The Internet of Things: A Survey

Jing Zhang*

Melbourne School of Engineering, the University of Melbourne, Melbourne, Australia

*Corresponding author e-mail: jzzh4@student.unimelb.edu.au

Keywords: Internet of Things, Wireless Integrated Network Sensors, Comparison of Key Approaches.

Abstract: The Internet of Thing is changing the world as the Internet did. Plenty of enabling technologies has been emerging, including WINSs, WSNs, ad hoc networks, wireless ad hoc sensor networks, MANET, and RFID. This paper aims to distinguish the definition of these terminologies and illustrate the relationship between them. Furthermore, the benefits and drawbacks will be discussed through the comparison of the key approaches of these technologies.

1. Introduction

The Internet of Things (IoT) is changing the world as the Internet did in the past. By far, a large part of the data on the Internet is collected and entered by people, who would delay and make some mistakes. The main feature of IoT is to collect the data obtained by devices automatically. If the Internet can be perceived as a network of people, then IoT can be envisioned as a network of devices. Through attaching Radio Frequency Identification or other kinds of sensors to physical objects, computers can receive data without stopping and precisely even in a severe environment [1].

Like the Internet, the IoT is also a network of networks, instead of a single network. The distinguished character of IoT is the ability that can connect anything (including people and objects) at any place at any time by assembling transceivers into physical objects [2].

The primary purpose of the paper is to provide a brief report of the IoT in terms of critical technologies of development and different approaches being investigated for the IoT.

The remainder of the paper is structured as follows. Section 2 introduces the related work of vital technologies of IoT. Section 3 compares the fundamental approaches and argues the advantages and disadvantages of them. Finally, Section 4 concludes the paper and discusses future directions.

2. Related Work

This section principally concentrates on enabling technologies and significant applications of Internet of Tings.

2.1 Enabling Technologies

This part would concisely present several specific technologies related to IoT, including wireless integrated network sensors (WINSs), wireless sensor networks (WSNs), ad hoc networks, wireless ad hoc sensor networks, and radio frequency identification (RFID). Some of the related terms of those technologies are similar and intricate. Therefore, definitions, components and characters of these technologies will be concluded to help researchers perceive relevant knowledge and distinguish similar terminologies. Additionally, Fig. 1 below demonstrates an overlapping relationship between those technologies. To be more specific, the intersection part of two rectangles presents the shared features of the two technologies.

  DOI: 10.25236/isaiee.2020.016

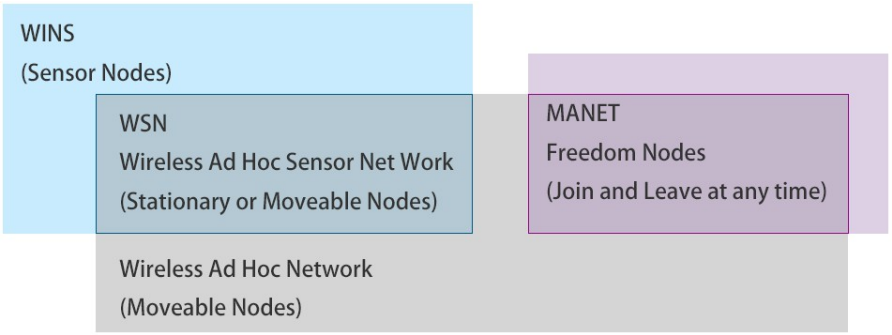

Figure 1. The relationship between IoT technologies.

2.1.1 Wireless Integrated Network Sensors (WINS)

Wireless integrated network sensors (WINS) can be visualised as a dense and low electricity consumption system enabling ongoing monitoring and observing of physical devices, the structure of WINS consists of a wireless sensor, data converter, analyser, and controller. WINS has the ability of sensing, processing, decision making and wireless networking. It can be attached to physical objects in a severe environment. Because the energy supply of WINS is achieved through batteries, the data transmitted in WINS are required to be delivered at a low bit rate with low power consumption transceivers to provide constant monitoring of objects [3].

2.1.2 Wireless Ad Hoc Networks (Ad hoc Networks)

Ad hoc networks is a wireless network between movable hosts, and the transportable hosts are called nodes in groups of academic papers. Unlike cellular networks who need no less than one fixed-location transceiver, ad hoc networks do not need fixed network infrastructures. More specifically, a node can communicate with the nodes which are in its radio scope, besides, for two nodes which are too far away from each other can still communicate if they can find a path through other nodes. Accordingly, ad hoc networks can be implemented more swiftly [4].

2.1.3 Wireless Sensor Networks (WSNs)

WSN is a wireless ad hoc network consisted of an enormous number of small sensor nodes, which communicate with each other by limited power and memory [5]. The set of tiny sensor nodes can be seen as WINS, which is discussed in section 2.2.1. There are four components in WSN, including hardware, communication stack, middleware and secure data aggregation. Compared with the wireless ad hoc network, nodes in WSN are not required to be moveable. That is to say, nodes in WSN can be stationary and moveable. Furthermore, Gubbi et al. (2013) concluded that WSN is the higher-end active FRID, which has relatively low computing and storing abilities [6].

Wireless Ad Hoc Sensor Networks. Wireless ad hoc sensor networks connect the physical world and the Internet, which implied wireless ad hoc sensor networks is the same with WSNs to some extent [7]. Also, wireless ad hoc sensor networks are deduced to be an integration of WINS and ad hoc networks [8].

2.1.4 Mobile Ad Hoc Networks (MANETs)

Mobile ad hoc networks (MANETs) without a central management node is a self-organising network. A node inside MANET can leave the network at any time; also, a node can join a network when the radio range the node can reach to the network. As a result of this, the topology of MANET is not stable and predictable [9].

2.1.5 Radio Frequency Identification (RFID)

Radio frequency identification (RFID) is a chip that can send and receive radio wave. It is composed of a pair of reader and tag. The function of the reader is to send a radio wave; on the other hand, the tag can send an identification frame. The message transmission depends on two protocols; the one is Tag Talk First (TTF), the other one is Interrogator Talk First (ITF). The interrogator here

refers to the reader. In the former protocol, the tag sends data to the reader firstly; however, in the later protocol, the reader sends a request at first. Besides, there are three kinds of tags which are active, passive and semi-active tags. The difference between them is whether they need batteries. Active tags have batteries; consequently, they can send data by themselves. By contrast, there are no batteries inside the passive tags; therefore, they depend on the reader to send identification messages. Semi-active is a mixed vision of the active and passive. There are batteries built-in semi-active tags, but they need a request from readers to become active [10].

2.2 Applications

This section presents the most common applications of the Internet of Things.

Monitoring and Tracking. A health monitoring and tracking system based on IoT could observe the health conditions and locate positions through a global positioning system (GPS) of the soldiers. IoT would send the data collected by the system to a control room which can analyse the situation of the soldiers to protect their precious lives [11]. Furthermore, IoT can enable objects such as smartphones and transportation to work together in an automated and collaborative manner, to provide services to humans [12]. For example, a smartphone can get the real-time data of weather and traffic congestion, and according to the information it can adjust the alarm based on the daily routine of his owner; therefore, he can get to his work in time.

3. Comparison of Key Approaches

This section will compare and discuss the advantages and weaknesses of IoT key approaches including WSN, wireless ad hoc network and MANET. Table 1 shows the specific structure of networks as well as characteristics, which will determine a variation in performance with this result in the benefits and disadvantages.

Table 1. Characteristics of Three IoT Networks.

Wireless Sensor Network	wireless ad hoc network	Mobile Ad Hoc Network
Powered by batteries	Powered by batteries	Powered by batteries
Limited bandwidth	Limited bandwidth	Limited bandwidth
No central management	No central management	No central management
Movable or stationary nodes	Movable nodes	Movable nodes
Unpredictable or fixed topology	Unpredictable topology	Unpredictable topology
Preestablish scale	Preestablish scale	Self-organization scale

As depicted in Fig. 1, WSN (also wireless ad hoc sensor network), wireless ad hoc network and MANET has overlapping features. Brief comparison is showed in Table 1. Common characteristics of them are discussed firstly. They have to be powered by batteries. The bright side is cables do not restrict sensors, and they can be attached to physical object everywhere. However, the life of sensor nodes depends highly on the life of batteries. Also, they can provide continuous and monitoring through wireless networks, but the limited bandwidth leads to a low bit rate. Besides, sensor nodes are distributed on physical objects without a central management node; in other words, each node can act as a transceiver, which means each node is a host and a router. So, the benefit is the loss of one node would not have a dramatic impact on the whole network; however, it is hard to control an enormously extensive scale network.

On the other hand, there are some distinguished attributes of each network. The movability of physical objects that sensor nodes attached to, in those networks, determine whether the sensor nodes

are fixed or moveable. Plus, the movability of nodes decides the topology of networks. As a result of this, sensor nodes of WSN can be moveable or stationary; by contrast, sensor nodes are movable in other networks. Consequently, the topology of WSN can be inconstant or fixed, but the topologies of others are uncertain due to moveable nodes. The advantage of changeable topology is that a network can be adapted and adjusted to meet the requirement rapidly. Nevertheless, unstable topology would lead to an increased loss of nodes.

Another contrast is nodes in MANET have the freedom to leave the network at any time and to join the network as long as their radio range can reach to it. So, MANET has a changeable scale and its a self-organisation network since it could not fix the number of nodes inside the network. Yet in other networks, they preestablish the scale. The traits of freedom joining and leaving in MANET enlarge the adaptability to an unstable environment such as a battlefield. Nevertheless, it can also boost the risk of malicious attacks.

4. Conclusions and Future Directions

The purpose of this article is to give a concise overview of IoT. First, related works are presented through three categories, which play an essential role in the field. Then, by comparing the key approaches, their advantages and disadvantages are discussed.

IoT is changing the world like the Internet did. For instance, DiDi, which can be viewed as the Chinese version of Uber, have been widely adopted as a transportation solution in China. However, DiDi drivers could not locate the passengers if they are not familiar with the district. Finally, IoT would enter into the life of individuals. But before that, figure out a more efficient way to let the components work in a seamless and interoperable manner is necessary.

On the other hand, security plays a significant role in IoT. Weber (2010) pointed out that IoT had a profound effect on the security and privacy of related users. Thereby, proper measurements, for instance, a legal framework which can provide a defense against attacks and protect the privacy of consumers, were crucial as they are supposed to secure the right to release and restrict (or even forbid) data.

Acknowledgments

I wish to show my appreciation to Dr. Ling Luo and Dr. Muhammad Usman, my lecturers at The University of Melbourne. Yifei Wang, my tutor at The University of Melbourne, also looked over my survey. I am also grateful for the insightful comments offered by Prof. Gang Chen at Nanjing University of Aeronautics and Astronautics.

References

[1] Ashton, K. (2009). That ‘Internet of Things’ Thing. RFID Journal

[2] International Telecommunication Union (2005). The Internet of Things – Executive Summary. ITU Internet Reports

[3] Asada, G., Dong, M., Lin, T., Newberg, F., Pottie, G., Marcy, H., & Kaiser, W. (1998).Wireless integrated network sensors: Low-power systems on a chip. In Proceedings of the 24th IEEE European Solid-State Circuits Conference (Den Hague, The Netherlands, Sept. 21–25).

[4] Zhou, L., & Haas, Z. (1999). Securing ad hoc networks. IEEE Network, 13(6), 24-30. doi: 10.1109/65.806983

[5] Ali, A., & Fisal, N. (2008). Security Enhancement for Real-Time Routing Protocol in Wireless Sensor Networks. 2008 5Th IFIP International Conference On Wireless And Optical Communications Networks (WOCN '08). doi: 10.1109/wocn.2008.4542492

[6] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, 29(7), 1645-1660. doi: 10.1016/j.future.2013.01.010

[7] Meguerdichian, S., Koushanfar, F., Qu, G., & Potkonjak, M. (2001). Exposure in wireless Ad-Hoc sensor networks. Proceedings Of The 7Th Annual International Conference On Mobile Computing And Networking - Mobicom '01. doi: 10.1145/381677.381691

[8] Sohrabi, K., Gao, J., Ailawadhi, V., & Pottie, G. (2000). Protocols for self-organization of a wireless sensor network. IEEE Personal Communications, 7(5), 16-27. doi: 10.1109/98.878532

[9] Fazeldehkordi, E., Amiri, I., & Akanbi, O. (2016). A study of black hole attack solutions (1st ed.). Waltham, MA: Elsevier.

[10] Gnimpieba, Z., Nait-Sidi-Moh, A., Durand, D., & Fortin, J. (2015). Using Internet of Things Technologies for a Collaborative Supply Chain: Application to Tracking of Pallets and Containers. Procedia Computer Science, 56, 550-557. doi: 10.1016/j.procs.2015.07.251

[11] Patii, N., & Iyer, B. (2017). Health monitoring and tracking system for soldiers using Internet of Things (IoT). 2017 International Conference On Computing, Communication And Automation (ICCCA). doi: 10.1109/ccaa.2017.8230007

[12] Weber, R. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30. doi: 10.1016/j.clsr.2009.11.008

[13] Zhu, C., Leung, V., Shu, L., & Ngai, E. (2015). Green Internet of Things for Smart World. IEEE Access, 3, 2151-2162. doi: 10.1109/access.2015.2497312