Survey on Internet of Things (IoT)

Name: Jiayu Wang

Student ID: 1039580

Username: WAJW4

Abstract

With the rapid development of IoT these years, there are increasing numbers of approaches in progress regarding every aspect of this field. This survey will involve the basic architecture of IoT, main protocols and technologies in IoT.

Introduction

Concept of IoT

The concept of Internet of Things (IoT) was first proposed in 1999 by Auto-ID Research Center under the Massachusetts Institute of Technology（MIT)[1]. The initial meaning of IoT was the connection of all items within the Internet through radio-frequency identification (RFID). What noteworthy is, the current concept of IoT has overturned traditional thinking by integrating the IT infrastructure and basic physical facilities into one and also no longer exclusively refers to RFID-based wireless sensor networks. IoT now can be supported by RFID, infrared sensors, GPS, laser scanners and other information sensing equipment.

Evolution of IoT

With the rapid development of Internet technology, the applications of Internet connectivity have become more ubiquitous and affordable. Nowadays devices have better processing and storage capability while in a more portable size, which is easier to be equipped with sensors and actuators.[2] Furthermore, physical items are more tagged by IoT technologies, for example, QR code and RFID tags, and smart devices like smartphones and tablets equipped with 'tag' readers can scan them. Such a combination of physical reality and virtual network enables IoT to be derived from the Internet.

The relationship between IoT and the Internet

IoT can be considered as an extension of the Internet. Apart from networks in the Internet, IoT additionally involves different types of sensor and actuator networks, especially wireless sensor networks (WSNs) [3]. The essence of the IoT is still the Internet, though the terminals are no longer computers as on the Internet but an embedded computer system with supporting sensors.

Impact of IoT

The terminology of “Things” in “Internet of Things (IoT)” extensively includes a wide range of physical items in many different fields, for example, personal smart devices, environmental elements and other electronic appliances able to connect to the Internet. In this way, the connectivity pattern has been transformed from “anytime, anywhere” for “anyone” to “anytime, anywhere” for “anything”[4].

Related work

3-layer architecture

There are various architectures of IoT with different layer models. Here, we will focus on the most basic 3-layer architecture (**Figure 1**), which includes the perception layer, network layer and application layer[5].

The perception layer is the physical layer to perform data acquisition in both the human and physical worlds. It consists of two major parts, basic sensor devices (various types of sensors, RFID tags and readers, GPS, etc) and the network of sensors (such as sensor network, RFID network, etc.).

The network layer, also known as the transmission layer, is to perform the transmission of data obtained by the perception layer, within a certain range (usually long distances). Its main function is access and transmission. Thus, the network layer can be considered as a data pathway for information exchange and transmission.

The application layer, also known as the processing layer, performs information processing and addresses the human-machine interface issues. Data transmitted from the network layer are processed in various information systems under this layer and interacts with people through various devices.

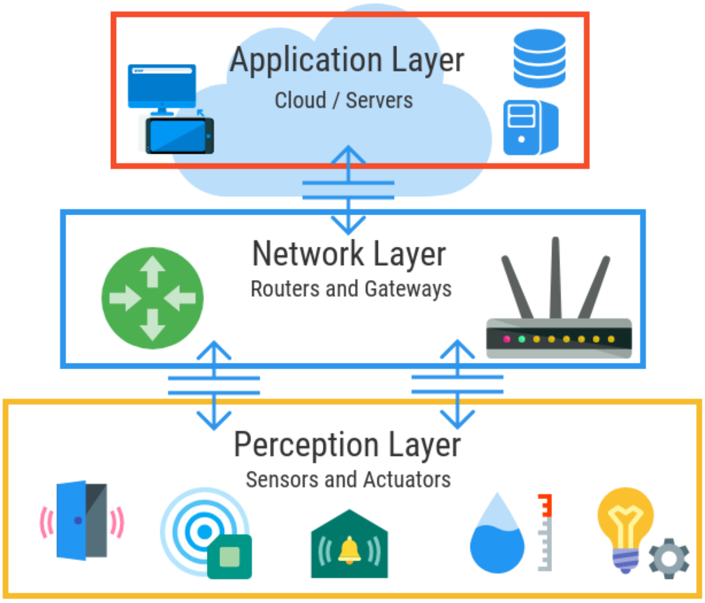


Figure 1. A schematic diagram for IoT 3-layer architecture [1]

Major IoT protocols

As shown in **Figure 2**, a sample IoT space involves communication environments like Ethernet, Wi-Fi, RFID, NFC (Near Field Communication), Zigbee, etc[6]. Each of the communication application protocols has a certain range of applicability, which are used in different networks or for different types of devices. There are various application-layer IoT protocols currently used, such as REST/HTTP, CoAP, MQTT, DSS, XMQP, AMQP, JMS, etc. In this section, I will focus on CoAP and MQTT. These two are lightweight and suitable for embedded devices and hence are frequently used in Machine-to-Machine (M2M) communication.

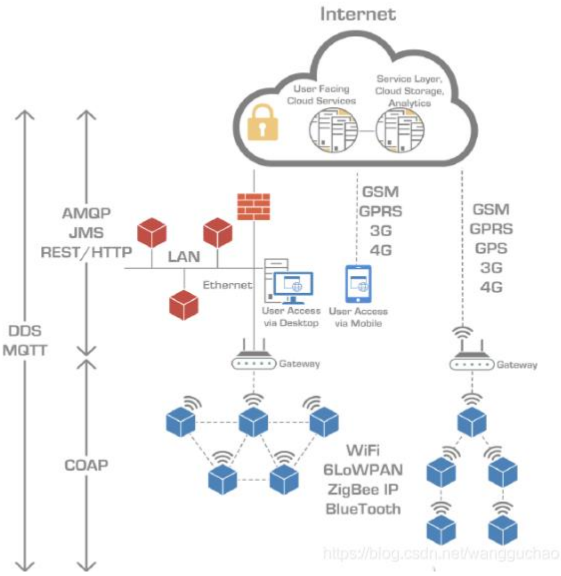


Figure 2. A schematic diagram for IoT connectivity space [6]

MQTT (Message Queuing Telemetry Transport) [8], developed by IBM, is a messaging protocol on the application layer. MQTT is mainly based on a topic-specific publish/subscribe architecture and all IoT terminals are connected to the cloud via TCP protocol **(Figure 3)**. Here 'topic-specific publish/subscribe' means the clients that have subscribed to a certain topic can receive all the messages published under this topic. MQTT can use minimal code and limited bandwidth to provide reliable real-time messaging services for those remotely connected devices, which is suitable for resource-constrained devices. MQTT protocol is lightweight, sample, and easy to implement due to its features.

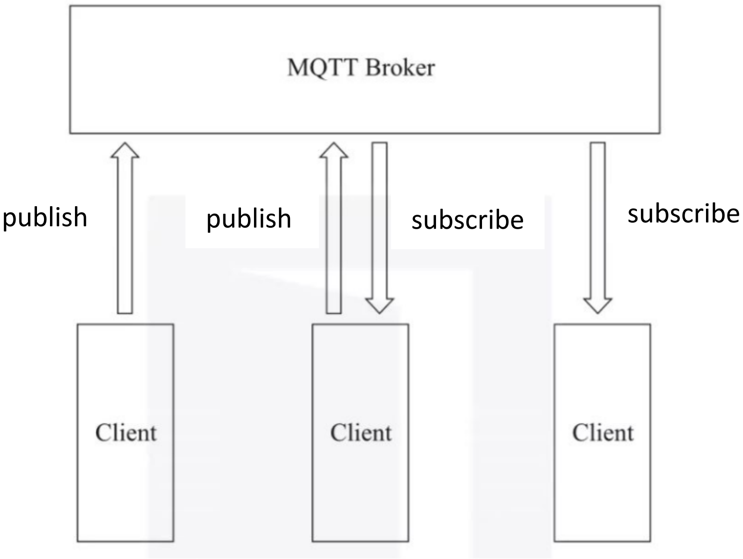


Figure 3. 'Topic-specific publish/subscribe' in MQTT

CoAP (Constrained Application Protocol) is another application-layer protocol that runs on resource-constrained devices, which is generally run over UDP protocol[7]. CoAP is also designed quite lightweight with a minimum packet size of only 4 bytes. CoAP uses a C/S architecture with a request/response interaction pattern that is similar to HTTP. Meanwhile, CoAP provides an observation mode where an observer can indicate the observed entity object to the CoAP server via the OBSERVE command. Similar to the subscription feature in the MQTT protocol, the observer in CoAP receives an update on the state of the entity object if any change happens. The communication model of the CoAP protocol is shown in **Figure 4**.

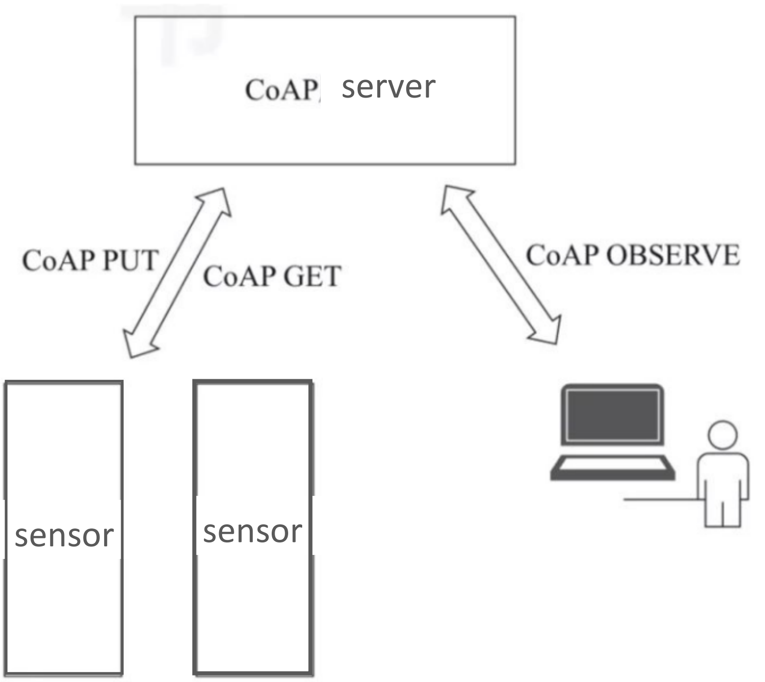


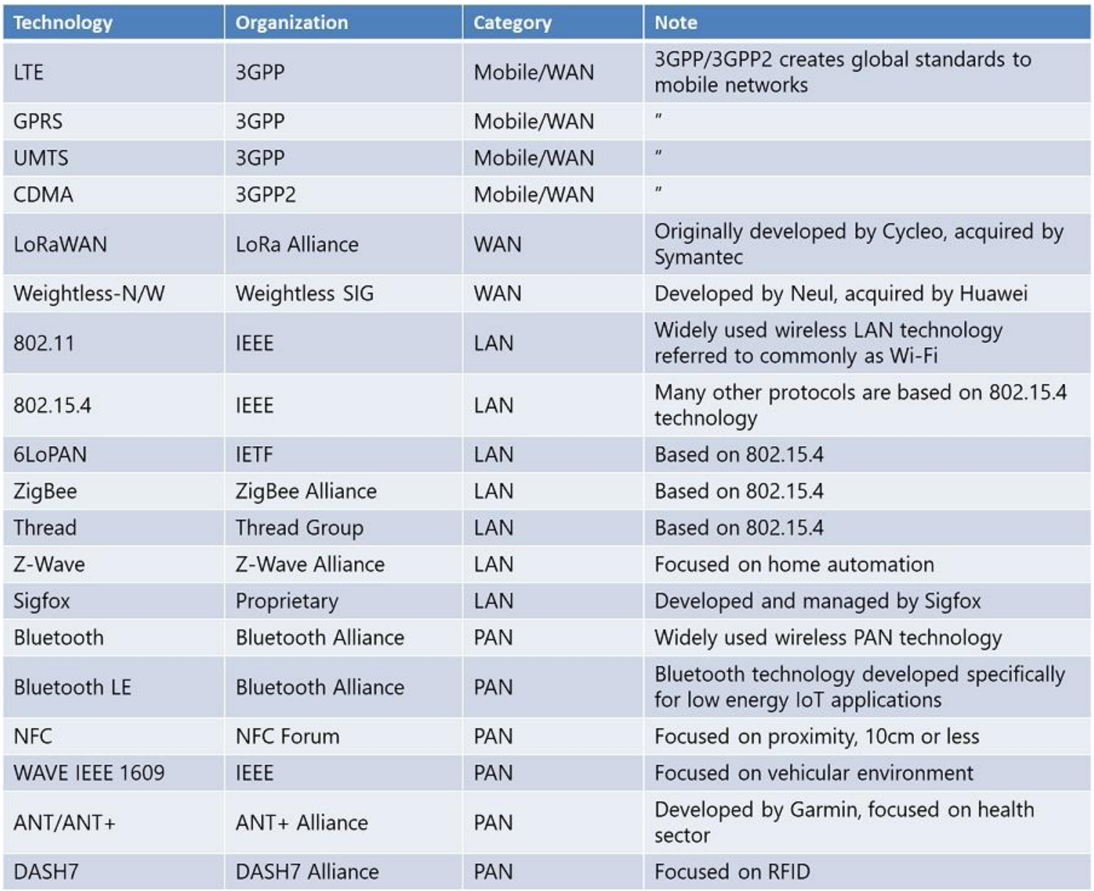
Figure 4. Communication model in CoAP

Network communication technologies currently used in IoT

The four core technologies of the current IoT generally include RFID, sensors, cloud computing, and network communication[8]. Under each core technology are numbers of sub-technologies which cannot cover in one report. Thus, this survey will mainly look into commonly used wireless communication technologies.

According to the classification by TAC (Technological Advisory Council) in 2015, main wireless IoT technologies and classifications are shown in **Table 1**. Here, we only look into several most used wireless IoT technologies.

Table 1. Main wireless technologies and classifications in IoT



Technology	Organization	Category	Note
LTE	3GPP	Mobile/WAN	3GPP/3GPP2 creates global standards to mobile networks
GPRS	3GPP	Mobile/WAN	″
UMTS	3GPP	Mobile/WAN	″
CDMA	3GPP2	Mobile/WAN	″
LoRaWAN	LoRa Alliance	WAN	Originally developed by Cycleo, acquired by Symantec
Weightless-N/W	Weightless SIG	WAN	Developed by Neul, acquired by Huawei
802.11	IEEE	LAN	Widely used wireless LAN technology referred to commonly as Wi-Fi
802.15.4	IEEE	LAN	Many other protocols are based on 802.15.4 technology
6LoPAN	IETF	LAN	Based on 802.15.4
ZigBee	ZigBee Alliance	LAN	Based on 802.15.4
Thread	Thread Group	LAN	Based on 802.15.4
Z-Wave	Z-Wave Alliance	LAN	Focused on home automation
Sigfox	Proprietary	LAN	Developed and managed by Sigfox
Bluetooth	Bluetooth Alliance	PAN	Widely used wireless PAN technology
Bluetooth LE	Bluetooth Alliance	PAN	Bluetooth technology developed specifically for low energy IoT applications
NFC	NFC Forum	PAN	Focused on proximity, 10cm or less
WAVE IEEE 1609	IEEE	PAN	Focused on vehicular environment
ANT/ANT+	ANT+ Alliance	PAN	Developed by Garmin, focused on health sector
DASH7	DASH7 Alliance	PAN	Focused on RFID

Bluetooth/Bluetooth Low Energy (BLE)

Bluetooth and Bluetooth Low Energy (BLE) are wireless technologies used within a short distance[9]. Its basic mechanism is to perform data transmission by UHF radio waves, which was standardized by IEEE 802.15.1. Currently, this technology is frequently applied to connect small devices to smartphones or tablets. For instance, many speaker systems use embedded Bluetooth modules. BLE is less powerful than Bluetooth, so it can perform data transmission data without consuming much power of the user's smartphone, and hence suitable for phone-connected devices (such as smartwatches, running trackers).

ZigBee

ZigBee is a two-way wireless communication technology based on the IEEE802.15.4 protocol[10]. It is a short-distant technology with a low transmission rate, low power, and low cost. Besides, Zigbee is of low latency and low duty cycle, which enables a maximum battery life for products. ZigBee protocol provides 128-bit AES encryption and supports mesh networks. The technical standards of Zigbee were not consistent with each other in the early days. But now great improvements regarding interoperability and compatibility have been made in the latest version Zigbee 3.0. Hence, Zigbee is frequently applied to locator devices and is also widely used in auto-control and remote-control industries.

NB-IoT

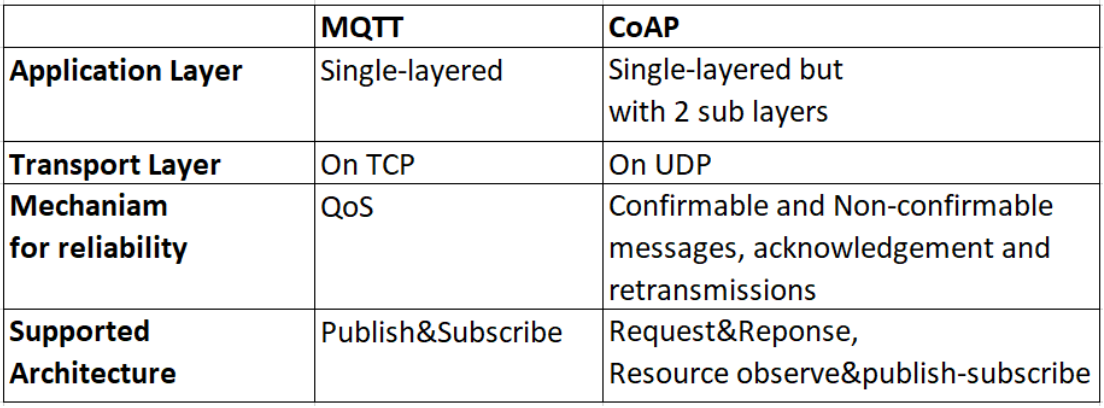
NB-IoT (Narrow Band Internet of Things) is a cellular-based narrowband IoT technology that was released in 2016 [11]. It is also called low-power wide area networks (LPWAs) since it can supports cellular data connectivity for devices with low power over WAN. The power of NB-IoT only occupies approximately 180 KHz of the frequency band. It can also be directly deployed in UMTS, GSM or LTE networks. The main features of NB-IoT are multiple connections and wide coverage with low power, low speed and well-designed architecture. These features are quite suitable for devices with a high network connectivity requirement as well as a short standby time.

Comparison of Key Approaches

Comparison of MQTT and CoAP

MQTT and CoAP are both communication protocols suitable for devices in IoT-constrained environments. They both can provide asynchronous transfer mode, both can run over IP, both are open standards, and both have a wide range of implementations. MQTT and CoAP are both widely used as IoT protocols, especially among small devices. But they are also quite different in some aspects as shown in **Table 2[12]**.

Table 2. Main differences between MQTT in CoAP



	MQTT	**CoAP**
Application Layer	Single-layered	Single-layered but with 2 sub layers
Transport Layer	On TCP	On UDP
Mechaniam for reliability	QoS	Confirmable and Non-confirmable messages, acknowledgement and retransmissions
Supported Architecture	Publish&Subscribe	Request&Reponse, Resource observe&publish-subscribe

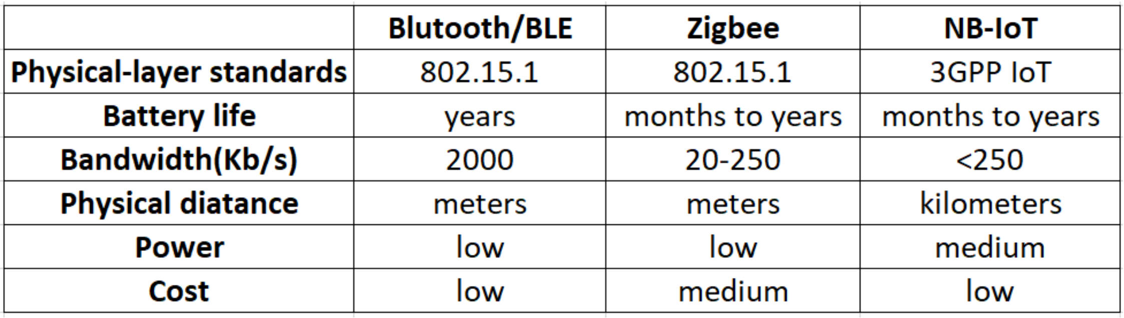
Besides, there are other differences in the application. As a many-to-many communication protocol, MQTT is commonly used in scenarios that transferring data between many clients through proxies. Though MQTT supports persistence to some degree, it is better used as an immediate data transfer bus. The most widely used peer-to-peer protocol is CoAP, a protocol can transfer real-time status between the client and the server. Though CoAP supports observation on its transferring data, it is more based on a status-transfer model instead of only based on events.

From the perspective of the current trend in IoT application development, MQTT has more advantages than CoAP due to the ‘first-mover’ advantage. Now major global cloud computing service providers, such as AWS, Azure, Aliyun, all support MQTT. However, future IoT application platforms are most possible to be compatible with more kinds of IoT application-layer protocols.

Comparison of Bluetooth/Bluetooth Low Energy (BLE), Zigbee and NB-IoT

According to the features of these three technologies, here we summarize the differences between them as shown in **Table 3** for the comparison purpose.

Table 3. Differences between Bluetooth (BLE), Zigbee and NB-IoT



	Blutooth/BLE	Zigbee	NB-IoT
Physical-layer standards	802.15.1	802.15.1	3GPP IoT
Battery life	years	months to years	months to years
Bandwidth(Kb/s)	2000	20-250	<250
Physical diatance	meters	meters	kilometers
Power	low	low	medium
Cost	low	medium	low

Conclusions and Future Directions

With the development of IoT technologies, the technical bottleneck in this field, such as energy supply, has been gradually overcome. The emergence of digital technologies such as blockchain, big data, cloud platforms, and 5G has brought the IoT to the next level. Also, technologies on different layers have started to form a unified standard, which accelerates the popularity and commercialization of IoT applications. Current IoT applications involve areas such as logistics, construction, transportation, security, energy, medical, manufacturing, home, retail and agriculture, especially the smart home area[13].

There are many possibilities for the future of IoT, here we will only talk about predictions in several aspects. First, the standardization in IoT will be realized in the near future. Standardization is the most effective solution to reduce the gaps between protocols to achieve interoperability across terminals, services and applications [14]. In this way, different roles under the IoT economy, namely, developer, regulator and users can all get benefit within a reasonable time. Secondly, the security issue in the IoT environment will be paid more attention to. There will be more advanced IoT security software developed, and hardware-level security measures will be focused on, especially for applications that handle sensitive data. Thirdly, there will be easier access to IoT. With the advent of 5G, access to IoT by mobile devices will increase and more IoT data will be accessed by more people. In the future, the development of IoT will be transformed towards making better use of the data collecting and processing technologies, rather than just focusing on the IoT technologies itself.

Reference

[1] N. Gershenfeld, *When Things Start to Think*: Henry Holt and Co., Inc., 1999.

[2] R. Khan, S. Khan, R. Zaheer *et al.*, *Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges*, 2012.

[3] A. Badach, "Internet of Things – IoT," 2014.

[4] L. Coetzee, and J. Eksteen, *Positioning Internet of Things Application, and Associated Human Behavioural Changes in a Developing Context*, 2012.

[5] G. Pujolle, "An Autonomic-oriented Architecture for the Internet of Things." pp. 163-168.

[6] T. Gomes, S. Pinto, T. Gomes *et al.*, *Towards an FPGA-based edge device for the Internet of Things*, 2015.

[7] C. Bormann, A. P. Castellani, and Z. Shelby, “CoAP: An Application Protocol for Billions of Tiny Internet Nodes,” *IEEE Internet Computing,* vol. 16, no. 2, pp. 62-67, 2012.

[8] M. Daud, Q. Khan, and Y. Saleem, "A study of key technologies for IoT and associated security challenges." pp. 1-6.

[9] K.-H. Chang, “Bluetooth: a viable solution for IoT?[Industry Perspectives],” *IEEE Wireless Communications,* vol. 21, no. 6, pp. 6-7, 2014.

[10] L. Jin-Shyan, “Performance evaluation of IEEE 802.15.4 for low-rate wireless personal area networks,” *IEEE Transactions on Consumer Electronics,* vol. 52, no. 3, pp. 742-749, 2006.

[11] M. Chen, Y. Miao, Y. Hao *et al.*, “Narrow Band Internet of Things,” *IEEE Access,* vol. 5, pp. 20557-20577, 2017.

[12] D. Thangavel, X. Ma, A. Valera *et al.*, "Performance evaluation of MQTT and CoAP via a common middleware." pp. 1-6.

[13] A. B. Pawar, and S. Ghumbre, "A survey on IoT applications, security challenges and counter measures." pp. 294-299.

[14] I. Ishaq, D. Carels, G. Teklemariam, J. Hoebeke, F. Abeele, E. Poorter, I. Moerman, and P. Demeester, “IETF Standardization in the Field of the Internet of Things (IoT): A Survey,” Journal of Sensor and Actuator Networks, vol. 2, no. 2, pp. 235–287, Apr. 2013.