A brief survey on Internet of Things

Jiawei Luo, *University of Melbourne*, Melbourne, Australia

Student id: 1114028

I. INTRODUCTION

The Internet of Things (IoT) has seen rapid growth in the last few years. In the era of rapid technological development, IoT related technology has also been many breakthroughs. Different from the direct data interaction between people on the traditional Internet, the IoT focuses more on the connection between devices. In the traditional Internet, people usually use personal devices to exchange data between people, such as personal computers, mobile phones. The birth of the IoT has dramatically changed that, with data exchange occurring directly on every device, including cell phones, watches, TVs, cameras. In this new era, machines will replace direct human communication, and the communication between people and devices, devices and devices will be more diverse[1].

IoT is essentially an extension of the Internet. The IoT integrates embedded system, sensors, smart terminals, cloud computing, and more. The advancement of the IoT technology depends on more than one aspect of technology development. Its research often relies on more underlying technologies, such as big data processing in computer science, network security, network protocols, machine learning, signal processing in electrical engineering and microelectronics. Based on the sensor network model of the IoT, objects can collect large amounts of data through sensors and transmit the data to the network for analysis and computation. Computing techniques (such as Cloud computing), Radio Frequency Identification(RFID) and wireless transmission techniques play essential roles[2, 3]. According to the study[2], The number of devices connected to the IoT is growing at an incredible rate, with the capacity to reach several times of the size of the global population, which will not only bring in unimaginable economic revenue but will also pose significant challenges to existing computing, Internet capacity and transmission technologies.

A single transport protocol or communication protocol cannot meet the needs of various IoT application scenarios. Generally speaking, IoT uses transport protocols for communication and data transfer between subnet devices, as well as communication protocols (e.g., TCP/IP protocol) built on the traditional Internet to enable data exchange and communication between devices, controllers, and servers over the Internet. In this survey, the IoT protocols for different scenarios will be introduced, such as Wi-Fi, RFID, Zigbee, LPWAN, Bluetooth, which has developed rapidly in the past few years.

II. RELATIVE WORKS

A. *Addressing protocols of IoT*

IoT devices are similar to the Internet, and Internet protocols used to solve many IoT problems in varies scenarios. Due to the scenario limitations of many IoT applications, such as inherent bandwidth limitations, as well as power and transmission distance limitations, unique solutions are often required for data transmission, network connectivity, direct interconnection of devices, and device discovery and communication. A large number of IoT devices require a low-power, broad-spectrum protocol, similar to the network protocol IPv4/IPv6, and each IoT device also requires a protocol that can accurately identify the device.

1) IPv4/IPv6

IPV4 and IPV6 are the two major IP versions of the Internet today. IPV4 uses 32-bit addresses, and it only allows about a billion unique addresses. That is not enough in today's vast Internet. In recent years, a large proportion of Internet devices have been using the IPV6 protocol, which has 128-bit addresses, which means that the shortage of IPV4 addresses can overcome. Moreover, for the IoT, that number of addresses is indispensable. The IoT brings many times as many terminals as the traditional Internet.

2) RFID

An RFID system usually consists of an electronic tag, a reader, and an antenna, the tag is composed of a coupling circuit and a chip, which can form a unique electronic identification code to be recognized by the reader through radio waves. It fits well with the low power technology that devices in the IoT need to reduce their power consumption, which is why RFID was one of the hallmarks of the early IoT[4].

RFID is more expensive than printed labels, but it works better with other technologies in the IoT. Combining IPV6 with RFID brings the following benefits: 1) a large number of identifiers to uniquely identify each object, and IPV6 brings 128-bit address space. 2) IPV6 protocol has a fixed packet header and structure, which is beneficial to the route planning of the IoT, and strengthens the QoS between networks so that the back-end can deal with the traffic more quickly and accurately. 3) in the mobile IoT, IP addresses can be updated in real-time, which meets the mobility requirements and improves the quality of IoT service.

B. *Short-range Wireless Sensor network (WSN)*

A WSN is a collection, processing, storage, analysis and dissemination network based on a large number of sensors, and is the foundation of an IoT system. The development of low-power integrated

circuits and technological advances in wireless communications have enabled WSNs to share data between nodes and to perform centralized or distributed analysis. A WSN network usually consists of WSN hardware, WSN communication stack, WSN Middleware, and Secure Data aggregation[6]. Data is collected by the hardware and transferred to a topology network of communication stack, while secure data aggregation ensures data security and reliability[3]. Many IoT short-range communications have been researched, either as new or as innovations on existing technologies. Among them, WSN based on Wi-Fi, Bluetooth (or BLE for IoT), or ZigBee is widely recognized and used in practical applications.

1) Zigbee

Zigbee is a low-speed, low-power, short-range, self-organizing wireless sensor technology[5], widely used in applications. The most significant advantage of Zigbee is that it can automatically form a network of devices, linking the data transmission between the various devices, but in this self-organizing network needs a central device to manage the entire Zigbee network. It means that in the network, there must be a "hub"-like component in the Zigbee device network that connects the devices to achieve the linkage effect between Zigbee devices. However, Zigbee management is not successful. Because of the different standards between manufacturers, if only the purchase of a single Zigbee device, or the purchase of devices between different manufacturers, there will be no use. Since ZigBee is not open source, it cannot interface with current IP-based network protocols, which further enhances the limitations of ZigBee. And the ZigBee's ability to transmit data is not strong, with short transmission distance, poor penetration, high wall loss, low non-linear transmission capacity.

2) Bluetooth

Bluetooth is a long-established, popularly recognized wireless communication technology, and BLE is known as a development on Bluetooth that empowers the IoT in terms of functionality. It enables short distance data exchange between devices including personal networks and mobile devices. Furthermore, Bluetooth 4.0 or BLE offers the advantages of low power consumption than traditional Bluetooth, the wide range in an IoT environment, and it supports a star topology[6], thus enabling one-to-many connections. It also has its weaknesses. The star-only network topology makes it dependent on a central node, which requires a smart device to operate, such as a mobile phone. The small size of the Bluetooth module makes it easy to integrate, and the fact that it supports the IPv6 protocol means that Bluetooth will be of great value in future IoT development [9].

3) Wi-Fi

Another widely known and used technology is wireless fidelity (WI-FI). Based on the Ethernet communication protocol, Wi-Fi terminals can send and receive high-frequency wireless signal data within a short range, providing high-speed, stable data exchange. The advantage of Wi-Fi is that local

area network deployment does not require the use of wires, reducing deployment and expansion costs. Besides, according to the Wi-Fi Alliance, Wi-Fi uses global standards, and any Wi-Fi standard device will work correctly anywhere in the world, while Wi-Fi is far more common than Zigbee, this means lower development and deployment costs, as well as shorter development cycles.

The advantages of Wi-Fi over Zigbee also include faster speeds, more extensive data transfers, and better user experience[5]. Smart devices with Wi-Fi can easily connect to mobile phones without the need for a gateway as Zigbee devices can do. The main disadvantage of Wi-Fi is the power consumption, the general standby power consumption of Wi-Fi devices is about 1W, while the general standby power consumption of BLE devices and Zigbee devices are within 0.1W. Compared to the power consumption of Wi-Fi devices is much better, so Wi-Fi is usually not the first choice for power-constrained devices, but its widespread presence makes it the choice in many scenarios. Besides, the number of accesses to Wi-Fi smart devices is also a big issue, and theoretically, the maximum number of Wi-Fi accesses is mainly determined by the number of nodes in the router. In the case of current home routers, if there are more than dozens of electronic devices that need to be connected in the router, the user experience is much reduced.

In terms of Non-line-of-sight (NLOS) [5], WSN based home application requires a high level of Non-line-of-sight ability. It refers to the ability of transmission radio in non-line-of-sight conditions, the resulting degradation in signal quality and reduced reception success by the receiver. Compared to Wi-Fi and BLE, Zigbee has little to no non-line-of-sight transmission, so its ability to transmit signals in many scenarios, like indoors, is drastically reduced with the slight interference.

C. Low Power Wide Area Network (LPWAN)

Zigbee, Bluetooth and Wi-Fi are often considered for short-range communication, which means they may not be suitable for some scenarios that require long-distance transmission. LPWAN is a technology with low power consumption and vast transmission distance, which makes up the shortcomings of other transmission methods. It also uses far less power than cellular communications technologies such as 4G and 5G.

1) NB-IoT

NB-IoT is an IoT system based on existing LTE functions. Its features include low cost, wide range and low power consumption and large capacity[8]. On top of existing LTE systems, it is possible to use existing hardware, upgrade the software, and adapt it to IoT needs, so it can be simplified and optimized to support most LTE capabilities in IoT. NB-IoT minimizes the capabilities of the LTE protocol by keeping the power and occurrence of the terminal system to a minimum. As a result, the terminal equipment requires only a small number of batteries to maximize its cost-effectiveness.

According to [8], by adding more NB-IoT carriers, NB-IoT allows terminal devices to connect at least 72k devices per cell, with the potential to expand capacity.

2) LoRa

LoRa is essentially a physical layer application, which is based on spread spectrum technology for long-distance wireless transmission, the characteristics of LoRa include: long-range, low power consumption, multi-node, low cost, immunity characteristics, while LoRa uses low rate signal, can only support small data transmission. Lora uses the unlicensed ISM band[7], which means that it only works on certain designated free bands below 1 GHz. Lora has won complete attention for its sensitivity, robust anti-interference capability, and excellent system capacity performance. Two-way communication is provided by chirped spread spectrum (CSS) modulation[7, 12], which spreads the narrowband signal over a wide channel bandwidth, making the signal highly resistant to interference and challenging to detect and interfere with.

LoRa and NB-IoT have different business scenarios. NB-IoT works in the authorized spectrum, and Lora works in the unauthorized spectrum. This means that if someone wants to use NB-IoT, it is necessary to use cellular companies' networks, and using NB-IoT is mainly dependent on the infrastructure of the carriers. In places where the infrastructure of many carriers is not fully covered, NB-IoT is almost unusable. Lora, on the other hand, is a more flexible, autonomous network that businesses and even individuals can deploy wherever they need to.

D. Cloud computing

If WSNs are compared to the human body's sensory network, then cloud computing can be treated as an organ like the brain for the IoT. Cloud computing provides an efficient, low-cost solution for the back-end services of the IoT. It designs to solve large scale data processing problems by building data centres through the distributed computing and the Virtualization Technology, providing data storage, analysis, and computing services to developers and enterprise users[2]. It provides a carrier and analysis scheme for a large amount of data produced by the IoT and solves the low-efficiency problem caused by the traditional network system.

E. Edge computing

In contrast to cloud computing, Edge Computing does not upload part of data to cloud for processing, but directly to the part that closes to the terminals of the computation. With the growth of the IoT, the demand for data storage and computing will bring higher pressures for cloud computing capabilities, and cloud computing is sometimes not up to the demands of computing vast amounts of data and getting immediate feedback in many scenarios. Edge computing, on the other hand, splits large services into smaller and easier-to-manage parts, which are not handled entirely by the central

node. This speed up the processing and transmission of data provides a high bandwidth service and reduces latency. At the same time, AI models, including deep learning, can be used widely and individually in edge computing[11]. The performance and feedback speed of the deep neural network can be improved by distributing the layers of deep neural network in edge nodes and cloud nodes. Meanwhile, the large amount of data collected by the IoT can provide a large number of data sets for deep learning, cloud computing, on the other hand, can provide training hardware for deep learning.

III. Comparison of Key Approaches

In Section II, several IoT protocols for different scenarios are introduced. In general, short-range WSN has the characteristics of high transmission rate and short coverage. LPWAN, on the other hand, applies to scenarios that require long-distance transmission, often using Narrow bands, which result in minimal bandwidth. In terms of data transmission speed, Wi-Fi can have 100M to 150Mbps throughput with a range of 300m outdoor and 100m indoor, and up to 2MKbps. The transmission rate of Zigbee is about 10 to 250Kbps with a range of 10-75m[5]. While BLE can also achieve higher throughput, compare with Zigbee[10]. However, LPWAN, in the analysis of [7] and [8], NB-IoT and LoRa give up to a few kbps transmission rate with a range of over 2 km coverages.

Regarding power consumption, Wi-Fi usually is not considered in many power-constrained scenarios due to its high power consumption, but it has a significant advantage on scenarios that great QoS required like smart home applications. Meanwhile, ZigBee, BLE provide lower power consumption to increase the mobility of devices and battery life. As for LPWAN, both NB-IoT and LoRa can have deficient power consumption for satisfying their requirement of design.

In terms of computing, the big trend is the collaboration between cloud computing and edge computing. Edge computing can functionally compensate for a large amount of data transmission problems, untimely feedback, and security issues associated with cloud computing[11]. Due to the current development of IoT, the data generated by WSN is a huge challenge for bandwidth if it is all transferred to the cloud. Today's data generation by a person is in the order of gigabytes per day, while for other applications, such as autonomous cars and aeroplanes, the data generated per second will be in the order of gigabytes. This data needs to be fed back immediately, or it could have serious consequences. Moreover, edge computing makes up for the lack of computing power in the cloud. In terms of security, because cloud computing transmits private data collected by body wearable, medical, and industrial manufacturing devices to the data centre via a long path, it is prone to the risk of data loss or information leakage. In contrast, edge computing is closer to the end device, and its transmission is

more secure. As such, they complement each other and work together to provide better performance for applications.

IV. Conclusions and Future Directions

This survey provides an overview of protocols in IoT for different scenarios and summarizes the difference between Wi-Fi, Zigbee, Bluetooth based WSN and two LPWAN techniques, as well as a brief discussion of cloud computing and edge computing, their pros and cons are discussed in terms of IoT requirements. As research on the IoT continues to increase, more advanced technologies will emerge, especially in the last few years with the current rapid deployment of 5G networks. The IoT will become increasingly integrated into our daily lives. They are becoming increasingly involved in terms of communication, interaction, data analysis, control, and models created from massive amounts of data. This will make the future of the movie not so far away.

More importantly, just as the birth of countless Internet applications has changed our lives, the advent of increasing IoT devices will change our lives in unpredictable ways. The market and research area of the IoT is like an untapped gold mine waiting to be explored, and the application scenario and user experience of the IoT applications are the focus of researchers.

References

[1] Lu Tan and Neng Wang, "Future internet: The Internet of Things," in 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), Aug. 2010, vol. 5, pp. V5-376-V5-380, doi: 10.1109/ICACTE.2010.5579543.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] D. Wang, D. Chen, B. Song, N. Guizani, X. Yu, and X. Du, "From IoT to 5G I-IoT: The Next Generation IoT-Based Intelligent Algorithms and 5G Technologies," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 114–120, Oct. 2018, doi: 10.1109/MCOM.2018.1701310.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/j.future.2013.01.010.

[4] X. Jia, Q. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in Internet of Things (IoT)," in *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Apr. 2012, pp. 1282–1285, doi: 10.1109/CECNet.2012.6201508.

[5] L. Li, H. Xiaoguang, C. Ke, and H. Ketai, "The applications of WiFi-based Wireless Sensor Network in Internet of Things and Smart Grid," in *2011 6th IEEE Conference on Industrial Electronics and Applications*, Jun. 2011, pp. 789–793, doi: 10.1109/ICIEA.2011.5975693.

[6] S. Al-Sarawi, M. Anbar, K. Alieyan, and M. Alzubaidi, “Internet of Things (IoT) communication protocols: Review,” in *2017 8th International Conference on Information Technology (ICIT)*, May 2017, pp. 685–690, doi: 10.1109/ICITECH.2017.8079928.

[7] K. Mikhaylov, - Juha Petaejaejaervi, and T. Haenninen, “Analysis of Capacity and Scalability of the LoRa Low Power Wide Area Network Technology,” in *European Wireless 2016; 22th European Wireless Conference*, May 2016, pp. 1–6.

[8] R. Ratasuk, B. Vejlgaard, N. Mangalvedhe, and A. Ghosh, “NB-IoT system for M2M communication,” in *2016 IEEE Wireless Communications and Networking Conference*, Apr. 2016, pp. 1–5, doi: 10.1109/WCNC.2016.7564708.

[9] M. Baert, P. Camerlynck, P. Crombez, and J. Hoebeke, “A BLE-Based Multi-Gateway Network Infrastructure with Handover Support for Mobile BLE Peripherals,” in 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Nov. 2019, pp. 91–99, doi: 10.1109/MASS.2019.00020.

[10] F. J. Dian, A. Yousefi, and S. Lim, “A practical study on Bluetooth Low Energy (BLE) throughput,” in 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Nov. 2018, pp. 768–771, doi: 10.1109/IEMCON.2018.8614763.

[11] H. Li, K. Ota, and M. Dong, “Learning IoT in Edge: Deep Learning for the Internet of Things with Edge Computing,” IEEE Network, vol. 32, no. 1, pp. 96–101, Jan. 2018, doi: 10.1109/MNET.2018.1700202.

[12] K. Mekki, E. Bajic, F. Chaxel, and F. Meyer, “A comparative study of LPWAN technologies for large-scale IoT deployment,” ICT Express, vol. 5, no. 1, pp. 1–7, Mar. 2019, doi: 10.1016/j.icte.2017.12.005.