Introduction to IoT

1. Introduction to IoT

1.1. Introduction

Building upon a complex network connecting billions of devices and humans into a multi-technology, multi-protocol and multi-platform infrastructure, the Internet-of-Things (IoT) main vision is to create an intelligent world where the real, digital and the virtual are converging to create smart environments that provide more intelligence to the energy, health, transport, cities, industry, buildings and many other areas of our daily life. It is expected to interconnect millions of islands of smart networks enabling access to the information not only “anytime” and “anywhere” but also using “anything” and “anyone” ideally through any “path”, “network” and “any service”. This will be achieved by having the objects that we manipulate daily to be outfitted with sensing, identification and positioning devices and endowed with an IP address to become smart objects capable of communicating with not only other smart objects but also with humans with the expectation of reaching areas that we could never reach without the advances made in the sensing, identification and positioning technologies. While being globally discoverable and queried, these smart objects can similarly discover and interact with external entities by querying humans, computers and other smart objects. The smart objects can also obtain intelligence by making or enabling context related decisions by taking advantage of the available communication channels to provide information about themselves and can access information that has been aggregated by other smart objects.

Figure 1: Internet-connected devices and the future evolution (Source: Cisco, 2011)

As revealed by Figure 1, the IoT is the new essential infrastructure which is predicted to connect 50 billion of smart objects in 2020 when the world population will reach 7.6 billion. As suggested by the ITU, such essential infrastructure will be built around a multi-layered architecture where the smart objects will be used to deliver different services through the four main layers depicted by Figure 2: a device layer, a network layer, a support layer and the application layer. In the device layer lies devices (sensors, actuators, RFID devices) and gateways used to collect the sensor readings for further processing while the network layer provides the necessary transport and networking capabilities for routing the IoT data to processing places. The service and application layer is a middleware layer that serves to hide the complexity of the lower layers to the application layer and provide specific and generic services such as storage in different forms (database management systems and/or cloud computing systems) and many other services such as translation.

Figure 2: IoT Layered Architecture (Source: ITU-T)

As depicted by Figure 3, the IoT can be perceived as an infrastructure driving a number of applications services which are enabled by a number of technologies. Its application services expand across many domains such as smart cities, smart transport, smart buildings, smart energy, smart industry and smart health while it is enabled by different technologies such as sensor, nanoeletronics, wireless sensor network (wsn), radio frequency identification (RFID), localization, storage and cloud. The IoT systems and applications are designed to provide security, privacy, safety, integrity, trust, dependability, transparency, anonymity and are bound by ethics constraints.

Figure 3: IoT-3Dimentional View (Source: [1])

Experts say we are heading towards what can be called a "ubiquitous network society", one in which networks and networked devices are omnipresent. RFID and wireless sensors promise a world of networked and interconnected devices that provide relevant content and information whatever the location of the user. Everything from tires to toothbrushes will be in communications range, heralding the dawn of a new era, one in which today's Internet (of data and people) gives way to tomorrow's Internet of Things. At the dawn of the Internet revolution, users were amazed at the possibility of contacting people and information across the world and across time zones. The next step in this technological revolution (connecting people any-time, anywhere) is to connect inanimate objects to a communication network. This vision underlying the Internet of things will be facilitated by implemented here the information will be accessed not only "anytime" and "anywhere" but also using "anything". This will be facilitated by using WSNs and RFID tags to extend the communication and monitoring potential of the network of networks, as will the introduction of computing power in everyday items such as razors, shoes and packaging. WSNs are an early form of ubiquitous information and communication networks. They are one of building blocks of the Internet of things.

1.2. Wireless Sensor Networks

A Wireless Sensor Network (WSN) is a self-configuring network of small sensor nodes (so-called motes) communicating among them using radio signals, and deployed in quantity to sense the physical world. Sensor nodes are essentially small computers with extremely basic functionality. They consist of a processing unit with limited computational power and a limited memory, a radio communication device, a power source and one or more sensors. Motes come in different sizes and shapes, depending on their foreseen use. They can be very small, if they are to be deployed in big numbers and need to have little visual impact. They can have a rechargeable battery power source if they are to be used in a lab. The integration of these tiny, ubiquitous electronic devices in the most diverse scenarios ensures a wide range of

applications. Some of the application areas are environmental monitoring, agriculture, health and security. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. These networks provide a bridge between the physical world and the virtual world. They promise unprecedented abilities to observe and understand large scale, real-world phenomena at a fine spatial-temporal resolution. This is so because one deploys sensor nodes in large numbers directly in the field, where the experiments take place. All motes are composed of five main elements as shown below:

1. Processor: the task of this unit is to process locally sensed information and information sensed by other devices. At present the processors are limited in terms of computational power, but given Moore's law, future devices will come in smaller sizes, will be more powerful and consume less energy. The processor can run in different modes: sleep is used most of the time to save power, idle is used when data can arrive from other motes, and active is used when data is sensed or sent to / received from other motes.

2. Power source: motes are meant to be deployed in various environments, including remote and hostile regions so they must use little power. Sensor nodes typically have little energy storage, so networking protocols must emphasize power conservation. They also must have built-in mechanisms that allow the end user the option of prolonging network lifetime at the cost of lower throughput. Sensor nodes may be equipped with effective power scavenging methods, such as solar cells, so they may be left unattended for months, or years. Common sources of power are rechargeable batteries, solar panels and capacitors.

3. Memory: it is used to store both programs (instructions executed by the processor) and data (raw and processed sensor measurements).

4. Radio: WSN devices include a low-rate, short-range wireless radio. Typical rates are 10-100 kbps, and range is less than 100 meters. Radio communication is often the most power-intensive omust incorporate energy-efficient techniques such as wake-up modes. Sophisticated algorithms and protocols are employed to address the issues of lifetime maximization, robustness and fault tolerance.

5. Sensors: sensor networks may consist of many different types of sensors capable of monitoring a wide variety of ambient conditions. Table 1 classifies the three main categories of sensors based on field-readiness and scalability. While scalability reveals if the sensors are small and inexpensive enough to scale up to many distributed systems, the field-readiness describes the sensor's engineering efficiency with relation to field deployment. In terms of the engineering efficiency, Table1 reveals high field-readiness for most physical sensors and for a few numbers of chemical sensors while most chemical sensors lie in the medium and low levels and biological sensors have low field-readiness.

Sensor Category	Parameter	Field-Readiness	Scalability
Physical	Temperature	High	High
	Moisture Content	High	High
	Flow rate,Flow velocity	High	Med-High
	Pressure	High	High
	Light Transmission (Turb)	High	High
Chemical	Dissolved Oxygen	High	High
	Electrical Conductivity	High	High
	pH	High	High
	Oxydation Reduction Potential	Medium	High
	Major Ionic Species (Cl-, Na+)	Low-Medium	High
	Nutrientsa (Nitrate, Ammonium)	Low-Medium	Low-High
	Heavy metals	Low	Low
	Small Organic Compounds	Low	Low
	Large Organic Compounds	Low	Low
Biological	Microorganisms	Low	Low
	Biologically active contaminants	Low	Low

Common applications include the sensing of temperature, humidity, light, pressure, noise levels, acceleration, soil moisture, etc. Due to bandwidth and power constraints, devices primarily support low-data-units with limited computational power and a limited rate sensing. Some applications require multi-mode sensing, so each device may have several sensors on board.

Following is a short description of the technical characteristics of WSNs that make this technology attractive.

1. **Wireless Networking**: motes communicate with each other via radio in order to exchange and process data collected by their sensing unit. In some cases, nodes can use other nodes as relays, in which case the network is said to be multi-hop. If nodes communicate only directly with each other or with the gateway, the network is said to be single-hop. Wireless connectivity allow to retrieve data in real-time from locations that are difficult to access. It also makes the monitoring system less intrusive in places where wires would disturb the normal operation of the environment to monitor. It reduces the costs of installation: it has been estimated that wireless technology could eliminate up to 80 % of this cost.
2. **Self-organization**: motes organize themselves into an ad-hoc network, which means they do not need any pre-existing infrastructure. In WSNs, each mote is programmed to run a discovery of its neighborhood, to recognize which are the nodes that it can hear and talk to over its radio. The capacity of organizing spontaneously in a network makes them easy to deploy, expand and maintain, as well as resilient to the failure of individual points.
3. **Low-power**: WSNs can be installed in remote locations where power sources are not available. They must therefore rely on power given by batteries or obtained by energy harvesting techniques such as solar panels. In order to run for several months of years, motes must use low-power radios and processors and implement power efficient schemes. The processor must go to sleep mode as long as possible, and the Medium-Access layer must be designed accordingly. Thanks to these techniques, WSNs allow for long-lasting deployments in remote locations.

1.3. Applications

The integration of these tiny, ubiquitous electronic devices in the most diverse scenarios ensures a wide range of applications. Some of the most common application areas are environmental monitoring, agriculture, health and security. In a typical application, a WSN is scatteEnvironmental monitoring applications of WSN include:

1. Tracking the movement of animals. A large sensor network has been deployed to study the effect of micro climate factors in habitat selection of sea birds on Great Duck Island in Maine, USA. Researchers placed their sensors in burrows and used heat to detect the presence of nesting birds, providing invaluable data to biological researchers. The deployment was heterogeneous in that it employed burrow nodes and weather nodes.
2. Forest fire detection. Since sensor nodes can be strategically deployed in a forest, sensor nodes can relay the exact origin of the fire to the end users before the fire is spread

uncontrollable. Researchers from the University of California, Berkeley, demonstrated the feasibility of sensor network technology in a fire environment with their FireBug application.

3. Flood detection. An example is the ALERT system deployed in the US. It uses sensors that detect rainfall, water level and weather conditions. These sensors supply information to a centralized database system.
4. Geophysical research. A group of researchers from Harvard deployed a sensor network on an active volcano in South America to monitor seismic activity and similar conditions related to volcanic eruptions.
5. Agricultural applications of WSN include precision agriculture and monitoring conditions that affect crops and livestock. Many of the problems in managing farms to maximize production while achieving environmental goals can only be solved with appropriate data. WSN can also be used in retail control, particularly in goods that require being maintained under controlled conditions (temperature, humidity,light, etc).
6. An application of WSN in security is predictive maintenance. BP's Loch Rannoch project developed a commercial system to be used in refineries. This system monitors critical rotating machinery to evaluate operation conditions and report when wear and tear is detected. Thus one can understand how a machine is wearing and perform predictive maintenance. Sensor networks can be used to detect chemical agents in the air and water. They can also help to identify the type, concentration and location of pollutants.
7. An example of the use of WSN in health applications is the Bi-Fi, embedded system architecture for patient monitoring in hospitals and out-patient care. It has been conceived at UCLA and is based on the SunSPOT architecture by Sun. The motes measure high-rate biological data such as neural signals, pulse oximetry and electrocardiographs. The data is then interpreted, filtered, and transmitted by the motes to enable early warnings.

1.4. Roles in a WSN

Nodes in a WSN can play different roles.

1. Sensor nodes are used to sense their surroundings and transmit the sensor readings to a sink node also called "base station". They are typically equipped with different kinds of sensors. A mote is endowed with on-board processing, communication capabilities and sensing capabilities.
2. Sink nodes also referred to as "base stations" are tasked to collect the sensor readings of the other nodes and pass these readings to a gateway to which they are directly connected for further processing/analysis. A sink node is endowed with minimal on-board processing and communication capabilities but with no sensing capabilities.

3. Actuators are devices which are used to control the environment, based on triggers revealed by the sensor readings collected in the environment. An actuator may have the same configuration as a mote but is also endowed with controlling capabilities: e.g switch a light on under low luminosity.

Gateways often connected to sink nodes are high energy devices usually connected to a stable power supply. These devices are normal computing devices such as laptops, notebooks, desktops, mobile phones or other emerging devices which are able to store, process and route the sensor readings to processing place. However, they may not be endowed with sensing capabilities. Being range-limited, sensor motes require multi-hop communication capabilities enabling 1) spanning distances much larger than the transmission range of a single node through localized communication between neighbor nodes 2) adaptation to network changes, for example, by routing around a failed node using a different path in order to improve performance and 3) using less transmitter power as a result of the shorter distance transmission mode enabled by the potential to achieve localized communication. They are deployed in three forms : (1) Sensor node used to sense the environment (2) Relay node used as relay for the sensor readings received from other nodes and (3) Sink node also often called base station which is connected to a gateway (laptop, iPad, iPod, Smart phone, desktop) with higher energy capable of either processing the sensor readings locally or to transmit these readings to remote processing places.

2. References.

[1] Ovidiu Vermesan & Peter Fress, “Internet of Things –From Research and Innovation to Market Deployment”, River Publishers Series in Communication, ISBN: 87-93102-94-1, 2014.