and highly secure human body related services needs to be supported in the IoT. Different countries have different laws and regulations on these services.
  NOTE – Human body related services refer to the services provided by capturing, communicating and processing the data related to human static features and dynamic behaviour with or without human intervention.
- Plug and play: Plug and play capability needs to be supported in the IoT in order to enable on-the-fly generation, composition or the acquiring of semantic-based configurations for seamless integration and cooperation of interconnected things with applications, and responsiveness to application requirements.
- Manageability: Manageability needs to be supported in the IoT in order to ensure normal network operations. IoT applications usually work automatically without the participation of people, but their whole operation process should be manageable by the relevant parties.

3 IoT reference model

Figure 4 shows the IoT reference model. It is composed of four layers as well as management capabilities and security capabilities which are associated with the four layers.

The four layers are as follows [2]:

- application layer

– service support and application support layer
– network layer
– device layer.

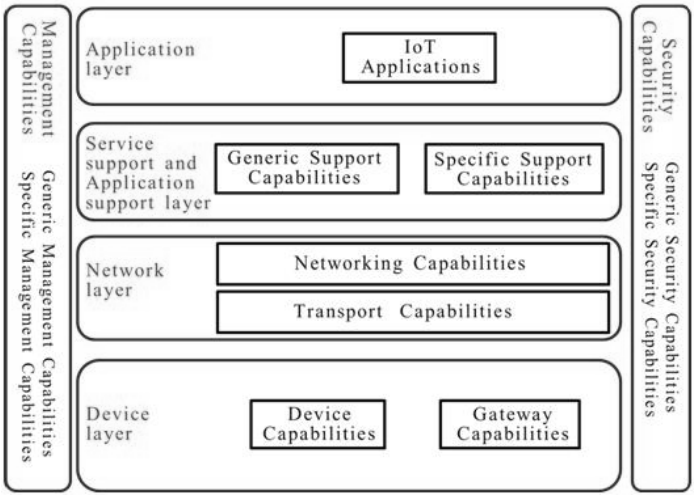

Fig. 4. IoT reference model

3.1 Application layer

The application layer contains IoT applications.

3.2 Service support and application support layer

The service support and application support layer consists of the following two capability groupings:

– Generic support capabilities: The generic support capabilities are common capabilities which can be used by different IoT applications, such as data processing or data storage. These capabilities may be also invoked by specific support capabilities, e.g., to build other specific support capabilities.
– Specific support capabilities: The specific support capabilities are particular capabilities which cater for the requirements of diversified applications. In fact, they may consist of various detailed capability groupings, in order to provide different support functions to different IoT applications.

3.3 Network layer

This consists of the following two types of capabilities:

- Networking capabilities: provide relevant control functions of network connectivity, such as access and transport resource control functions, mobility management or authentication, authorization and accounting (AAA).
- Transport capabilities: focus on providing connectivity for the transport of IoT service and application specific data information, as well as the transport of IoT-related control and management information.

3.4 Device layer

Device layer capabilities can be logically categorized into two kinds of capabilities:

- **Device capabilities:**
  The device capabilities include but are not limited to:
  Direct interaction with the communication network: Devices are able to gather and upload information directly (i.e., without using gateway capabilities) to the communication network and can directly receive information (e.g., commands) from the communication network.
  Indirect interaction with the communication network: Devices are able to gather and upload information to the communication network indirectly, i.e., through gateway capabilities. On the other side, devices can indirectly receive information (e.g., commands) from the communication network.
  Ad-hoc networking: Devices may be able to construct networks in an ad-hoc manner in some scenarios which need increased scalability and quick deployment.
  Sleeping and waking-up: Device capabilities may support "sleeping" and "waking-up" mechanisms to save energy.

NOTE – The support in a single device of both capabilities of direct interaction with the communication network and indirect interaction with the communication network is not mandatory.

- –**Gateway capabilities:**
  The gateway capabilities include but are not limited to:
  Multiple interfaces support: At the device layer, the gateway capabilities support devices connected through different kinds of wired or wireless technologies, such as a controller area network (CAN) bus, ZigBee, Bluetooth or Wi-Fi. At the network layer, the gateway capabilities may communicate through various technologies, such as the public switched telephone network (PSTN), second generation or third generation (2G or 3G) networks, long-term evolution networks (LTE), Ethernet or digital subscriber lines (DSL).
  Protocol conversion: There are two situations where gateway capabilities are needed. One situation is when communications at the device layer use different device layer protocols, e.g., ZigBee technology protocols and Bluetooth technology protocols, the other one is when communications involving both the device layer

and network layer use different protocols e.g., a ZigBee technology protocol at the device layer and a 3G technology protocol at the network layer.

3.5 Management capabilities

In a similar way to traditional communication networks, IoT management capabilities cover the traditional fault, configuration, accounting, performance and security (FCAPS) classes, i.e., fault management, configuration management, accounting management, performance management and security management.

The IoT management capabilities can be categorized into generic management capabilities and specific management capabilities.

Essential generic management capabilities in the IoT include:

- device management, such as remote device activation and de-activation, diagnostics, firmware and/or software updating, device working status management;
- local network topology management;
- traffic and congestion management, such as the detection of network overflow conditions and the implementation of resource reservation for time-critical and/or life-critical data flows.

Specific management capabilities are closely coupled with application-specific requirements, e.g., smart grid power transmission line monitoring requirements.

3.6 Security capabilities

There are two kinds of security capabilities: generic security capabilities and specific security capabilities. Generic security capabilities are independent of applications. They include:

- at the application layer: authorization, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus;
- at the network layer: authorization, authentication, use data and signaling data confidentiality, and signaling integrity protection;
- at the device layer: authentication, authorization, device integrity validation, access control, data confidentiality and integrity protection.

Specific security capabilities are closely coupled with application-specific requirements, e.g., mobile payment, security requirements.

4 Examples of practical application of IoT concept

4.1 Sensor Control Networks (SCN)

SCNs are intended for controlling over human and machine objects (actuators) on real-time basis depending on environment parameters. For environment parameter measurement is deployed a mote infrastructure which is an evolution of sensor net-

works. In comparison with a sensor in a sensor network, a mote in a SCN, besides physical conditions monitoring, may also provide data manipulation, intelligent commutation and actuator connectivity capabilities. Motes can be connected to NGN by the use of a gateway or directly and may also act as an access network to the SCN applications for actuators [3].

The goal of any SCN application is decision making process which consists in providing all the actuators with relevant control commands. This process includes a diversity of data acquisition, transfer and manipulation activities [5]. A range of architecture models starting from centralized to fully distributed may be employed for SCN application decision making process depending on capabilities of actuators and motes. E.g., an actuator may just use commands provided by SCN application to itself, customize it to meet its own capabilities and user requirements or fulfil decision making completely by itself basing on the data provided by the SCN application.

A number of applications of SCNs exist in:

- everyday life: navigation, excursions, sports;
- medicine: consistent body control, call in an ambulance;
- enterprise: logistics, stock management;
- industrial field: fabrication automation, production process control;
- military field: combat assistance, remote piloting;
- disaster management: early warning, evacuation, orchestration of civilians and rescuers, automatic danger elimination.

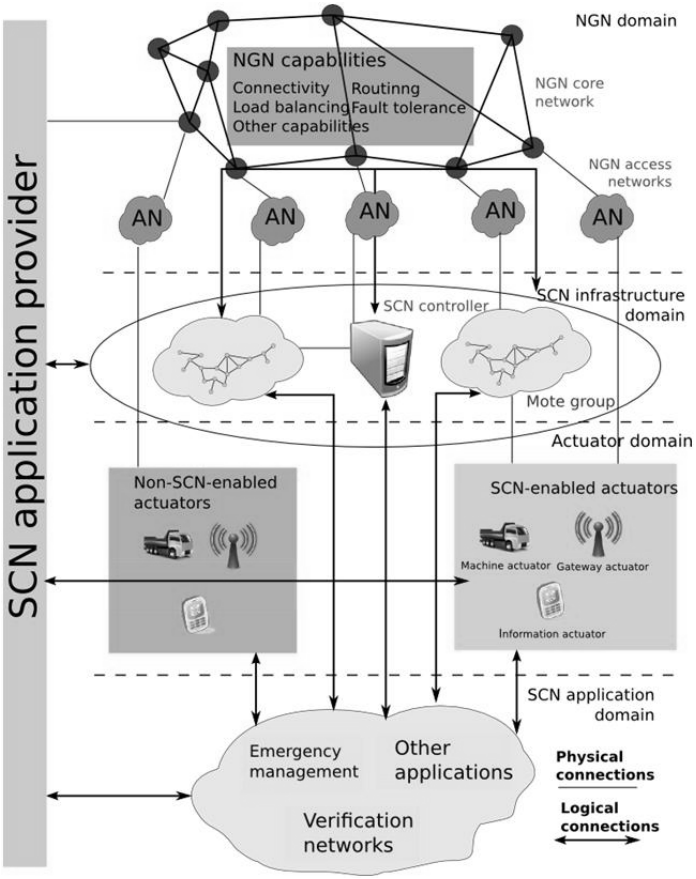

Fig. 5. SCNs and their applications [3]

4.2 Ubiquitous Plant Farming

IT Convergence with agriculture is expected to bring more efficiency and quality improvement in producing, distributing, consuming of agricultural products with the aid of information processing and autonomous control technologies of the IT area. Practical implementation of such a convergence recognizes that there exist many dif-

ficulties to establish services and systems to actualize the IT convergence service in the agricultural field to cope with various objects such as time-varying weather changes, growth condition of farm products, and continual diseases or technical problems such as battery life, sensor malfunctions at severe conditions. In addition, the gap of viewpoints between the people engaged in farming and the IT engineers may cause more problems for accomplishing this mission [4].

Ubiquitous Plant Farming can be run autonomously without human intervention when we apply the most advanced technologies such as sensors, computers, or control systems. Ubiquitous Plant Farming could be supported by future network services, i.e., farm products theft service, farm products traceability service, remote farm management service, farm production regulation service, as shown in the Figure 6. Detailed description on these service features will be given next.

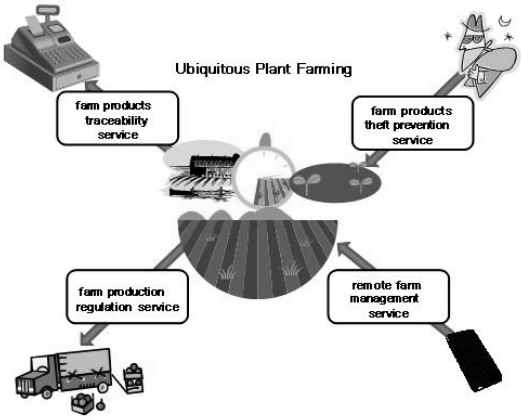

Fig. 6. Conceptual diagram of network-based Ubiquitous Plant Farming [4].

References

1. ITU report "The Internet of Things" (2005)
2. Recommendation ITU-T Y.2060 "Overview of Internet of Thing" (06/2012)
3. Draft Recommendation Y.2222 (Y.SCN) "Sensor control networks and their applications over NGN" (TD GEN 59, February – March meeting of ITU-T Study Group 13)
4. A.Iera, C.Floerkemeier, J.Mitsugi, G.Morabito. "The Internet of Things." IEEE Wireless Communications. Dec. 2010, v.17,#6.

5. Draft Recommendation "Service model and scenarios for Ubiquitous Plant Farming based on networks" (TD GEN 81)
6. Valery V. Butenko, Anatoly P. Nazarenko, Viliam K. Sarian, Nikolay A. Sushchenko, and Alexander S. Lutokhin. “Personal safety in emergencies - Innovative application for mobile phones”. ITU News March 2012, Nr 3
7. Malcolm Johnson. “ITU-T Highlights 2009 - 2012”, WTSA-12, November 2012