International Journal of Engineering & Technology, 7 (3.34) (2018) 594-597

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

The Research on Security Technology for Low-Performance Iot Sensor Node

Youngkwan Ju[1], Hyung-JinMun[2*]

[1]Department of Software, Chungbuk National University, Republic of Korea
*[*2]Dept. of Information & Communication Engineering, Sungkyul University, 14097, Republic of Korea*
[*]Corresponding author E-mail: jinmun@gmail.com

Abstract

Background/Objectives: IoT developmental background: IoT, which is the key technology in the fourth industrial revolution, utilizes the Internet. Particularly, the growth of convergence products that utilize it has been constant with the demands of IoT services using the network of the Internet.
Methods/Statistical analysis: IoT network consists of products equipped with various sensors to communicate; sensor nodes are made up of low volume memory, low performance CPU, and battery when they are used in the network. There has been the demand of secure transmission of information measured by a sensor node to the IoT platform. We conduct a study on how we can improve security in the IoT environment.
Findings: Generally, sensor nodes are applied with basic security provided by IoT communication protocol rather than their own encryption. Therefore, sensor nodes are vulnerable in terms of security and the IoT platform that utilizes information collected by them would process distorted information.
In order to draw a strategy to prevent security breach, we analyze security threat and the type of attacks.
Improvements/Applications: We suggest a countermeasure to deal with security threat of sensor nodes and situations in which sensor nodes are vulnerable in IoT environment. To secure integrity of communication and transaction between a sensor node and an IoT platform in the future, the application of block chain technology into the IoT environment is necessary.

Keywords: *Internet of Things, IoT security, Sensor node, MQTT, CoAP, XMPP*

1. Introduction

Smart IoT convergence products that provide user convenience using the network are on the market. An IoT convergence product utilizing sensor nodes linked to the Internet connects thing to thing or thing to person so as to provide information and services necessary for the user. These products are expected to improve the quality of human life by autonomously collecting information, processing information, and providing customized information. Gartner, a global market research company, predicts that IoT products will be used in many ways in our lives and the number of them will reach 26 billion in 2020[1].
IoT service consists of an IoT platform that generates information to be provided for users and a sensor node that collects required information[2,3]. IoT service includes many technologies to generate information for users. It employs networking technologies to connect the sensor node with the platform and device-operating technologies for the sensor node to independently collect information. Furthermore, it utilizes big data technology to process massive information, AI technology to extract information required by a user, and interface technology of human computer that connects thing to person. IoT service carries out the role to create and provide information required by thing, person, or to get other services by storing, processing, and analyzing collected information. With integrated sensor nodes collecting useful information, IoT service has made human life more convenient and beneficial[4-6].
IoT service, however, has vulnerability regarding security because of service implementation technology or method. There is possibility for IoT service to cause inconvenience, financial and mental harm because of malicious code or malfunction that undermines IoT platform[7,8]. Therefore, it is necessary to systematically devise security technology for IoT service in order to provide IoT service that is secure and trustworthy.

2. Related Works

2.1. MQTT

MQTT(Message Queue Telemetry Transport)[9] is an open application protocol that OASIS(Organization for the Advancement of Structured Information Standards) adopted and approved as the standard protocol of IoT on May 2013.MQTT has features that it has narrow bandwidth and efficient battery consumption and it has been used as the mobile messenger protocol of Facebook. It secures transmission without loss by supporting QoS level 3 in transmitting important messages.
The weakness of MQTT is that it does not have encryption of base protocol and it restricts idle time of a sensor node with the structure that maintains all the time connection. MQTT-S[10] that resolved the problem related to the idle time of the sensor node has been used.

2.2. CoAP

CoAP(Constrained Application Protocol)[11], a low-power asynchronous communication protocol, utilizes asynchronous communication based on UDP unlike MQTT. The first draft of CoAP was released in 2010; it is a newly made protocol compared to other protocols. To support QoS of application level, CoAP message is displayed as 'Verified' or 'Unverified;' It supports DTLS(Datagram Transport Layer Security), UDP version of TSL as existing SSL/TLS encryption was impossible with UDP.

The weakness of CoAP is that it is one on one protocol that cannot support one to many that MQTT supports. However, CoAP protocol supports RESTFul(REpresentational State Transfer) method that supports HTTP and utilizes DTLS(Datagram Transport Layer Security) for encryption.

2.3 Xmpp

XMPP(Extensible Messaging and Presence Protocol)[12] is a message-oriented middleware communication protocol based on XML. Jabber, the open source community, developed it in 1999.XMPP server can be separate from open XMPP network and adopts SASL and TLS, powerful security methods. SASL(Simple Authentication and Security Layer) is a framework for authentication in the Internet protocol and data security.

XMPP protocol has the strength that it provides multiple connection support library to materialize distributed environment. The weakness of it is that it does not support end-to-end password function or QoS. However, it supports security of transmission level for services provided by SASL.

3. IoT Environment and Security Threat

3.1 Iot Environment

A sensor node is a device that collects physical values from many fields like electronics, buildings, machines, vehicles, and airplanes and transmits the data into the server that collects, processes, and manages them. As shown in Fig. 1, the sensor node sends values to IoT platform that manages sensor information through the network.It has a structure that transmits collected information to manage and request information to display.

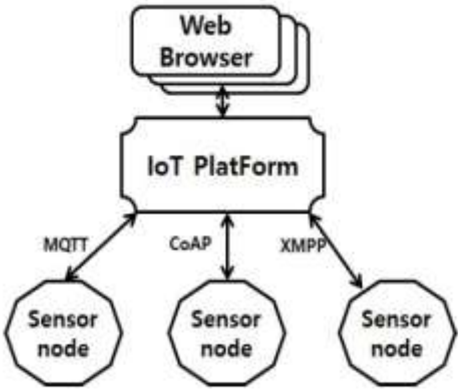

Figure 1: Basic Blocks of IoT

As seen in Fig. 1, sensor nodes and IoT platform communicate one another using different protocols and verify information with the web browser connected to IoT platform.

Web Browser: It plays the role to access IoT platform to display information. Web browser utilizes HTTP protocol and uses web socket in responding.

IoT Platform: It plays the role to collect information via each node and different interfaces to process and provide information for the browser.

Sensor Node: It plays the role to collect actual details to be sent to IoT platform, being placed at the tip of IoT environment. The node selects one from MQTT, CoAP, XMPP that IoT platform supports and transmits data with the platform.

The sensor node described in Fig. 1 is able to collect required information when it runs without interference. However, an ill-intended attacker is also able to collect information of the sensor node. It is necessary to protect information collected from the sensor node and IoT platform, and transmitted in communication.

In this paper, we suggest an information policy and a protective method of the sensor node to block ill-intended attacks. We first look into security threats of IoT environment and suggest a solution to the threats.

3.2 Security Threat in Iot Environment

IoT environment consists of a variety of nodes closely connected to our daily lives. A lot of sensor nodes carry out processing our demands by collecting information from us. As there are many ways to attack IoT by exploiting security vulnerability, we aim to find out which security problem exists through case study.

As consumer goods and services applied with IoT technology advance with refrigerator, TV, vehicle, medical device, the security threat targeting these has been growing. With Smart Home hacked, information leakage or malfunction of home appliances can be incurred and vehicle connected to the network can be stopped or moved to an unwanted place.

Moreover, not only security threat to sensor nodes but also risk of network connection failure has been increasing. For example, as sensor nodes are linked together to build a network, the whole network can be affected by one of nodes with connection failure. Thus, an organized security system to protect IoT environment is required.

Table 1 shows various fields which can be threatened; it is categorized. In particular, bio-information leakage of an individual can be very risky since it can be exploited for authentication by exploiting the information.

Table 1: IoT attack threats

Division	Security Threat Cases
Smart Electronics [13]	- Electronics such as smart TV, washing machine, refrigerator, which support IoT environment are used. - IoT electronics are controlled by communication between person and thing using different messages via network. - When IoT electronics are hacked, they can send domestic information to the hacker and malfunction to cause confusion.
Autonomous Vehicle [14]	- Autonomous vehicles recently introduced employ many IoT sensors. - With IoT sensors hacked, a driver can have problems driving the vehicle properly. And he would risk his life.
Bio-information Breach [15]	- Bio information has been used for authentication in many fields regarding access control. - If bio information is hacked, an ill-intended hacker can neutralize the security function with approval of access.

3.3. The Types of Iot Attack

The types of IoT attack can be categorized into four.

Because light and low power sensor nodes are hardly equipped with encryption function to protect data and they transmit data in plain text, data forgery attack can be made.

Without integrated administrative system that centrally controls sensor nodes, the process of ID issue and authentication is not secure or properly controlled; an attacker can easily forge sensor nodes to disrupt IoT environment.

As the network security policy in IoT environment, there are basics such as authentication procedure and password intensity; however, it is not easy to respond to the infection by malicious code in a network or heavy increase in traffic in a network channel.

Attacks to cause out of service time can be made with forgery of data between sensor nodes and service platform or malfunction, which causes errors of collected data.

4. Conclusion Countermeasure to Security Threat

Regarding security threat of IoT environment, because of limited computing capability and limited time to use power, sensor nodes are more vulnerable than a system with enough computing capability and power.Low-performance sensor nodes are hardly equipped with the function to process high quality data encryption because of low processing capability and low power. For this reason, sensor nodes have become the vulnerability to disrupt security of the entire system.

In the paper, we suggest a system with which the IoT platform collectively controls security of low-performance nodes. We designed the IoT platform to have a system that entirely controls registration and encryption transmission to resolve the vulnerability. This chapter deals with the security system of IoT platform and compares message protocol for IoT purpose the platform can utilize.

4.1. Security System of IoT Platform

Sensor node protection in IoT environment should be made in the entire IoT environment. As seen in Fig. 2, the system consists of IoT platform that corresponds to an integrated administrative server and Sensor that corresponds to sensor nodes. As seen in Fig. 2, to protect the service, IoT platform carries out registration of a sensor, authentication, key generation, key management, data encryption and decryption, and sensor node monitoring; the sensor carries out sensor authentication, message encryption, channel encryption by sending and receiving data to and from the platform.

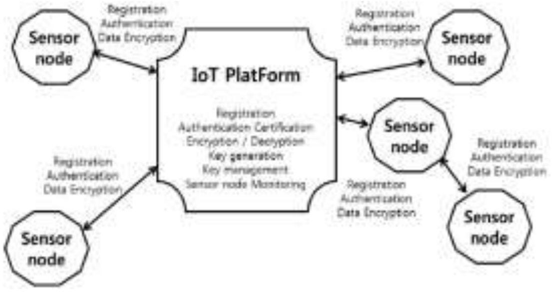

Figure 2: Integrated Security System of IoT Environment

4.1.1. Sensor Node Registration and Management

Sensor node registration is the process for IoT platform to register sensor nodes in the platform to manage sensor nodes. For example, when a new sensor node requests ID from IoT platform, it checks whether the ID is registered and if not, it conducts registration process. In the process to register, it checks whether it is normal or abnormal based on requested information of sensor nodes. When it is a normal ID, IoT platform provides response by transmitting information of sensor nodes. In order for IoT platform to make sensor nodes have a distributed task and to check if there is a sensor node required, it can send inquiry to all the sensor nodes around and receive the result.

4.1.2. Sensor Node Key Generation and Management

IoT platform issues private key based on registered IDs in sensor nodes when generating a sensor node. Sensor nodes carry out registration process that combines transmitted numbers of a sensor node's ID and platform and encrypts them as a public key to be sent based on private key. IoT platform regularly manages registered values of sensors under a set of rules.

4.1.3. Sensor Node Status Monitoring

Sensor node status monitoring means that IoT platform checks the status information by requesting sensor node's status from sensor nodes by certain time or condition set.

Sensor node status checkup is used to verify sensor node's status information in response to the search after IoT platform searching for sensors around it. For example, in the case of water level measurement sensor, when the command, "measure" is sent, the sensor node sends water level measurement information to IoT platform.

Sensor node status monitoring, considering computing capability and power usage time of sensor nodes, operates scheduling policy that can arrange a task of a sensor node.

4.2. Comparison of Communication Protocols of Iot Platform

IoT platform is supposed to support MQTT, CoAP, XMPP protocols that sensor nodes utilize and protect transmitted data with these protocols. Each protocol employs encryption of SSL, TLS, DTLS, and SASL to protect data.

Table 2: Comparison of IoT Communication Protocols

	MQTT	CoAP	XMPP
Protocol	TCP (MQTT-SN)	UDP	TCP
Communication mode	M:N	1:1	M:N
Power consumption	Middle	Low	High
QoS	3 Level	1 Level confirm/non confirm	no support
Encryption	SSL/TLS	DTLS	SSL/TLS/SASL
MSG type	binary	binary	Text
etc	Pub/Sub w Broker	RESTful support	Pub/Sub w Broker, req/resp

Table 2 is a summary of the feature of each protocol. Communication mode was only supported with CoAP and MQTT showed the best power consumption efficiency. The quality of transmitted data through MQTT was the best; it supports QoS level 3 which XMPP does not support. CoAP added menus of confirm and non confirm to support QoS through UDP. Regarding etc section, MQTT and XMPP have the issuer/receiver structure in which Broker that plays a role of intermediate connector exists; CoAP transmits a message with the server/client structure.

5. Conclusion

IoT is one of the key technologies of the fourth revolution, on which the number of devices connected to one another are expected to reach 26 billion in 2020. Promising IoT cannot secure confidentiality because of limited resource of hardware such as low capacity and low power or wireless mobile environment; moreover, it has physical vulnerability. In particular, because low power and low performance sensor nodes lacking resource cannot ensure security, a safer security method suitable for sensor nodes is required.

In the paper, we studied security problems that can be incurred in materializing IoT-based sensor nodes and countermeasures to them. We suggested the security management system that includes sensor node registration management, sensor node status checkup, sensor node monitoring, sensor node key management, and communication protection of IoT platform with regard to secure communication between IoT platform and sensor nodes in IoT environment. Additionally, it would be necessary to activate encryption in data transmission section between IoT platform and a sensor node or sensor nodes for secure transmission in IoT environment. Even in the case of a low-performance node, applying encryption function to it can contribute to building secure IoT environment. In IoT environment, we described the security system from registration of sensor node to data encryption between IoT platform and sensor nodes.

We aim to conduct a following study to secure credibility of information between IoT platform and sensor nodes; the study is expected to deal with application of blockchain algorithms to protect information between low-performance sensor nodes and IoT platform.

References

[1] Saha, H. N., Mandal, A., & Sinha, A. (2017, January). Recent trends in the Internet of Things. In Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual (pp. 1-4). IEEE.

[2] Lea, R., & Blackstock, M. (2014, December). City hub: A cloud-based iot platform for smart cities. In Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on (pp. 799-804). IEEE.

[3] Yang, G., Xie, L., Mäntysalo, M., Zhou, X., Pang, Z., Da Xu, L., ...& Zheng, L. R. (2014). A health-iot platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE transactions on industrial informatics, 10(4), 2180-2191.

[4] Mishra, N., Lin, C. C., & Chang, H. T. (2015). A cognitive adopted framework for IoT big-data management and knowledge discovery prospective. International Journal of Distributed Sensor Networks, 11(10), 718390.

[5] Fantacci, R., Pecorella, T., Viti, R., & Carlini, C. (2014, March). Short paper: Overcoming IoT fragmentation through standard gateway architecture. In Internet of Things (WF-IoT), 2014 IEEE World Forum on (pp. 181-182). IEEE.

[6] Maarala, A. I., Su, X., & Riekki, J. (2017). Semantic reasoning for context-aware Internet of Things applications. IEEE Internet of Things Journal, 4(2), 461-473.

[7] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

[8] Bertino, E., & Islam, N. (2017). Botnets and internet of things security. Computer, 50(2), 76-79.

[9] Tang, K., Wang, Y., Liu, H., Sheng, Y., Wang, X., & Wei, Z. (2013, September). Design and implementation of push notification system based on the MQTT protocol. In International Conference on Information Science and Computer Applications (ISCA 2013) (pp. 116-119).

[10] Hunkeler, U., Truong, H. L., & Stanford-Clark, A. (2008, January). MQTT-S—A publish/subscribe protocol for Wireless Sensor Networks. In Communication systems software and middleware and workshops, 2008. comsware 2008. 3rd international conference on (pp. 791-798). IEEE.

[11] Rahman, R. A., & Shah, B. (2016, March). Security analysis of IoT protocols: A focus in CoAP. In Big Data and Smart City (ICBDSC), 2016 3rd MEC International Conference on (pp. 1-7). IEEE.

[12] Saint-Andre, P. (2011). Extensible messaging and presence protocol (XMPP): Core.Retrieved fromhttps://tools.ietf.org/html/rfc6120.html

[13] Li, B., & Yu, J. (2011). Research and application on the smart home based on component technologies and Internet of Things. Procedia Engineering, 15, 2087-2092.

[14] Bécsi, T., Aradi, S., & Gáspár, P. (2015, June). Security issues and vulnerabilities in connected car systems. In Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2015 International Conference on (pp. 477-482). IEEE.

[15] Pienaar, J. P., Fisher, R. M., & Hancke, G. P. (2015, July). Smartphone: The key to your connected smart home. In Industrial Informatics (INDIN), 2015 IEEE 13th International Conference on (pp. 999-1004). IEEE.