Course: Internet of Things - 521043S
Home Exam

Tri Hong Nguyen

May 2019

1 Internet of Things (IoT)

Internet of Thing (IoT) is a keyword for a variety of fields mentioning a way to extend or develop the Internet through physical realm [1]. In this section, a general discussion is about IoT based on its concepts, challenges and technologies.

1.1 Key Concepts

The term "Internet of Thing" has been much well-known recently; however, it also raises the manifold definition of this term. Following [1], the concept of IoT includes three pillars which are identification, communication and interaction of smart objects. Similarly, [2] showed three main orientations of IoT.

- **Thing oriented:** this perspective is the definition of IoT derives through the Auto-ID labs [2] (the thing indicates to simple items with Radio-Frequency IDentification (RFID) tags). These Auto-ID institutes have targeted to the architecture of IoT as primary development of Electronic Product Code (EPC) in order to help the spread of RFID and standards which enhance the object visibility for EPC global network. However, RFID is just only a part of the IoT story. IoT also can be a place for Ubiquitous IDentifier (uID) architecture whose idea is to develop solutions for global visibility of objects [3]. In addition, connectivity technologies are the other components of IoT supporting links in the digital world. Another thing then focused in the term "Thing oriented" is about the *spime*. It is to indicate objects which can be tracked through space and time with sustainability and enhancement [4].

- **Internet oriented:** as a part from IoT, the "Internet oriented" vision plays a role of trait d'union among "thing oriented"[2]. Its main vision hence is about simplicity in promoting Internet Protocol for connection between smart objects through the IP for Smart Object (IPSO) [5] and Internet $\emptyset$ [6].

- **Semantic oriented:** the idea is to exploit solutions for several problems inside IoT. In more details, semantic technologies can solve things description, reasoning over data from IoT, execution environment and also the architecture of IoT requirements for storage and communication [2].

1.2 Challenges

Following [2], it can be seen open issues of IoT based on three main categorizes standardization activity, issues related to networking, security and privacy. In more detail, these issues can be listed as below [2]:

- Standards mobility support as a part of standardization activity is a problem which is hard to integrate between different frameworks into a comprehensive one. Hence, the scalability and adaptability of IoT can be important problems due to heterogeneous technologies.
- Naming Object Name Servers (ONS) is another issue which is about description or identification of objects.
- Transport protocol is a challenge of IoT systems due to many reasons including excessive buffering, and the useless existing transport protocol from connection setup and congestion control mechanism.
- Traffic characterization and QoS support can become other issues in IoT scenarios due to new QoS requirements and data traffic with different patterns from the current Internet.
- Authentication is a problem from IoT scenarios since current authentication infrastructures are not satisfied with the IoT view. Another issue related to authentication can be a man-in-the-middle attack.
- Data integrity is protected by passwords; however, the level of this protection depends on the length of the password which is short in IoT devices.
- Privacy is the main problem in the IoT field because many private and sensitive information about anyone can be collected and stored without awareness of these people. With data storage collected with IoT devices, several other techniques used with machine learning or data mining can retrieve useful information and obtain benefits.

1.3 Technologies and Protocols

In term of technologies and protocols related to IoT scenarios, [2] mentioned two main groups identification, sensing and communication technologies and middleware.

- Identification, sensing and communication technologies: in term of communication, wireless technologies have played the key role. Moreover, RFID systems including readers and RFID tags are key parts of IoT to monitor objects for connection between the real world and virtual world with standard ISO18000. To cooperate between RFID systems, sensor networks can be a role for this task to obtain a general status of information. In more detail, solutions for wireless sensor network are based on IEEE 802.15.4. The last technology in this term is sensing RFID systems for building an RFID sensor network [2].

- Middleware is a software layer which is placed between technology and application levels. This layer becomes important day by day because of the development of services and integration of legacy technologies [2]. With the idea based on Service Oriented Architecture (SOA), complex and monolithic systems can be decomposed into simple ecosystem based on well-defined components.

2 Web of Things (WoT)

With the development of IoT, Web of Things (WoT) is a trend from this growth. The main idea of WoT is the use of web standards for sharing and communicating information between different devices. Through WoT, smart things can enhance the physical world and reduce the gap between the virtual and real worlds.

2.1 Key Concepts

[7] indicated that smart objects can act as web servers which provides service through the web. With this perspective, there are two matters which can be considered: a way to use the web from the physical thing and exchange of information from physical objects through web services.

- Integrating Smart Things to the Web: there are two approaches to integrate smart objects to the web (direction and indirection). To directly integrate objects to the web, there is the main requirement that is the IP address for these objects to connect to the Internet. With this requirement, web servers can be embedded into these devices, which helps the connection through web standards as GET and POST operations. However, there are other solutions for direct integration of smart objects in the web such as web API [8], web services [9] and HTTP protocol [10]. In turn of indirect integration, because of the limitation and need of several devices using the web, indirect integration is a general idea in this case with a user of intermediate proxy playing between smart things and the web.

- Web service paradigms: there is a question which is to abstract smart things through reusable web services. REST-compliant web services and arbitrary web services[1] are two main paradigms of web services, which aims to control and manage web resources based on stateless operations.

2.2 Challenges

In this subsection, a list of challenges in WoT is generally mentioned through Zeng et al. consideration [7].

- Heterogeneity and scalability: since smart devices use various methods in communications, computation, storage and so on, heterogeneity of device level is a challenge of WoT without a suitable way to fit all devices. In addition, the difference between types of data from data processing and the way to consume data can require bandwidth, latency and reliability.

[1] http://www.w3.org/TR/ws-arch/

- Security and Privacy: it cannot be deniable the openness and sharing resources can lead to privacy and security issues. Due to the trade-off between these issues and scalability, it is really hard to find a suitable approach to adapt to both requirements.
- Search and Discovery: in the WoT world, there is a requirement of discovering existing objects. [11] indicated two general search engines (push and pull); nevertheless, these search engines need to consider a trade-off between scalability and accuracy.
- Ambient Intelligence: due to the web services which should be responsive to the interaction of users and condition of the environment, Ambient Intelligence (AmI) is proposed to address stand-alone systems; however, with AmI, WoT's scalability and heterogeneity can be affected. In addition, some AmI applications require to discover web services and adapt users' requirements.

2.3 Technologies and Protocols

From [7] consideration, there have been many studies related to the communication between smart objects. However, as a trend of interaction in smart things through the web environment, web servers can be built in devices to utilize benefits including the flexible, open, free, and scalable web.

- 6LoWPAN: to become as a web server, the devices should have their own address, which leads to the propose of IPv6-based network from IETF with a project named IPv6 over Low Power Wireless Personal Area Network (6LoWPAN). This project aims to define an encapsulation and header supporting communication between devices.
- CoAP: there is a framework supporting the use of applications with various resources through constrained networks. This framework utilizes a Constrained Application Protocol (CoAP) which can be viewed as HTTP protocol in the traditional network.
- Embedded Web Server: the use of embedded web servers supports the transmission between smart objects through web language; however, it is noticed a requirement of the simple and small process from these web servers. There are several ideas through embedded internet devices and embedded web server-based home appliance using HTTP and Ethernut-based web servers, respectively [12, 13].
- Service Composition Development: following [7], smart objects should combine with each other in order to explore their potential. Nevertheless, it is hard to integrate objects because of different manufacturers. With the idea [8], there are two mashup styles (physical-virtual and physical-physical) to embedded devices and present through Web 3.0.

3 Machine to Machine communication (M2M)

The machine to machine (M2M) communication is novel technology as the next generation of communication system [14]. It helps connection and communication between intelligent devices to form several applications such as e-healthcare, home area network and so on.

3.1 Key Concepts

The M2M communication between devices includes three interlinked domains (M2M device domain, network domain and application domain) [14].

- M2M device domain: a large number of devices and gateways form an M2M network to transmit their data to each other. After exchanging data, these devices together generate "intelligent decisioins" to send data to gateway, while gateway as a "intelligent device" receives and sends data in optimal ways based on multi-hop or single-hop channels.
- Network domain: this is a domain as an intermediate layer placed between M2M and application domains. This domain utilizes long-range wired/wireless network protocols for efficient and reliable channels.
- Application domain: in term of the application domain, a back-end server and M2M application clients are placed in this domain. This domain is considered as an integration point to contain information in the M2M device domain with other features.

3.2 Challenges

There are several challenges indicated by [14] including energy efficiency, security, reliability, and so on.

- Energy efficiency: it is clear that in M2M device and application domains there are several battery-powered devices. Therefore, a long time use without charging or replacement can be a challenge. Otherwise, the collected data can be wrong in some cases.
- Reliability: due to wireless channels in M2M communications are not reliable with noise or large traffic. To improve this matter, [15] indicated to exploit redundancy technologies.
- Security: it is clear that a way to secure communicative channels is an issue in M2M communications; however, to improve the security, it becomes trouble because of the communication between heterogeneous devices in the network.
- Ultra-scalable connectivity: to reduce the amount of energy consumption, a scalable network is an issue. [16] proposed a solution as hierarchical architecture which allows M2M devices directly connect to WAN connection or indirectly to an M2M gateway.
- Device heterogeneity: due to a large number of heterogeneous objects, it raises many matters in communication such as scalability and security. To solve this problem, [17] mentioned to the future wireless communication systems with more secure, energy-efficient and so on.

- Spectrum management: the purpose of spectrum management is about optimization of spectrum resources based on time, bandwidth, dimension and frequency. With the efficiency of spectrum management, the network can efficiently consume energy. To resolve this issue, [18] proposed a CM2M architecture in the smart grid to obtain the spectrum efficiency.

- Quality-of-Service (QoS): since there is latency in data transmission, the QOS can be degraded. However, in some special cases or applications, the latency can raise many problems. Hence, the QOS is required to guarantee, which can be solved by the improvement of network capacity and transmission range from M2M devices.

- Intermittent connectivity: the problem with intermittent connectivity is also based on the heterogeneous device communication. In this issue, there are hard and soft intermittent connectivities related to the mobility of a node and unavailability of a node in turn.

3.3 Technologies and Protocols

Due to other communication technologies, M2M communication includes ZigBee-like and 2G/3G/4G mobile network, but recently with the requirement of low power/energy consumption, there are several other uses of low-power wifi and Bluetooth low energy [19].

- ZigBee-like technologies: IEEE 802.15.4 and its derivatives (ZigBee, WirelessHART, etc.) have played a crucial role in M2M communication. It provides an energy-efficient technology in a short distance with a high data rate; however, in the case of M2M communication, it requires a long distance connection. Therefore, the use of repeaters is considered to connectivity.

- Low-power Wi-Fi: the main feature of general Wi-Fi is a huge popularity of devices. A good point of this technology is about less energy in the transmission of data due to the utilization of single-hop channel. In comparison with ZigBee-like, low-power Wi-Fi consumes less energy than since ZigBee-like requires an amount of energy when listening transmission of data from neighbors.

- Proprietary cellular: this is the most important technology for M2M communication due to a large coverage for M2M devices. Nevertheless, this technology with 2G, 3G and LTE is slow standardization cycle. In addition, the high costs of license and narrowband are other issues of this technology.

- Standardized cellular: it cannot be deniable the importance of cellular networks in M2M communications. With standardized cellular M2M technologies, M2M devices can roam and move with connectivity. In addition, a consideration based on radio resource management (RRM) can be used to guarantee the latency or throughput problems.

Acknowledgement

I would like to express my sincere gratitude to Dr. Ella Peltonen, MSc. Rouhollah Ehsani, and MSc. Kennedy Opoku Asare through lectures and exercises in the course "Internet of Things" at the University of Oulu.

In addition, I wrote down my comments as feedback to improve the course for the next turn.

References

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad hoc networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[3] K. Sakamura, "Challenges in the age of ubiquitous computing: a case study of t-engine, an open development platform for embedded systems," in *Proceedings of the 28th international conference on Software engineering*, pp. 713–720, ACM, 2006.

[4] B. Sterling, "Shaping things (mediaworks pamphlets)," 2005.

[5] A. Dunkels and J. Vasseur, "Ip for smart objects, internet protocol for smart objects (ipso) alliance, white paper# 1, september 2008."

[6] N. Gershenfeld, R. Krikorian, and D. Cohen, "The internet of things," *Scientific American*, vol. 291, no. 4, pp. 76–81, 2004.

[7] D. Zeng, S. Guo, and Z. Cheng, "The web of things: A survey," *JCM*, vol. 6, no. 6, pp. 424–438, 2011.

[8] D. Guinard and V. Trifa, "Towards the web of things: Web mashups for embedded devices," in *Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), in proceedings of WWW (International World Wide Web Conferences), Madrid, Spain*, vol. 15, 2009.

[9] O. Akribopoulos, I. Chatzigiannakis, C. Koninis, and E. Theodoridis, "A web services-oriented architecture for integrating small programmable objects in the web of things," in *2010 Developments in E-systems Engineering*, pp. 70–75, IEEE, 2010.

[10] B. Ostermaier, M. Kovatsch, and S. Santini, "Connecting things to the web using programmable low-power wifi modules," in *Proceedings of the Second International Workshop on Web of Things*, p. 2, ACM, 2011.

[11] B. Ostermaier, K. Römer, F. Mattern, M. Fahrmair, and W. Kellerer, "A real-time search engine for the web of things," in *2010 Internet of Things (IOT)*, pp. 1–8, IEEE, 2010.

[12] A. Wilson, "The challenge of embedded internet design," *Real-Time Magazine*, no. 1, pp. 78–80, 1998.

[13] M. C. Filibeli, O. Ozkasap, and M. R. Civanlar, "Embedded web server-based home appliance networks," *Journal of Network and Computer Applications*, vol. 30, no. 2, pp. 499–514, 2007.

[14] P. K. Verma, R. Verma, A. Prakash, A. Agrawal, K. Naik, R. Tripathi, M. Alsabaan, T. Khalifa, T. Abdelkader, and A. Abogharaf, "Machine-to-machine (m2m) communications: A survey," *Journal of Network and Computer Applications*, vol. 66, pp. 83–105, 2016.

[15] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "Grs: The green, reliability, and security of emerging machine to machine communications," *IEEE communications magazine*, vol. 49, no. 4, pp. 28–35, 2011.

[16] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2m: From mobile to embedded internet," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 36–43, 2011.

[17] J. Zhang, L. Shan, H. Hu, and Y. Yang, "Mobile cellular networks and wireless sensor networks: toward convergence," *IEEE Communications Magazine*, vol. 50, no. 3, pp. 164–169, 2012.

[18] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: Visions and potentials for the smart grid," *IEEE network*, vol. 26, no. 3, pp. 6–13, 2012.

[19] C. Anton-Haro and M. Dohler, *Machine-to-machine (M2M) communications: architecture, performance and applications*. Elsevier, 2014.