Advanced Industrial SCIence
Vol. 2, No. 1, pp. 1-7, 2023

ISSN 2951-2476
https://doi.org/10.23153/AI-Science.2023.2.1.001

Research on Secure IoT Lightweight Protocols

Sunghyuck Hong
Professor, Division of Advanced IT, IoT major, Baekseok University

사물인터넷용 경량 프로토콜 비교 연구

홍성혁
백석대학교 첨단IT학부 IoT전공 교수

Abstract The use of Internet of Things(IoT) in smart cities and smart homes is essential. The security of the sensor nodes, which are the core of the IoT, is weak and hacking attacks are severe enough to have a fatal impact on real life. This research is conducted to improve the security of the Internet of Things by developing a lightweight secure communication protocol for the Internet of Things, and to build a safe Internet of Things environment suitable for the era of the 4th Industrial Revolution. It contributes to building a safe and convenient smart city and smart home by proposing key management and identifier development to increase the confidentiality of communication and the establishment of an Internet authentication system.

Key Words : IoT, Smart city, Smart home, Lightweight protocol, Security

요 약 스마트시티와 스마트 홈에서 사물인터넷의 사용이 필수적이다. 사물인터넷의 핵심인 센서 노드들에 대한 보안성이 취약하여 해킹공격을 받을 경우 실생활에 치명적인 영향을 미칠 만큼 심각하나, 사물인터넷을 구성하는 센서 노드들의 물리적 기술적 제약으로 인하여 보안모듈이 탑재되어 운영되지 못하고 있는 실정이어서 사물인터넷용 경량 보안 통신 프로토콜을 개발하여 사물인터넷의 보안성을 향상하고, 앞으로 4차산업혁명 시대에 맞는 안전한 사물인터넷 환경 구축을 위해 본 연구를 실시하며, IoT사물인터넷 인증체제 구축과 통신의 기밀성을 높이기 위한 키 관리 및 식별자 개발을 대한 제안을 하여 안전하고 편리한 스마트시티와 스마트 홈을 구축하는데 기여한다.

주제어 : 사물인터넷, 스마트시티, 스마트홈, 경량프로토콜, 보안

1. Introduction

1.1 Research Goal

In recent years, the keyword Internet of Things (IoT) has become a hot topic. Cisco estimates there will be 5 billion devices connected to its network in 2020. This is about 6.5 times the projected global population of 7.6 billion in 2020. Gartner predicts that the added value created by IoT will reach about $1.9 trillion by 2020. Cisco, Google, and Microsoft are accelerating the development of technologies to secure global competitiveness in IoT.

IoT is a technology that is the main axis of various services directly related to human life, such as smart home, smart medical care, smart

*This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2020R1F1A1048684).

*Corresponding Author : Sunghyuck Hong(shong@bu.ac.kr)

Received February 2, 2023 Revised February 28, 2023
Accepted March 20, 2023 Published March 20, 2023

car, smart energy, and smart factory. It is 'security'. This is because security threats in the IoT environment where everything such as people, things, space, and data are connected can threaten not only economic damage but also life and national infrastructure. They are jumping into the competition to secure technology. Representatively, Cisco has established and is operating a dedicated department (IoT systems and software group, IoT security group) to strengthen its IoT business and security capabilities. Cisco announced new key words such as Fog Computing and IoE (Internet of Everything), We are preparing for the IoT era very quickly, such as establishing specific plans to apply IoT to transportation systems. In addition, technology development such as an IoT security platform for IoT device protection is also very active. Intel acquired McAfee, a security specialist, and launched some products by mounting security solutions on Intel's IoT gateways. Verizon has developed security solutions for cloud-based IoT device identification, authentication, and communication data protection, and GE (General Electric) has also acquired security company Wurldtech and is developing security solutions for refineries, power grids, and medical devices.

1.2 Importance of This Research

Since IoT security is vulnerable, there is a possibility of invasion of privacy and, furthermore, a possibility of developing into a criminal target, so the development of a communication security protocol between sensors is very important. For example,

Fig. 1 shows an example of an IoT product/service in which a scale is connected to the Internet and can be linked with various analysis functions and various services.

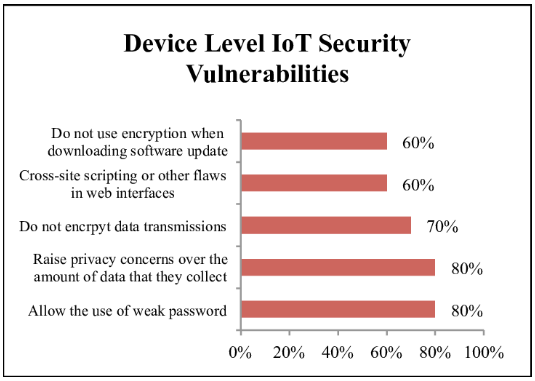

Fig. 1 Device Level IoT Security Vulnerabilities

The weight information measured by the user is transmitted to the service provider's cloud, and the user can check the information through an application on a terminal such as a smart phone. Although the mentioned flow of weight information seems simple and the service is simple, individual weight information can be used for a wide variety of services. For example, some IoT scales can upload measured personal weight information to SNS such as Twitter according to the individual's choice. Since this is open information, insurance companies can utilize the information to sell customized insurance products to users. In addition, if you are already an insurance subscriber, you may want to influence the user by recognizing the change in your health risk according to the change in your weight and worrying about your insurance loss. In addition, individual weight information stored in the service provider may be used for malicious purposes, and the service provider may convert it into other information with high added value from the viewpoint of the company through analysis/processing for its own benefit. In any case, since the data is used against the will of the original data owner, privacy infringement occurs. However, in this situation, if the user of the scale (the owner of weight information) wants to secure the right to control his/her information, it is questionable whether he can easily obtain the right to control his own information in the current IoT service environment. For instance, if a company processes the information it holds and sells it to a third party, the company that provided the information will no longer have control over the user's information after the sale. The processed information will remain stored in its original form. Since it cannot be regarded as information of weight, it cannot be seen that the first owner of weight information has control over the information in this case. So far, information processing and management has been carried out by a single company, and there has been no case where multiple subjects are involved like in the IoT environment, so the existing laws and systems related to privacy need to be rearranged to suit the new IoT environment. In addition to the aforementioned possibility of invasion of privacy, as shown in Fig. 1, if a malicious attacker intercepts the information sensed by the scale and transmitted through the wireless communication channel, the attacker uses the information to infer the user's physical characteristics, and it could be used for malicious purposes. Since many IoT devices and platforms do not implement high-level technologies in access control and authentication/authorization technologies, they are relatively vulnerable to attacks. If the scale has a motion sensor, an attacker can penetrate the weak security system and gain control over the sensor, making it easy to find out not only personal weight information but also whether or not you live in the house. As such, IoT products and services have special security and privacy issues, and because they are too broad, it is important to develop IoT security communication protocols at the national level.

2. Related Work

2.1 Lightweight Protocols

Lightweight protocols are communication protocols that are designed to be simple, efficient, and easy to implement, typically requiring less processing power, memory, and bandwidth compared to heavier protocols. They are often used in resource-constrained devices such as sensors, IoT devices, and low-power wireless networks. Here are some popular lightweight protocols that are commonly used for IoT and resource-constrained devices:

- MQTT (Message Queuing Telemetry Transport)
- CoAP (Constrained Application Protocol)
- XMPP (Extensible Messaging and Presence Protocol)
- AMQP (Advanced Message Queuing Protocol)
- LwM2M (Lightweight M2M)
- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks)

The choice of protocol depends on the specific requirements of your application and the devices that you are using. MQTT and CoAP are commonly used for IoT applications, while XMPP is often used for real-time communication and instant messaging. AMQP is a more comprehensive messaging protocol that is used for a variety of applications, including IoT. LwM2M is a specific IoT protocol for managing devices, while 6LoWPAN is used for low-power wireless networks [1-3].

2.2 MQTT, CoAP, and XMPP Protocols

MQTT is a lightweight publish-subscribe messaging protocol designed for IoT devices and networks with limited bandwidth and low-power capabilities. It uses a client-server architecture where clients (devices) connect to a server (broker) and subscribe to topics of interest. Fig. 2 shows the overview of MQTT protocol[5].

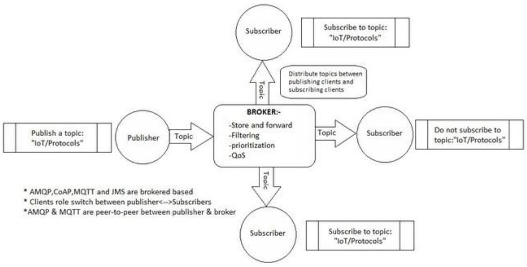
Subscriber
Subscribe to topic: "IoT/Protocols"
Topic
Distribute topics between publishing clients and subscribing clients
Publish a topic: "IoT/Protocols"
Publisher
Topic
BROKER:-
-Store and forward
-Filtering
-prioritization
-QoS
Topic
Subscriber
Do not subscribe to topic:"IoT/Protocols"
Topic
* AMQP,CoAP,MQTT and JMS are brokered based
* Clients role switch between publisher<-->Subscribers
*AMQP & MQTT are peer-to-peer between publisher & broker
Subscriber
Subscribe to topic: "IoT/Protocols"

Fig. 2. MQTT Overview

The clients can then publish data to these topics, and the broker distributes the data to all subscribers. MQTT is designed to be low overhead, efficient, and easy to implement, making it well suited for use in resource-constrained environments.

CoAP allows for device-to-device communication, as well as device-to-server communication, and can be used for a variety of IoT applications, including sensor networks and industrial automation. Like MQTT, CoAP is designed to be low overhead, efficient, and easy to implement, making it well suited for use in resource-constrained environments.

CoAP is a lightweight communication protocol for IoT devices and networks that are designed to be simple, efficient, and scalable [6]. It is based on the UDP (User Datagram Protocol) and is designed to support RESTful (Representational State Transfer) web services [7]. Fig. 3 shows CoAP protocol overview.

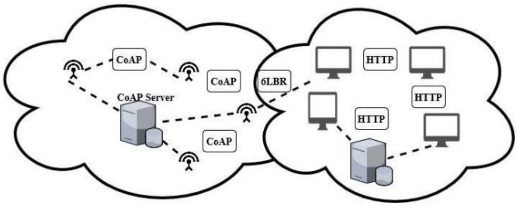

Fig. 3. Overview of CoAP Protocol

CoAP allows for device-to-device communication, as well as device-to-server communication, and can be used for a variety of IoT applications, including sensor networks and industrial automation. Like MQTT, CoAP is designed to be low overhead, efficient, and easy to implement, making it well suited for use in resource-constrained environments.

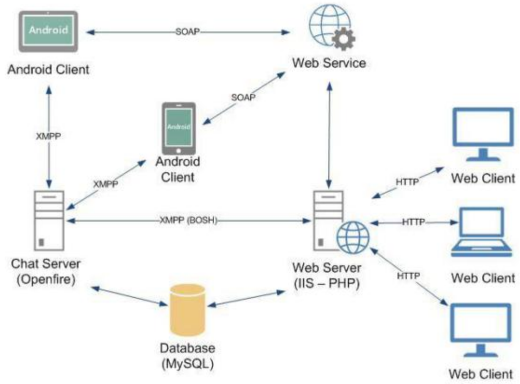

Fig. 4. Configuration of Extensible Messaging and Presence Protocol (XMPP)

XMPP is an open-standard, real-time communication protocol for instant messaging and presence information [8]. It was originally developed for instant messaging applications but has since been adopted for other use cases, including IoT. XMPP uses an XML-based data format for communication and is designed to be extensible, allowing for the development of new features and extensions. The protocol uses a client-server architecture, where clients (devices) connect to a server and exchange messages in real-time. XMPP supports a variety of communication modes, including one-to-one messaging, group chat, and publish-subscribe, making it well suited for use in a variety of IoT and real-time communication applications. Fig. 4 shows the brief overview of XMPP.

3. Proposed Lightweight Protocol

3.1. The most chanllenging in IoT Lightweight Protocols

There are several challenges associated with IoT lightweight protocols, including:

- Interoperability: Different IoT devices use different protocols, making it difficult for them to communicate with each other. This leads to the need for standardization and interoperability solutions.
- Bandwidth and Latency Constraints: IoT devices often operate on low-power networks with limited bandwidth and high latency. This makes it challenging to send large amounts of data or to use complex protocols.
- Security: IoT devices are vulnerable to various types of attacks, such as eavesdropping, tampering, and denial-of-service (DoS) attacks. Lightweight protocols must be secure enough to prevent these attacks and protect the privacy of users' data.
- Power Efficiency: IoT devices are often battery-powered and have limited energy resources. This makes it important to choose a lightweight protocol that minimizes power consumption and extends the device's battery life.
- Scalability: IoT is a rapidly growing field, and the number of devices is expected to increase dramatically in the coming years. Lightweight protocols must be scalable to accommodate this growth and accommodate the increasing number of devices.
- Reliability: IoT devices often perform critical functions and must be reliable. Lightweight protocols must be able to ensure that data is transmitted accurately and without errors, even in challenging network conditions.

Terminals and sensors used in the IoT service environment have limitations in their functions. In particular, in the case of various sensors or RFID(Radio Frequency Identification) tags, usable power and computational power are limited. Therefore, it is difficult to apply a high-level security technique applied to a general computing environment. Therefore, it is necessary to study an efficient security technique different from the existing techniques. In particular, IoT services are more exposed to the threat of information leakage by attackers because most of them communicate through wireless networks. Therefore, in order to minimize the threat of invasion of privacy that may occur in the step of authenticating people or objects when using IoT services, encryption of transmitted data must be preceded. In recent studies, it is necessary to standardize the encryption method for the IoT service environment in the future by analyzing various techniques for applying lightweight encryption and studying to achieve this in the standardization stage. ZigBee (English: ZigBee) is a standard technology for communication by configuring a personal communication network using a small, low-power digital radio. It was created based on the IEEE 802.15 standard. Zigbee devices use a mesh network method to transmit data to destinations through several intermediate nodes, enabling wide-range communication despite low power consumption. Due to the characteristics of an ad-hoc network, it is suitable for applications where there is no separate central node. Zigbee is used in applications requiring long battery life and security while only requiring low transmission rates. It has a transmission speed of 250 kbit per second, and is most suitable for data transmission for simple signal transmission such as periodic or intermittent data transmission or sensors and input devices.

Applications include wireless light switches, home power meters, traffic management systems, and other personal and industrial devices that require short-range, low-speed communications. The Zigbee standard was created to be relatively simpler and cheaper than other WPAN(Wireless Personal Area Network) technologies such as Bluetooth or Wi-Fi[9]. Zigbee network provides security using 128-bit symmetric key encryption. For home automation applications, the transmission distance ranges from 10 to 100 meters in line of sight, depending on output strength and wireless environment[10]. The concept of direct cost began in 1998, the first standard was established in 2003, and revised in 2006. The name Zigbee is derived from the bee dance performed by bees returning to the hive [11].

4. Conclusion

In conclusion, lightweight protocols play a crucial role in the Internet of Things (IoT) and are designed to meet the communication needs of resource-constrained devices and networks. They are designed to be simple, efficient, and easy to implement, typically requiring less processing power, memory, and bandwidth compared to heavier protocols. Examples of lightweight protocols include MQTT, CoAP, XMPP, AMQP, LwM2M, and 6LoWPAN. The choice of protocol depends on the specific requirements of the application and the devices being used. Lightweight protocols are helping to enable widespread deployment of IoT devices and are playing a key role in the growth and development of the IoT ecosystem.

REFERENCES

[1] Vinoski, S. (2006). Advanced message queuing protocol. *IEEE Internet Computing, 10(6),* 87-89.

[2] Rao, S., Chendanda, D., Deshpande, C., & Lakkundi, V. (2015, August). Implementing LWM2M in constrained IoT devices. *In 2015 IEEE Conference on Wireless Sensors* (ICWiSe) (pp. 52-57). IEEE.

[3] Verma, A., & Ranga, V. (2020). Security of RPL based 6LoWPAN Networks in the Internet of Things: A Review. *IEEE Sensors Journal, 20(11),* 5666-5690.

[4] KaiFang, F. (2009, August). Design and implementation of an instant messaging architecture for mobile collaborative learning. *In 2009 ISECS International Colloquium on Computing, Communication, Control, and Management* (Vol. 3, pp. 287-290). IEEE. DOI : 10.1109/CCCM.2009.5268060.

[5] Thangavel, D., Ma, X., Valera, A., Tan, H. X., & Tan, C. K. Y. (2014, April). Performance evaluation of MQTT and CoAP via a common middleware. *In 2014 IEEE ninth international conference on intelligent sensors, sensor networks and information processing* (ISSNIP) (pp. 1-6). IEEE.

[6] Naik, N. (2017, October). Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP. *In 2017 IEEE international systems engineering symposium (ISSE)* (pp. 1-7). IEEE. DOI : 10.1109/SysEng.2017.8088251

[7] Fernandes, J. L., Lopes, I. C., Rodrigues, J. J., & Ullah, S. (2013, July). Performance evaluation of RESTful web services and AMQP protocol. *In 2013 Fifth international conference on ubiquitous and future networks* (ICUFN) (pp. 810-815). IEEE.

[8] Saint-Andre, P., Smith, K., Tronçon, R., & Troncon, R. (2009). *XMPP: the definitive guide.* " O'Reilly Media, Inc.".

[9] Ramya, C. M., Shanmugaraj, M., & Prabakaran, R. (2011, April). Study on ZigBee technology. *In 2011 3rd international conference on electronics computer technology* (Vol. 6, pp. 297-301). IEEE.

[10] Park, E. J., & Song, J. H. (2022). A Study on the Design of Automatic Recording System for Discharge of Wastewater Discharge Facilities Based on Zigbee Communication. *Journal of the Korea Academia-Industrial cooperation Society, 23(9),* 607-612. DOI : 10.5762/KAIS.2022.23.9.607

[11] Yeo, J. S., Kim, B. S., Huh, K. S., H, M. R., & Choi, H. J. (2022). Industrial Disaster Prevention Smart

Safety Equipment Using ZigBee and central safety management system. *Proceedings of the Korean Conference on Control and Robot Systems,* 748-749.

홍 성 혁 (Sunghyuck Hong) [종신회원]

· 2007년 8월 : Texas Tech University, Computer Science (공학박사)

· 2012년 3월 ~ 현재 : 백석대학교 첨단IT학부, IoT 전공 주임 교수

· 관심분야 : 핀테크, 딥러닝, 블록체인, 사물인터넷 보안

· E-Mail : shong@bu.ac.kr