APPLICATIONS AND OPEN ISSUES OF INTERNET OF THINGS: A BRIEF OVERVIEW

JINGHUA DING, NAVRATI SAXENA

1,2College of Information & Communication engineering Sungkyunkwan University, Suwon, Korea
E-mail: jhding@skku.edu, navrati@skku.edu

Abstract- In this paper, the Internet of Things (IoT) is discussed from many perspectives. Primarily, several challenging issues are to be addressed urgently to exploit the full functioning of the internet system. Internet of Things (IoT) possesses several problems concerning network and resource. In terms of both energy capacity and computational power, the resources are utilized ineffectively. From academic to industry field, few researchers and experiments are conducted to resolve these negative and future issues so as to develop the standardization. Therefore, the main objective of this paper is to present IoT-related knowledge. In addition, the in-depth future developments of IoT concerning various protocols, algorithms and proposed solution for the open issues in IoT are also provided. Furthermore, risk factors and the drawbacks involved in IoT are reviewed in this paper, and the possible issues remain to be addressed are suggested.

Keywords- Internet of Things, Wireless Sensor Networks, Machine to machine.

I. INTRODUCTION

The term “Internet of Things” was first proposed by Kevin Ashton. He commented that “Today, computers, and the Internet are almost wholly relied on by human beings for acquiring information”. With the coming centuries, people are becoming busier, leaving limited time and energy to pay attention to the accuracy of things happening in real world. So they turn to the Internet. Almost in all of the organizations, information travels along the familiar paths, namely, wired and wireless networks, which are used to connect actuators and objects embedded in the physical objects. But with time slipping by the predictable routes changes. And the physical world is becoming a kind of information system. Though the spreading of internet of things all over the world takes time, data in the internet is increasing, as well as the reliance of people on their the data due to the fast advancement in underlying technologies.

With the advancement and standardization of the wireless communication networking, it is possible for sensors to collect data almost anywhere at any time. Though it is still not adopted and deployed by many companies. It is however expected the range of its subsequent deployment will increase with the advancement and maturity. Considering above importance, it is surprising that IoT is included by the US National Intelligence Council in the list of six “Disruptive Civil technologies” with potential impacts on US national power.

Multiple definitions of Internet of Things (IoT) can be found in the research community, which has attracted strong attention and led to heated debates in the public. The debates are constituted of two categories: the first one proposes a vision that IoT is network-based, while the second term lays particular stress on general “objects” which are regarded as parts of a general framework. As a matter of fact, semantically speaking, “Internet of Things” means “a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols”. It is implied that a large number of (heterogeneous) objects are brought into this process. The unique addressing and the representation of the object and the storage of exchanged information become the most challenging issues, directly leading to a third perspective of IoT—“Semantic oriented”. As shown in Fig.1, standards and technologies of IoT can be classified and emphasized in accordance with the leading concepts - IoT vision, and they are conducive to the optimal characterization. It is obviously shown by the illustration that IoT paradigm is the combination of the aforesaid visions.

II. EMPOWER TECHNOLOGIES

In this section, a picture of the role that the technologies will play in the IoT will be provided briefly rather than investigate each technology comprehensively.
The standardization activity of IoT enabling the integration of devices in the internet is reviewed briefly. Furthermore, various issues related to the addressing and networking part and the challenges concerning security and privacy issues are also discussed in detail.

2.1. Applications
With the rise of the internet revolution, the worlds of network users are heading towards a ubiquitous network society. Today we are standing on the plateau of digital era. There are a lot of fields in which we use or are dependent on the networking things. In the aspect of our daily life, we come across new environment and new applications. Along with objects which work using network intelligence, it would be more helpful if we could also make the non-digital objects equipped with communication capabilities. In all applications, the mobile phone is the primary means for providing the window to things-specific content and services that run on the web. For this and other reasons (simplicity, mobility, computing power, sensor richness, security level, network infrastructure, adoption rate, etc.), many believe that the mobile phone is bound to be the mass computer of the future.

If we could make our TV and refrigerator smarter, giving us updates about the contents. Perishable food items such as fruits, ready-cut vegetables, meat and dairy products are vital part of our body nutrition. The quality and the quantity need to be monitored to avoid uncertainty with respect to the conservation status. Smart TV multi-channel capabilities help to fulfill demands of various members according to their preferences.

2.1.1. Residential Domain
Slowly the analog homes are walking towards futuristic digital homes. Today our houses are equipped with several digital devices like sensors and actuators. We need them to make our day to day life more comfortable. Think how good it would be if our home adjusts everything by itself according to the weather or our needs. How good it would be if it reminds us of switching on or off the electrical and heating appliances. The power grids authorities are trying to involve the consumers by using pricing policy. This not only saves energy, also plays an active part to fight back power failure by shifting peak load period. Automatic time set in some devices like rice cooker, microwave and electric fans saves energy and time, which is as precious as money for a busy scheduler.

For the manufacturing of complete products, the raw materials have to be processed through a series of processes. To make quality product according to the manufacturer want, there should be a good coordination among the different machines and devices. Goods are manufactured in quantities, so there is need for more communication among the machines. Day by day we are reducing the manual involvement to avoid accidents and save time. So this puts a pressure to have staff working so as to have a well-functioning production system.

2.1.2. Industrial Domain
A smart industrial environment helps us in improving the industrial plants with a massive deployment of wireless sensors and RFID tags. Industries must become electricity-smart and water-smart. To develop and modernize the technical basis and enable smart manufacturing system we need to evolve towards using the full spectrum of actionable energy information models, data representation methods and cyber security requirements. The machine mounted with wireless sensor monitors the vibration and keeps record of the device status. This helps to quality control and improving the lifetime of the machines. In case of emergency, the robots help to shut down the operation.

For the manufacturing of complete products, the raw materials have to be processed through a series of processes. To make quality product according to the manufacturer want, there should be a good coordination among the different machines and devices. Goods are manufactured in quantities, so there is need for more communication among the machines. Day by day we are reducing the manual involvement to avoid accidents and save time. So this puts a pressure to have staff working so as to have a well-functioning production system.
a smarter way by automatically switching off the electrical appliances when not needed.

2.1.4. Transportation Domain
Deploying the roads and trails along with the vehicles with actuators, sensors and processing power may help to exchange information between the driver and passenger for safety and better navigation. These would help to avoid accidents and collision. The drivers can avoid traffic jam and find the right path using wireless navigation system. Also with respect to vehicles carrying goods, the companies can have updated information about its movement along with the status of goods that it is carrying and the delivery time and delays. Having accurate information about the number and kind of vehicles, busy hours and non-busy hours would help government bodies to plan accordingly to the need for the future.

2.1.5. Healthcare domain
1. Diagnosing, treatment and prevention of disease: Network access to healthcare varies depending on the countries and its people, also largely influenced by its economic condition and social status.

A well-functioning healthcare system requires well maintained facilities, reliable information exchange and logistics to deliver quality service to the people. Today’s health care includes different types of medical equipment, instrumental applications and services providing real-time information on patient health indicators. As well as, diagnostic laboratories substances, biotechnology and drug manufacturing and delivery. 2. Identification and authentication: This paradigm refers to patients' identification, his illness records to avoid wrong treatment and harmful incidents such as overdose, improper medication timing and procedure. To identify infants, youth and old patients and also to authenticate the hospital staff improvement of employee morale is done by addressing patient safety issues. 3.

Health care management: Health systems management or health care systems management describes the leadership and general management of hospital, hospital networks and/or healthcare systems. There is widespread rising of problems in the health systems related to balancing the cost issue, access, standard of service and quality of the hospitals.

The solution demands a well-functioning health management system in all the levels. Communication among all levels should be reliable, secure and fast. IoT provides many benefits to this sector like reducing processing time, automatic care and medical inventory management.

2.1.6. Smart Entertainment Domain
In present day’s hectic life, it’s very difficult to find some time for leisure and entertainment. We can take help of IoT technologies to fully utilize our precious time but also be fully entertained. Having a smart gym center in the office premises or near our residence would keep us relaxed and active with just some short breaks. Also the trainer can upload instruction files and videos needed for the trainee or a beginner into the individual training machine, helping it to automatically recognize the person. Also the trainer can keep data and records about the trainee workout whether he is overdoing it, or doing it the wrong way. Smart museum, theatre, water resort, amusement parks and resort are other examples where the IoT technologies can be deployed to enhance the entertainment and security of both the entertainer and the audience. The people can take advantage of the highly advanced networking system to exploit their facilities to the best.

2.1.7. Smart Entertainment Domain
In present day’s hectic life, it’s very difficult to find some time for leisure and entertainment. We can take help of IoT technologies to fully utilize our precious time but also be fully entertained. Having a smart gym center in the office premises or near our residence would keep us relaxed and active with just some short breaks. Also the trainer can upload instruction files and videos needed for the trainee or a beginner into the individual training machine, helping it to automatically recognize the person. Also the trainer can keep data and records about the trainee workout whether he is overdoing it, or doing it the wrong way. Smart museum, theatre, water resort, amusement parks and resort are other examples where the IoT technologies can be deployed to enhance the entertainment and security of both the entertainer and the audience. The people can take advantage of the highly advanced networking system to exploit their facilities to the best.

III. OPEN PROBLEMS

This section briefly reviews the standardization activity of IoT enabling the integration of devices in the internet. Furthermore various issues related to the addressing and networking part and the challenges concerning security and privacy issues are also discussed in detail.

3.1 Standardization
The unification of several embedded devices and the internet reveals numerous unexpected challenges to be addressed. Since most of these devices cannot fit in the existing internet technologies and protocols well, it's time to upgrade the internet system according to the requirement. Most of these attempts and efforts just focuses on the networking layer: IETF routing over low-power and lossy networks IPv6 over Low-Power Wireless Personal Area Networks (RFC 4919), Transmission of IPv6 Packets over IEEE 802.15.4 Networks (RFC4944) [6] are a few mentioned.
To exploit and understand all great opportunities that the IoT can provide us, an embedded counterpart of the web technology is needed. As a driving force for the successful deployment of the sensor network, these technologies are able to connect with IPv6 Internet and use the embedded web service technology to build applications.

However, RFID technology is being slowed down recently by shattered attempts towards the standardization of principal areas like RFID frequency and tags-reader communication protocols, labels and data formats placed on tags, which is mainly researched by standard bodies of EPCglobal, ISO and ETSI. Among them, EPC global is a nonprofit standard organization GS1.

### 3.2 Addressing and Networking issues:

In context of internet of things a lot of devices are incorporated with the network and these devices are applying different technologies. As for the convergence of Information and communication technology, they can be achieved through internet homogeneity. That is to say, one is asked to identify the different equipment so as to run the whole system smoothly. Thus, some effective addressing schemes should be designed. In this vast network the identifiers for different classes of devices need to be defined. IPv6 addressing scheme expressed by 128 bits was suggested for low power wireless communication nodes. That will be enough to define 1038 addresses, 64-96 bits identifiers are used for RFID tags, so some techniques to integrate RFID tags into IPv6 networks must be thought. The authors in investigated on RFID tags integration into IPv6 networks. 64 bits are used for RFID identifiers and other 64 bits for the gateway between the RFID system and the internet. In another article the authors suggest a mapping between the native addressing of each technology and an IPv6 address depending on a set of rules.

Another scheme is proposed using a network element called agent. The agent maps the RFID identifier into a 64 bits field. Which will be used as the interface ID of the IPv6 addresses. The agent keeps the mapping updated between the IPv6 addresses generated and the RFID tag identifier. But it’s to be noted that in all these above cases RFID mobility is not carried out. Rather RFID can be attained by the gateway between RFID system and the network. Now to support RFID mobility in IoT atmosphere several solutions have been proposed in. The scalability and the adaptability rate have to be checked to be sure for their success in the IoT scenarios. Higher scalability can be achieved based on the implementation of a home agent like Mobile IP.

Traffic characteristics are also important issues concerning the networking aspects. A large number of data generated is traversing through internet and has different traffic characteristics due to heterogeneity. Also the knowledge of traffic characteristics is important for the infrastructure planning by the network providers. Thus to provide quality of service (QoS) the knowledge of modeling and the knowledge of traffic characteristics and traffic requirements are needed.

### 3.3 Security and Privacy

The IoT is easy to be attacked for the following reasons: firstly, the unwatched components are easy to be attacked; secondly, the wireless communication is easily wiretapped; finally, the IoT components are mostly inferior in energy and computing resources; especially the passive components. Therefore, it is impossible for them to perform complicated procedures for supporting security.

Even more particularly, authentication and the integrity of data are the main problems relevant to security. It is hard for authentication because it needs proper servers and authentication infrastructures which achieve their objective by exchanging proper messages with other nodes. As passive RFID tags cannot exchange too many messages with the authentication servers, such approaches are impracticable in the IoT. The same is true for the sensor nodes.

In this context, note that several solutions have been proposed for sensor networks in the recent past. Nevertheless, if sensor nodes are regarded as part of a sensor network linked to the rest of the Internet by means of some nodes as gateways, existing solutions can be implemented. On the contrary, it is a must to take sensor nodes as nodes of the Internet so that authenticating them from nodes belonging to another sensor network becomes necessary.

Recently, there are several solutions raised for RFID systems which all have critical problems as represented in . The last point, all the existing solutions are fail to help in solving the proxy attack problem, also called the man-in-the-middle attack.

Sensor networks as well. For instance, the read and write operations are protected by both EPC Global Class-1 Generation-2 and ISO/IEC 18000–3 tags on their memory with a password. Actually, there are five areas of memory in the EPC Global Class-1 Generation-2 tags. With a specific password independently, each of them can be protected in read or write. However, by defining a pointer to a memory address, ISO/18000–3 tags protect all memory areas with a lower memory address and a password. Messages may be protected based on the Keyed-Hash Message Authentication Code (HMAC) scheme in order to avoid the second kind of attack, which is relying on a common secret key shared between the destination of the message and the tag for combining with a hash function for authentication.
If RFID systems are thought to have serious problems, the said solutions will be put forward to support data integrity. Actually, the length of password supported by most tag technologies is not long enough for strong protections. In addition, the management is still a challenging task in spite of supported by longer passwords, especially when entities belonging to different organizations are involved, as in the case of the IoT.

In the end, it should be noticed that all the above solutions for supporting security adopt several cryptographic methodologies. Large amount of resources concerning energy and bandwidth both at the source and the destination are spent by energy and bandwidth both at the source and the destination. As elements like RFID tags and sensor nodes are seriously limited on energy, communications, and computation capabilities, the above solutions are not feasible for IoT. The required new solutions shall be able to offer a favorable level of security in spite of the resources shortage. From this point of view, there have been some solutions put forward for light symmetric key cryptographic schemes (see for RFID scenarios and for sensor network scenarios). Key management schemes, however, are still in the startup phase, especially in the case of RFID, and a lot of efforts shall be spent on.

Privacy, which is recognized in all legislations of civilized countries, has also become an important part of our civilization. And the diffusion of IoT-involved technologies is a hidden danger. Data collection, mining, and provisioning in IoT are accomplished in the ways completely different from what we know now. Personal data can be collected in innumerable occasions. Consequently, people are unable to control the disclosure of their personal information personally.

As digital forgetting has only become a key issue recently, studies on it are still immature. For example, though some experimental solutions have been developed and released for public use recently, with which users can insert and share pictures and other types of files via the Internet, these pictures will definitely expire at a time and be deleted afterwards (see drop.io and the Guest Pass features on Flicker for example). If such solutions are to be ported to the IoT context, more efforts are required, which remains to be an open challenge.

CONCLUSION

The development of internet has upgraded the interactions between people in real life to a virtual level in several spheres from professional life to societal life. For this the IoT is considered as the overall future of the internet. The current internet paradigm usually focused on host–to-host communication limits the full exploitation of the current internet. Today internet is being mostly used for communication and exchange of information and therefore, information should be the focus of communication and networking solutions, thus leading to the concept of data-centric networks, which has been investigated only recently. In this paper we have gone through and surveyed various and most important aspects of internet of things. Present technologies made the internet of things feasible and advanced but still it doesn’t fit in the requirements to be faced in future well. We have emphasized on how today’s internet is working and what are the future issues to be researched further.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology project Number: S-2013-1002-000

REFERENCES

Applications and Open Issues of Internet of Things: A Brief Overview

41