Horizon Scanning Series

The Internet of Things

Telecommunications

This input paper was prepared by Zhanwei Hou with contributions from Peng Cheng, Wibowo Hardjawana, Yifan Gu and Branka Vucetic

Suggested Citation

Hou, Z, Cheng, P, Hardjawana, W, Gu Y and Vucetic, B (2019). The Internet of Things: Telecommunications. Input paper for the Horizon Scanning Project "The Internet of Things" on behalf of the Australian Council of Learned Academies, www.acola.org.

Telecommunications

This input paper was prepared by Dr. Zhanwei Hou, with contributions from Dr. Peng Cheng, Dr. Wibowo Hardjawana, Dr. Yifan Gu and Prof. Branka Vucetic from University of Sydney.

1 Communication Technologies for IoT

The IoT devices including sensors and actuators, equipment, machines, and computers are connected to each other by communication networks, which collect, analyse and act on the data without human intervention. As such, communication technologies are the backbone of the infrastructure of IoT. In this section, we will compare different communication technologies and foresee the future technology advancements.

1-1 Technology Comparison

In this section, we compare some popular communication technologies for the IoT as shown in Table 1[1,2,3].

Table 1 Comparison of communication technologies for the IoT

	Standard	channel bandwidth	Data rate	Latency	Transmission range	Energy consumption	Cost
Cellular network	4G: LTE	5-20MHz	DL:0.1-1Gbit/s UL: 50Mb/s	10-100ms	Cellular coverage area	High	High
	5G: NR	up to 800 MHz	1-20Gb/s	1-5ms		High	High
Cellular IoT	LTE-M: 3GPP R12, R13, R14	1.4 MHz	1Mb/s	10-15ms	11km	Low	Low
	NB-IoT: 3GPP R13, R14	180 kHz	250kb/s	1.6-10s	35km	Very low	Low
WiFi	IEEE 802.11a/b/g/n/ac	20-40MHz	1Mb/s–1 Gb/s	10-100ms	20–100 m	High	High
	IEEE 802.11ah	1-16MHz	0.3-347Mb/s	10-100ms	1km	Low	Low
WiMAX	IEEE 802.16	1.25-20MHz	1Mb/s–1 Gb/s	50ms	<50km	Medium	High
ZigBee	IEEE 802.15.4	2MHz	40–250 kb/s	60-100ms	10–20 m	Low	Low
Bluetooth	IEEE 802.15.1	1 MHz	1 Mb/s	100-500ms	8–10 m	Bluetooth: Medium BLE: Very Low	Low
LoRa	LoRa(PHY) LoRaWAN(Networking layer)	125-500kHz	0.3–50 kb/s	1-15s	15 km	Very Low	Low

[1] Ray, Partha Pratim. "A survey on Internet of Things architectures." Journal of King Saud University-Computer and Information Sciences 30, no. 3 (2018): 291-319.
[2] Elkhodr, Mahmoud, Seyed Shahrestani, and Hon Cheung. "Emerging wireless technologies in the internet of things: a comparative study." arXiv preprint arXiv:1611.00861 (2016).
[3] Sinha, Rashmi Sharan, Yiqiao Wei, and Seung-Hoon Hwang. "A survey on LPWA technology: LoRa and NB-IoT." Ict Express 3, no. 1 (2017): 14-21.

1) WiFi and Wimax

The 802.11 protocol family with its variants of IEEE 802.11a/b/g/n/ac is among the first technology choices for supporting the IoT since they have been widely deployed[4]. These protocols can provide data rates from 1Mb/s to 1Gb/s with transmission range of around 20m indoor and 100m outdoor. WiMax used to be an alternative option, but it has been replaced by LTE and other technologies.

In many IoT applications, the IoT devices have limited hardware capability, low-power consumption and low-cost requirements. As such, low-cost and low-power wireless technologies are needed. ZigBee, Bluetooth and LoRa are some popular technology options for the low-power IoT applications. To extend the application scenarios of WiFi, IEEE 802 LAN/MAN Standards Committee (LMSC) developed an IEEE 802.11ah protocol aiming at the low-power applications. It operates on unlicensed sub-1GHz band, provides coverage of 1km, can support around 8000 nodes in one access point[5].

2) ZigBee, Bluetooth and LoRa

Compared with IEEE 802.11a/b/g/n/ac, ZigBee and Bluetooth (or Bluetooth Low Energy, BLE) are intended for portable devices for a low data rate application with limited battery power over short ranges. By using the unlicensed ISM frequency band, the data rate is generally less than 1Mb/s and the transmission range is less than 20m. Bluetooth can provide a slightly larger data rate but a lower number of nodes, i.e., eight nodes per network/piconet. ZigBee can support more nodes, which is approximately 65,000 in theory, but may be less in practice due to collisions caused by carrier sense multiple access/collision avoidance (CSMA/CA) protocol and limited computing capacity of devices.

The emerging LoRa technology, developed by the LoRa Alliance, is intended for the low-power wide-area network (LPWAN) [6] . LoRa uses chirp spread spectrum modulation, which can support a large transmission range of up to 15km with a relatively low data rate of 0.3–50 kb/s by using the unlicensed ISM frequency band. Moreover, LoRa has a very high capacity to receive messages from a very large amount of end nodes. In Jan. 2019, the LoRa Alliance announced that more than 100 network operators have deployed and operate LoRaWAN networks, which are both public and private[7].

3) Cellular IoT

Aiming at low-power wide-area network (LPWAN), cellular IoT technologies developed by 3GPP include LTE-M and NB-IoT. Among these protocols, NB-IoT is the most recent one standardised in 2016. The deployment options for NB-IoT are quite flexible: 1) standalone, reusing 200kHz bandwidth of GSM; 2) guard-band, using the guard band of two adjacent LTE carriers; 3) in-band, 200KHz of the LTE band is reserved for NB-IoT.

---

[4] Li, Li, Hu Xiaoguang, Chen Ke, and He 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, pp. 789-793. IEEE, 2011.

[5] T. Adame, A. Bel, B. Bellalta, J. Barcelo, J. Gonzalez, and M. Oliver, "Capacity analysis of IEEE 802.11 ah WLANs for M2M communications," in Multiple Access Communications, ed: Springer, 2013, pp. 139-155.

[6] Lavric, Alexandru, and Valentin Popa. "Internet of things and LoRa™ low-power wide-area networks: a survey." In 2017 International Symposium on Signals, Circuits and Systems (ISSCS), pp. 1-5. IEEE, 2017.

[7] https://lora-alliance.org/in-the-news/lora-alliance-passes-100-lorawantm-network-operator-milestone-coverage-100-countries

Different from LoRa working in the unlicensed spectrum, NB-IoT operates in licensed bands. As such, it can provide better QoS at the expense of a higher cost. The applications requiring higher QoS prefer NB-IoT. Because of the infrequent but regular synchronization with the base station in NB-IoT, it has a lower latency but consumes extra energy and thus the battery life of NB-IoT is lower than that of LoRa, which operates in asynchronous way. Applications sensitive to latency and requiring higher data rates would benefit more from NB-IoT. In March 2019, the Global Mobile Suppliers Association announced that over 100 operators in 53 countries have deployed/launched either NB-IoT or LTE-M networks[8].

4) Evolving from 4G to 5G and future 6G

Different from WiFi, 4G can provide better QoS, support mobility and large area coverage. It can be used for the IoT applications to connect to the Internet, which require better QoS than WiFi, and mobility support. Compared to LTE-M and NB-IoT it can support higher data rates, as for example for IoT based video surveillance.

The emerging 5G cellular networks provide connectivity for these three groups of scenarios: enhanced Mobile Broadband (eMBB), which improves data rates and capacity of 4G, massive Machine-Type Communications (mMTC), for a massive number of IoT devices in dense urban environments with low data rates and limited computing resources, and ultra-reliable low latency communication (URLLC), which intends to provide extremely high reliability with very low latency. By using Software Defined Networking (SDN), Network Function Virtualization (NFV) and mobile edge computing (MEC), 5G will enable network slicing to support multiple communication networks optimised for different services over the same physical infrastructure. For eMBB, a peak data rate can reach 20Gb/s, which is targeting high speed mobile connections and supporting emerging virtual/augmented reality services. mMTC will support smart metering, transport logistics and environment monitoring. By contrast, 4G generally operates at up 28Mb/s. 5G could even replace many landline connections. 5G base stations will be able to handle up to a million connections, versus the 4,000 that 4G base stations can cope with. That should make communications at sporting events, and concerts much easier, and it could enable many IoT applications.

The most innovative part of 5G is URLLC, which is targeting wireless control of mobile robots in industrial automation, self-driving connected cars, smart grids, telerobotic surgery, and the Tactile Internet. They will enable large scale automation and increased industrial productivity, road safety, improved healthcare, higher energy efficiency and integration of renewable energy sources into energy grids. As such, 5G is one of the critical pillars of the fourth industrial revolution, also referred to as "Industry 4.0" or "the Industrial Internet of Things (IIoT)" or "the Industrial Internet". In our work, we will not differentiate the subtle differences among these terms but use the term "Industrial Internet of Things" instead. URLLC in 5G will guarantee 1 ms end-to-end (E2E) delay and the reliability of 99.999%, compared to more than 50ms latency in 4G and network availability of 95%. To satisfy the ultra-low E2E delay requirement, some techniques have been applied to reduce latency in the 5G standard, such as using "mini-slots" in 5G New Radio (NR)[9] to reduce the transmission delay and grant-free access to reduce the access delay. To improve the reliability in the short delay regime, different kinds of diversities are introduced, such as time and frequency diversities (e.g., K- repetition with frequency hopping), spatial diversity (e.g., massive MIMO), and multi-

[8] https://gsacom.com/paper/global-narrowband-iot-lte-m-networks-march-2019/

[9] 3GPP TR 38.802 V2.0.0, “Study on new radio (NR) access technology; physical layer aspects (release 14),” 2017.

connectivity. By introducing diversities, the reliability is improved at the cost of reduced resource utilisation efficiency[10]. Since the spectral resources shared by multiple devices for communications are quite limited, achieving the E2E delay and reliability requirements with affordable spectral resources and limited energy supply is very challenging.

By August 2019, the Global Mobile Suppliers Association announced that “296 operators in 100 countries have launched with limited availability, demonstrated, deployed, are trialling or testing, or have been licensed to conduct field trials of mobile 5G or fixed wireless access (FWA) 5G. Moreover, 56 operators in 32 countries have announced the deployment of 5G within their network”[11]. Apart from being deployed in mobile operator networks, 5G is expected to be used in private networks, such as those in the Industrial IoT or enterprise networking.

Similar to the deployment of 5G, the next generation 6G is in its infant stage. An unprecedented proliferation of new IoT services are emerging including XR Cross Reality services composed of virtual reality (VR), augmented reality (AR) and mixed reality (MR), telemedicine, Tactile Internet, brain-computer interfaces, flying vehicles and automated driving[12]. To support these new applications, 6G must simultaneously deliver high reliability, low latency, and high data rates, for heterogeneous IoT devices[13]. The enabling technology will be Terahertz communications, satellite communications and artificial intelligence (AI). 6G will impact the IoT significantly in the next ten years.

5) Wired technologies for IoT

It should be noted that there are still some scenarios where wired communications are employed for IoT applications, such as building automation, power utility and industrial automation[14]. Traditionally, dedicated wired technology named “fieldbus" were used to replace the parallel cables between sensors, actuators, and controllers. Various kinds of fieldbus systems, such as controller area network (CAN) or Modbus have been developed, most of which are very simple with a data rate of 1-10Mb/s and a transmission range of less than 100m. The big problem of fieldbus systems is the incompatibility with the Ethernet or IP based local area network (LAN), which becomes a great hurdle of the integration with external Internet. As such, a new wave of Ethernet-based networks has emerged with a larger data rate of 100Mb/s. To deal with the real time applications, some modifications are made to improve the real-time capability of the standard Ethernet, such as real-time Ethernet (RTE). The wired network is traditionally considered to be more reliable than wireless networks and can be used to supply electric power at the same time. However, wireless solutions are becoming preferred connectivity options, with much higher flexibility, scalability, less expensive deployment and maintenance. 5G URLLC will offer 1ms latency with 99.999% network availability, which will meet the requirements of many real time applications, e.g., industrial and energy grid automation. In the future five to ten years, both wired and wireless communication technologies will be employed according to the different requirements of the applications.

[10] Hou, Zhanwei, Changyang She, Yonghui Li, and Branka Vucetic. "Ultra-Reliable and Low-Latency Communications: Prediction and Communication Co-Design." In ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1-7. IEEE, 2019.

[11] https://gsacom.com/technology/5g/

[12] Giordani, Marco, Michele Polese, Marco Mezzavilla, Sundeep Rangan, and Michele Zorzi. "Towards 6G Networks: Use Cases and Technologies." arXiv preprint arXiv:1903.12216 (2019).

[13] Saad, Walid, Mehdi Bennis, and Mingzhe Chen. "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems." arXiv preprint arXiv:1902.10265 (2019).

[14] Alessandra Flammini, Paolo Ferrari, Daniele Marioli, Emiliano Sisinni, and Andrea Taroni. "Wired and wireless sensor networks for industrial applications." Microelectronics journal 40, no. 9 (2009): 1322-1336.

1-2 Opportunities, Challenges

In the future IoT networking, there will be different application scenarios with various of demands in terms of data rates, latency, reliability, transmission range, power consumption, cost, QoS requirement and so on. As such, multiple communication technologies will be applied in IoT. Currently, Lora and NB-IoT are competing for the low-power wide-area networks and may replace the Zigbee or Bluetooth to some extent. At the same time, WiFi and LTE can support the application requiring high data rate. In the future five years, 5G will provide much faster Internet connection for mobile users, and URLLC will create new opportunities for ultra-high reliability and low latency applications in the Industrial Internet of Things. In the next ten years, 6G empowered by Satellite and AI will lead to unprecedented innovative applications in XR (VR/AR/MR), telemedicine, Tactile Internet, brain-computer interfaces, flying vehicles and automated driving.

1) National IoT Network

Past or current IoT communication networks are mainly proprietary and deployed over small areas with a range of a few hundred meters, Increasingly, with emerging standards, such as NB-IoT and LoRa, it becomes possible to establish a national communication infrastructure for the IoT. For example, Poland has developed a national infrastructure of IoT, called “The Things Network”, which used 87 LoRa gateways connecting the whole ground territory with network coverages of 30km^2 in urban areas even including indoor buildings and 450km^2 in the open space areas[15]. A national IoT network will avoid repetitive construction, improve the efficiency and reduce the cost by sharing the unified IoT infrastructure.

It should be noted that hybrid technologies may be used in the same application. For example, in the Industrial IoT, URLLC will be used for real time control applications and low power technologies like LoRa and NB-IoT can be used for monitoring purposes. As such, it is important to ensure secure interoperable communications among various IoT systems, which create a harmonious ecosystem of smart IoT devices.

2) Industrial IoT

In the next five years, the Industrial IoT will revolutionise industry, transportation, agriculture, and energy. By connecting sensors, machines, equipment and computers, it will collect, analyse and act on data in industrial processes, agriculture production and critical infrastructure, to intelligently optimise their behaviour without or with minimal human intervention.

A major challenge for the Industrial IoT lies in the development of wireless communications with high standards of reliability, latency and security, i.e., ultra-reliable low latency communications (URLLC). Despite the academic research and on-going standardization efforts towards URLLC, there are still many challenges, including how to the ensure the ultra-high reliability and low latency within the limited radio spectrum.

To tackle the above challenge, the research on URLLC, standardisation of communication protocols and developing IIoT applications should be addressed.

3) Satellite and AI empowered 6G

[15] https://www.thethingsnetwork.org/country/poland/

In the next ten years, 6G empowered by Satellite and AI will lead to unprecedented innovative applications in XR (VR/AR/MR), telemedicine, Tactile Internet, brain-computer interfaces, flying vehicles and automated driving, which will significantly impact human life, economy and environment. It will provide data rates of up to 1-terabyte-per-second, that would allow downloading 300 movies in a second. It will also enable to realise the full capabilities of URLLC, that 5G envisioned. 6G will provide a full integration of the physical, biological and digital world, through digital twinning by making digital copies of the real-world using sensors. It will provide faster connection to the Internet, connect billions of IoT devices, and ultra-reliable low latency communication with high data rate for XR, telemedicine, and Tactile Internet. Specifically, the Satellite can work together with the terrestrial national IoT network seamlessly providing coverage for the vast land of Australia, which, for example, will provide unprecedented supports for the smart agriculture/forest in economics, for the smart water in environmental sustainability and for the smart transportation to improve social efficiency of Australia. This will cause an amazing effect where new products and services can be built to utilize 6G's bandwidth and other improved features to their fullest extents. 6G might eventually approach the upper limits of the mmWave radio spectrum and reach extremely high frequency levels of 300 GHz, or even terahertz ranges.

6G will enable ultrafast, reliable and low latency communication for AI based collaborative processing of large amounts of data generated in real time to optimise transportation networks, smart grids, financial market monitoring and healthcare systems. It could take up to 2030 before 6G is standardised and deployed.

2 Spectrum considerations

Spectrum is a critical input to Australian communications and media industries as increasing services and activities are relying on wireless connectivity. The emerging and existing wireless technologies are continuously driving demand for spectrum, such as 5G cellular networks, the booming Internet of Things (IoT) applications, and smart satellite technologies. To meet this challenge, the government regulator, Australian Communications and Media Authority (ACMA)[16], endeavours to provide efficient and effective spectrum management to maximise the economic benefits of all parties involved.

2-1 Wireless broadband, including 5G

5G utilises spectrum across a wide range of frequency bands. This will include low-band spectrum below 1 GHz, mid-band spectrum between 1 and 6 GHz, and high-band millimetre wave (mmWave) band[17]. Below 1 GHz, the ACMA aims to optimise the efficient configuration of the existing 850 and 900 MHz band allocations. The mid-band between 1 and 6 GHz are currently the focus of 5G deployments, particularly around 3.4 to 3.7 GHz in Australia. In December 2018, the ACMA allocated 125 MHz of spectrum in the 3.6 GHz band (3575–3700 MHz), in metropolitan and regional areas. In the mmWave band, the ACMA is currently focusing on the bands above 24 GHz.

[16] ACMA, Five-year spectrum outlook 2018-22

[17] Flore, Dino, 5G-NR workplan for eMBB, 2017. online: https://www.3gpp.org/news-events/3gpp-news/1836-5g_nr_workplan

2-2 Machine-to-machine communications and the Internet of Things (IoT)

The IoT can use frequency allocations across the entire spectrum. For example, devices providing industrial metering, switching and/or control (including smart infrastructure) feature very low data rates and operate in low-power wide-area (LPWA) networks. Typically, these devices can operate in the 900 MHz band. IoT devices can also operate within the 4G spectrum, over NB-IoT and LTE-M. In Germany, there is 100MHz of dedicate allocated spectrum between 3.7 and 3.8GHz in 5G for industrial IoT. New space based IoT services enabled by small satellite technologies can be delivered within the established satellite bands.

2-3 Satellite communications

There is continuing growth in the delivery of satellite communication and in space science services. Satellite broadband high throughput systems (HTS) is fuelling a demand for spectrum arrangements to support ubiquitous earth stations for user terminals. The current Australian spectrum management can provide broadband HTS by using 1.55 GHz total uplink/downlink spectrum in Ku-band and 2.6 GHz in Ka-band. To meet the future growth in satellite broadband HTS, the ACMA is investigating possible changes in both the Ku-band for additional downlink spectrum shared with terrestrial fixed links in 10.7–11.7 GHz and the uplink range of 27.5–29.5 GHz in Ka-band.

2-4 New approaches to spectrum sharing

Across Australia and around the world, demand for access to spectrum by new and increasingly sophisticated wireless technologies such as 5G cellular networks and IoT applications continue to put pressure on the current spectrum management strategies. Motivated by the observation that localised temporal and geographic spectrum is significantly under-utilised[18], dynamic spectrum access (DSA) based spectrum sharing is fundamental to effective spectrum management and a key tool in maximising the benefits achieved through use of the spectrum resource. Some government regulators such as the Federal Communications Commission (FCC) in US and Ofcom in UK have proposed the specific DSA framework, where secondary users monitor, identify, and exploit instantaneous spectrum opportunities with no or limited interference to primary users (PUs). Industry and standardization initiatives, under the auspices of major regulatory agencies, have mobilized to bring such management concept into standardization, including early standard version of IEEE 802.22 and new standards such as IEEE 802.11af and ECMA 392. It is worth noting that the above standards have been designed for the specific TV white space, where a device can obtain an available channel list from TV white space database.

Due to technological constraints such as hidden node problems and interference control, the DSA implementations to date is still in its infancy. The government regulators will continue to monitor technical developments, investigate and implement DSA when and where appropriate.

[18] M. McHenry, “NSF spectrum occupancy measurements project summary,” Shared Spectrum Co., tech. rep., Aug. 2005.

3 Transmission and Core Networks

3-1 Cloud Architecture

In order to support various IoT services, the NB-IoT and LTE-M, will continue evolving as part of the 5G specifications. The NB-IoT andthe LTE-M target on providing IoT services with low cost, long battery life, large coverage and high capacity. On the other hand, the 5G cellular system adopt the software-defined networking (SDN) and Network Function Virtualization (NFV) for the underlying physical infrastructure, which cloudifies the access, transmission, and core networks. The cloud structure of the 5G system separates user plane and control plane, allowing the operator to generate flexible network slices to fulfil the requirements of different IoT applications[19]. Due to the vast connectivity, low latency and high reliability provided by the 5G, it is foreseeable that in the near future, e.g., 2-5 years, the cloud architecture of 5G, with the existing NB-IoT and LTE-M technologies, is likely to dominate the IoT services.

3-2 Fog Architecture

The requirements of many new emerging IoT services, such as industrial control systems and autonomous vehicles, may not be fulfilled with the existing cloud structure. Specifically, the industrial control systems require very low latency within a few milliseconds [20]. The autonomous vehicles require a large network bandwidth, which was estimated to reach one gigabyte per second for each vehicle[21]. Moreover, the number of IoT devices is expected to reach 26 Billion by 2020, and there will likely be hundreds, or even thousands of IoT devices in any building in the future, creating a significant traffic flow. These stringent requirements fall far outside the current cloud architecture of 5G can achieve. Recently, a new concept of fog architecture is proposed with the functionalities such as computing, storage, control and networking distributed the edge of the IoT networks[22]. This is because sending all the data to the cloud requires excessive high bandwidth and high costs. More importantly, it is often unnecessary to deliver all the data to the cloud and approximately 90% of the data can be stored and processed locally[23]. To enable the fog architecture, the current transmission and core networks need to be altered from a centralised to a distributed architecture. Small data centres will be built at the edge of the IoT networks. Fog architecture is appealing to IoT services because of its cognition, efficiency, agility and low latency. It is foreseeable that the fog architecture will be dominant in the future, e.g., in 10 years.

3-3 Opportunities and Challenges

There are several opportunities in the development of fog architecture for transmission and core networks. Firstly, the universities in Australia have a solid research background in both

---

[19] Huawei Technologies Co., Ltd., "5G network architecture, a high-level perspective," 2016. Online: https://www.huawei.com/minisite/hwmbbf16/insights/5G-Nework-Architecture-Whitepaper-en.pdf

[20] Weiner, Matthew, Milos Jorgovanovic, Anant Sahai, and Borivoje Nikolié. "Design of a low-latency, high-reliability wireless communication system for control applications." In 2014 IEEE International conference on communications (ICC), pp. 3829-3835. IEEE, 2014.

[21] L. Mearian. "Self-Driving Cars Could Create 1GB of Data a Second". Online: http://www.computerworld.com/article/2484219/emerging-technology/self-driving-cars-could-create-1gb-of-data-a-second.html

[22] Chiang, Mung, and Tao Zhang. "Fog and IoT: An overview of research opportunities." IEEE Internet of Things Journal 3, no. 6 (2016): 854-864.

[23] R. Kelly. "Internet of Things Data to Top 1.6 Zettabytes by 2022". Online: https://campustechnology.com/articles/2015/04/15/internet-of-thingsdata-to-top-1-6-zettabytes-by-2020.aspx

Information Technology and Communication, which provides a fundamental resource. Secondly, Australia is expected to create the next “Youtube” or “Facebook”. This cannot be realised with the lack of fundamental infrastructure, such as the fog architecture. At last, the IoT market will rise continuously and reach a total value of $300 billion dollars by 2020[24]. Economic and commercial opportunities can be generated in developing the IoT infrastructure.

However, the development of the fog architecture for the transmission and core networks also face many challenges. The fog interface with the existing cloud architecture should be well defined and studied. The fog architecture should be compatible with the existing cloud architecture. Besides, distributed systems are more vulnerable to attacks than centralised systems. The security is another challenge in the development of the fog architecture. At last, there are currently no off-the-shelf edge devices for the fog architecture. Those network devices are more powerful and diverse than the existing network devices for the cloud architecture. The development of fog network devices can be challenging.

4 Interoperability

The IoT enables ubiquitous connection and automated monitoring and control for many devices that have sensing, processing, and communication capabilities to support various services. In the development of the IoT networks, one of the major problems is the integration of heterogeneous objects[25], i.e. the interoperability. Interoperability is defined by the IEEE as “the ability of two or more systems or components to exchange information and to use the information that has been exchanged”[26]. In the following, we focus on the interoperability because it appears to be a bottleneck in the large-scale deployment of the IoT.

4-1 Lack of Interoperability

Improving the interoperability of the IoT networks is crucial. Big vendors, such as Amazon, Cisco, IBM, Apple, etc., have dominated the IoT market in the recent years. However, they all use different IoT platforms and each of these platforms has its own protocols and interfaces, which are not compatible with each other. According to the European project Unify-IoT, there are more than 300 IoT platforms existing in the IoT market[27]. The lack of interoperability causes multiple problems in IoT networks, including vendor lock-in, difficulty in plugging IoT devices to non-compatible platforms, and the lack of cross-platform and cross-domain IoT applications[28].

4-2 Opportunities and Challenges

The interoperability of IoT can be achieved by the development of a universally accepted standard, such as the TCP/IP standard in the computer network. Interoperability offers opportunities in the IoT market, and it is stated that 40% of the potential benefits of the IoT

---

[24] Gartner Inc., “Forecast: The internet of things, worldwide”, 2013. Online: http://www.gartner.com/newsroom/id/2636073

[25] Vega-Barbas, Mario, Diego Casado-Mansilla, Miguel A. Valero, Diego López-de-Ipina, José Bravo, and Francisco Flórez. "Smart spaces and smart objects interoperability architecture (S3OiA)." In 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, pp. 725-730. IEEE, 2012.

[26] Radatz J, Geraci A, Katki F (1990) IEEE standard glossary of software engineering terminology. IEEE Std 610121990(121990):3.

[27] Unify-IoT project, BDeliverable D03.01 Report on IoT platform activities - UNIFY-IoT, 2016.

[28] Noura, Mahda, Mohammed Atiquzzaman, and Martin Gaedke. "Interoperability in internet of things: Taxonomies and open challenges." Mobile Networks and Applications 24, no. 3 (2019): 796-809.

can be obtained with the interoperability[29]. However, the development of interoperability is challenging and requires efforts from both academia and industry, i.e., different universities and vendors working together. Note that it is hard for the vendors and the existing platforms to reach an agreement due to their self-interests. It is predicted that in the near future, e.g., 2-**5** years, several interfaces between big IoT platforms will be developed to improve the interoperability. A universal and globalised standard for the IoT network is expected to finalise in 10 years.

Different universities and vendors need to collaborate to overcome this hurdle. Also, additional standard bodies can be founded. For policy makers, new policies may need to balance the interests for different vendors to make them easier in shifting from the current platform to a globalised platform.

5 Data Analyses and Management

Although the IoT has created unprecedented opportunities to increase revenues, reduce costs, and improve efficiencies, collecting a huge amount of raw data alone is insufficient. To derive benefits from the IoT, it is necessary to leverage a big data platform that can manage diverse data sources and analyse a massive volume of sensor data in a scalable and cost-effective manner. Data management and analytics allow organisations to transform big data into valuable insights, thereby revolutionising their business processes through intelligent decision-making techniques. For example, analysing the smart transport data can smooth the traffic, improve road safety, and enhance end-to-end user experience in terms of delivery time. In smart grids, the analysis of smart grid data can enable grid operators to know which parts of the electricity load and power frequency are inefficient, and which lines are faulty.

5-1 Key Requirements

The requirements of big data and analytics in the IoT have exponentially increased over the years and promise dramatic improvements in decision-making processes. Several key requirements for big data analytics in the IoT environment can be summarised as follows. The priority is to provide a reliable and seamless connectivity to facilitate the combination and integration of huge volumes of machine-generated sensor data. The second element involves the efficient storage technique to handle very large amounts of unstructured data in low-cost hardware on a real-time basis. Third, due to a variety of system protocols of wired, wireless and hybrid type in a dynamic networking environment, the IoT presents different quality of service (QoS) requirements from conventional homogeneous networks. Integrating the QoS architecture into IoT is another key requirement for efficient data analytics. Finally, streaming analytics has rapidly emerged as a key IoT initiative for timely decision-making processes. Big data implementations should perform analytics with real-time queries to help organisations obtain insights quickly, rapidly make decisions, and interact with people and other devices.

5-2 Big Data Analytics Platforms

There are several big data processing and analytics platforms suitable for large amounts of IoT-generated data. Hadoop[30] is an open source data processing platform that stores and

[29] Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J, Aharon D (2015) The internet of things: mapping the value beyond the hype. McKinsey global institute. McKinsey Glob Inst 3.

[30] Nandimath, Jyoti, Ekata Banerjee, Ankur Patil, Pratima Kakade, Saumitra Vaidya, and Divyansh Chaturvedi. "Big data analysis using Apache Hadoop." In 2013 IEEE 14th International Conference on Information Reuse & Integration (IRI), pp. 700-703. IEEE, 2013.

processes large amounts of data on a cluster of commodity hardware. As the core components, Hadoop Distributed File System (HDFS) is used to store the data, while MapReduce is used to process these data in a distributed manner. Another famous platform is 1010data[31], which provides advanced analytic services for large-scale infrastructure, including optimisation and statistical analysis. In addition, SAP-Hana[32] and HP-HAVEn[33] can also be used as big IoT data platforms.

5-3 Open Challenges

One of the major challenges for IoT data analytics lies in security issues. The attacks such as massive DDOS can have devastating effects on the businesses of many critical industries, threaten national security, and even directly or indirectly affect human lives. Therefore, solving these security issues must be given priority in the IoT realm. IoT security needs to move from single products to end-to-end solutions and eventually to the entire security architecture.

6 Hardware and Software capabilities

Sensor networks detecting rare events, such as a fire or an intrusion, must be both sensitive and selective, such that no important events are missed yet no false alarms are triggered[34]. In parallel, developments in materials science and sensor technologies are also driving a new wave of customized health, providing clinicians and patients with access to personalised data and diagnostics on the spot, at the point of care[35].

6-1 Hardware Capabilities

Advances in the Industrial Internet are accelerating the development of future IoT through an increase in the network agility, integrated artificial intelligence (AI) and the capacity to deploy, automate, orchestrate and secure diverse use cases at hyperscale. One of the basic requirements for the above is to have the capacity for millions of devices, machines, and computers to talk each other, sometimes across large distances. For this to happen, three future types of base technology are needed to create the hardware infrastructure on which the IoT can flourish: low-cost-low-power ultra-secure hardware sensors and ubiquitous connectivity devices[36].

1) Low-cost, Low-power Ultra-secure Hardware

Increasingly actuators and sensors are being embedded in various hardware as 'things' are explicitly designed to function within the IoT. With the cost of core sensor component, microelectromechanical systems (MEMS), dropping significantly every year, the IoT hardware segment is rapidly increasing in sophistication in terms of sensor capabilities, battery life,

---

[31]Morabito, Vincenzo. "Managing change for big data driven innovation." In Big Data and Analytics, pp. 125-153. Springer, Cham, 2015.

[32] Färber, Franz, Sang Kyun Cha, Jürgen Primsch, Christof Bornhövd, Stefan Sigg, and Wolfgang Lehner. "SAP HANA database: data management for modern business applications." ACM Sigmod Record 40, no. 4 (2012): 45-51.

[33] S. Burke, Hp haven big data platform is gaining partner momentum, CRN (2013). Online: http://www.crn.com/news/applications-os/240161649

[34] NICTA 2015, "Enabling Business to Government Digital Interaction: A Report to the Australian Government", prepared for the Australian Taxation office, June 2015

[35] Commonwealth Scientific and Industrial Research Organisation 2017, "Distributed Ledgers: Scenarios for the Australian economy over the coming decades", Hanson RT, Reeson A, Staples M.

[36] McKinsey&Company, "The Internet of Things: Mapping the Value beyond the Hype", 2015

security and processing power. In term of sensor capabilities, we expect to have a cheap unified sensor that monitors everything instead of having a bunch of sensors, each performing a single measurement, throughout an area. That is, digitally networked sensors can measure several variables. While there has been enormous interest in using ambient energy [37] to recharge capacitors or batteries, from solar to vibration, pressure, thermal differentials, and various other sources, the lifespan of rechargeable batteries has been the gating factor, expected to be resolved in the future. New state-of-the-art security approaches by using encryption keys and secured protocols such as Blockchain or quantum cryptography[38][39] will be integrated in the design of IoT hardware sensors to further enhance the current hardware security. Future intelligent sensors will require a computational processing unit to make decisions within a small amount of delay and without sending information back to the cloud data centre. This requirement will be fulfilled by the development of hardware sensors with integrated computational processing power provided by a graphical processing unit (GPU) by big vendors[40].

2) Connectivity Devices

There are many connectivity options available across different network types. These connectivity technologies range from emerging networks such as Sigfox, LoRa and NB-IoT to well established ones such as WiFi and 4G to the latest deployments such as 5G. Telstra and Thinxtra (the Sigfox licensee in Australia) are currently the leading IoT connectivity providers in the Australian market, with Telstra presently dominating given the strong coverage advantage of their 4G cellular footprint. To date, the hardware for these connectivity devices are locked into predefined connectivity types. Further, these devices have proprietary interfaces and design, limiting flexibility in configurations and customisation employed by different vendors. Revoking hardware proprietary characteristic will allow the use of huge volumes of actionable applications or user data to automate diverse IoT communication network processes. Expect in the future to have a fully open IoT connectivity hardware devices equipped with completely open connectivity interfaces for different connectivity reconfigurations and to make communication network decisions[41].

6-2 Software Needs and Systems Integration

Two capabilities will be required in the future, software to make sense of data and multi-system interoperability to allow seamless multiple system integrations. First, the real value of IoT applications comes from analysing data from multiple sensors and making decisions based on those data. This depends on advances in predictive analytics such as algorithms that can predict a heart attack before it happens based on subtle changes in patient data recorded by home health monitors, or software that can predict when a piece of industrial equipment requires maintenance before it fails. Today, analytics software has not progressed to the point where it can be easily applied in every case—one reason that so much of the data

[37] Jeff Briner, IoT for all, Energy Harvesting for IoT Devices, 2019. Online: https://www.iotforall.com/energy-harvesting-iot-devices/

[38] Patrick Nelson, Network World, Quantum-embedded chips could secure IoT, 2019. Online: https://www.networkworld.com/article/3333808/quantum-embedded-chips-could-secure-iot.html

[39] Steven Mcgrath, Hackernoon, Resolving IoT Security Issues with Blockchain Technology, 2019. Online: https://hackernoon.com/resolving-iot-security-issues-with-blockchain-technology-3ffb36357094

[40] Janakiram MSV, The New Stack, NVIDIA Brings Affordable GPU to the Edge with Jetson Nano, 2019. Online: https://thenewstack.io/nvidia-brings-affordable-gpu-to-the-edge-with-jetson-nano/

[41] Isolani, Pedro Heleno, Maxim Claeys, Carlos Donato, Lisandro Zambenedetti Granville, and Steven Latré. "A Survey on the Programmability of Wireless MAC Protocols." IEEE Communications Surveys & Tutorials 21, no. 2 (2018): 1064-1092.

that is collected goes unused. The hard work of developing and tuning these algorithms for the peculiarities of specific use cases is largely still undone, and the skills and capabilities to do this work remain in short supply[42].

Secondly interoperability between different IoT systems is required to capture the complete behaviour of most available or future IoT devices. Unfortunately, at the moment most of these systems are often not interoperable. There are many barriers to interoperability, including lack of common software interfaces, standard data formats, and common connectivity protocols. One potential path to overcoming these hurdles is to create common technology open standards. Industry associations, technology suppliers, and policy makers have started to collaborate to create such standards (e.g., Open Connectivity Foundation (OCF) forum etc.). Translation/aggregation platforms, including common application programming interfaces (APIs), are also needed to manage communication among different applications. Expect these standards to make big impacts in the development of IoT software of the future.

6-3 Opportunities and Challenges

The IoT hardware and software market is well served by overseas players. With Australia's engineering and manufacturing base limited in terms of skills and scale, focusing on IoT hardware design and manufacturing at scale is not likely to be a successful strategy for Australian stakeholders. Furthermore, significant global competition and advances in manufacturing, but also increasingly scale, have significantly reduced the prices of these components over the last two decades. For example, in 2004 the average cost of a sensor was $1.30; in 2020 it is expected to be just $0.38. Expect the eroding prices to continue, quickly driving commoditisation of the IoT hardware segment, offering little commercial opportunities. There may, however, be opportunities for local start-ups and some incumbents in the development of specific IoT hardware and software that supports specific industries where Australia has expertise (e.g. agriculture, healthcare) or global scale (e.g. mining)[43].

The development of specialised IoT devices for cities and regions that supports the above-mentioned industries will results in major technology development that will transform 'vertical' industry productivity, innovation and business opportunities. The IoT offers Australia significant and economic and environmental benefits by embedding intelligence in the critical infrastructure and assets and therefore making cities and regions smart. Here emerging disruptive technologies such as open data, analytics, mobile, cloud, social media, "crowd sourcing" (e.g. Kickstarter) and the "sharing economy (e.g. Uber, AirBnB), are enabling cities to embrace smarter ways to design, build and operate their critical infrastructure, provide new citizen centric services and create new industries. This translates into an opportunity for the Australian economy of up to AUD$120 billion by 2025 – however this is contingent upon strong collaborations between industry, academia and government agencies to innovate rather than being a technology user on the assumption that taxpayers' money is not being wasted[44].

---

[42] McKinsey&Company, "The Internet of Things: Mapping the Value beyond the Hype", 2015. Online: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx

[43] Australian Computer Society and PricewaterhouseCoopers Consulting (Australia) Pty Limited, "Australia's IoT Opportunity: Driving Future Growth", 2019. Online: https://www.acs.org.au/content/dam/acs/acs-publications/ACS-PwC-IoT-report-web.pdf

[44] IoT Alliance Australia, "IoT and Government's Role in the Development of Cities", July 2017. Online: https://www.aph.gov.au/DocumentStore.ashx?id=229cdb32-7586-4867-8e40-d43158edf35f&subId=514420