

A Design and Implementation of Gateway for Smart Home Sensor Network Management

Bokrae Jang¹ and Seunghyun Oh^{2*}

¹MS Scholar, Department of Computer, Dongguk University, Gyeongju,
South Korea

²Professor, Department of Computer Engineering, Dongguk University, Gyeongju,
South Korea

¹Pse5802@dongguk.ac.kr, ²shoh@dongguk.ac.kr

Abstract

The smart home network is a complex industrial field combining a variety of IT technologies, such as network and information processing based on a high-speed infrastructure, that connect home information appliances to various devices. It is a field that can provide services. The structure of the smart home network is composed of a plurality of sensors, and the sensors are provided in the form of a miniaturized chip in a home appliance. The sensor provided in this way has a problem in that it can process only a simple operation because it is inexpensive. In fact, in a home network environment, a sensor can perform the function of transmitting its own measurement value or receiving and processing a specific command, so an object that can control and manage the sensor is required. The communications module of the sensor is not standardized, and various heterogeneous communications modules are used. In this paper, we propose using the Message Queuing Telemetry Transport protocol, which is one kind of Internet Protocol (IP) device, for non-IP-based communications sensors to collect data, and we discuss how to manage the sensor through the sensor. We show that we can manage the smart home network effectively and reliably through the gateway-based heterogeneous network management method proposed.

Keywords: Wireless Sensor Network, Sensors, Smart Home Networks, Gateway, MQTT

1. Introduction

This paper investigates gateways that support data collection and sensor management of various heterogeneous sensors in a smart home network. In the home network architecture, sensors come in various types, and since most of these sensors have little memory and computation ability, only simple operations can be processed [1, 2, 3]. Therefore, a server or gateway, which is an essential element of a network, must be able to collect sensor data and manage sensors. For the server, it is more stable to allow the gateway to manage the sensor network, since the load may be concentrated in the actual environment. From the viewpoint of communications, sensors can be classified as communicating with an Internet Protocol (IP) address or communicating without an IP address (that is, a non-IP communicating sensor). For a sensor supporting an IP address, it is possible to manage it using the Message Queuing Telemetry Transport (MQTT) protocol[4], but that presents a problem that a non-IP sensor does not have.

In this paper, we propose a method to collect messages using the MQTT protocol for IP-based communications sensors, and to collect messages and manage the sensors

Received (January 3, 2018), Review Result (March 9, 2018), Accepted (March 12, 2018)

* Corresponding Author

through the gateway for a smooth message service and sensor management in the home network. Finally, we aim to design a framework that can efficiently manage sensor networks in a smart home network structure. Figure 1 below shows how various types of sensors used in smart home networks are classified according to the availability of IP addresses and the data collection cycle. From the network management aspect, this type of classification is necessary, because the data collection period of the sensor is event-based, and periodic collection is different.

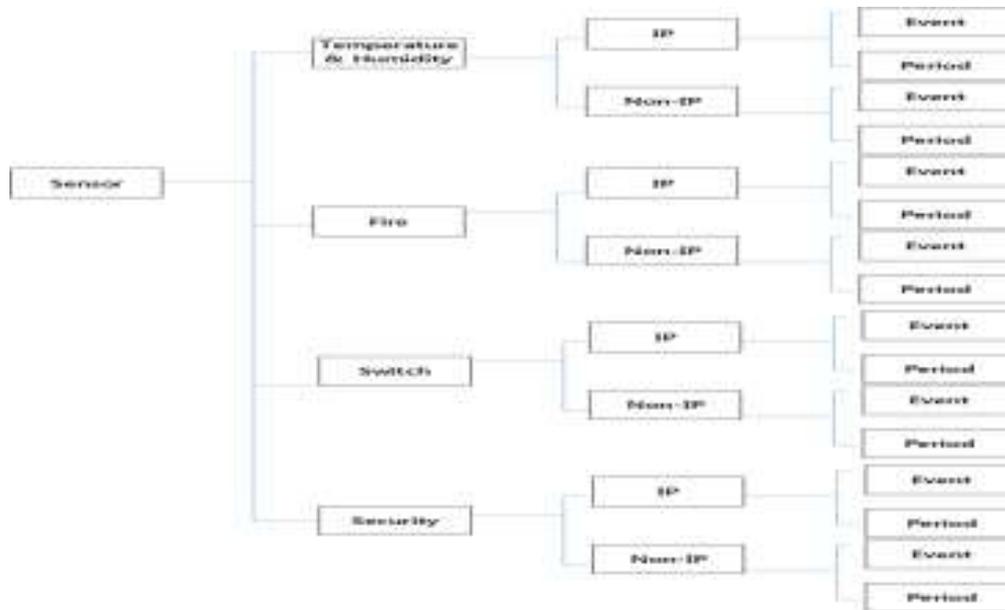


Figure 1. Category of Sensors Type

In order to control sensor devices that do not support IP, this research studies them in the following order. First, in sensor classification, the sensors are grouped into sensors that are related to each other, rather than seeing them as one independent structure. In other words, the group is divided according to the use of the sensor, sensors are classified into IP-based or non-IP-based, and they are classified as sensors that periodically transmit data or sensors that generate an event. The second step explores how the gateway can manage the sensor. That is, in order to solve the problem where the MQTT protocol is used for a sensor supporting IP-based communications, and where the existing MQTT protocol cannot be used for a sensor of a non-IP communications module, communication is performed according to the communications protocol devised in this study, and we show how to manage the battery level and collected data. Third, we propose a system architecture based on the proposed gateway-based management method.

Fourth, the implementation environment for realizing the whole system structure and the implementation scope are implemented only for sensors that perform non-IP communications. Fifth, we will describe an experiment with the implemented system, and provide a description of the implemented function and the structure of the implementation function. The experimental result aims to provide the user with the simplest interface possible.

The composition of this paper is as follows. In Section 2, we present related work on how to manage heterogeneous sensor networks. Section 3 describes the gateway-based design proposed in this study. Section 4 describes the implementation of the system and the experimental results from the user's point of view. Finally, Section 5 presents conclusions and future research projects.

2. Related Work

Various studies have been carried out to integrate and manage sensor networks. This paper proposes a framework for the home sensor network as well as a study on how to integrate and manage heterogeneous network modules at the gateway. In order to solve this problem, a research using a user card slot and a protocol converter [6] proposed a gateway as shown in Figure 2.

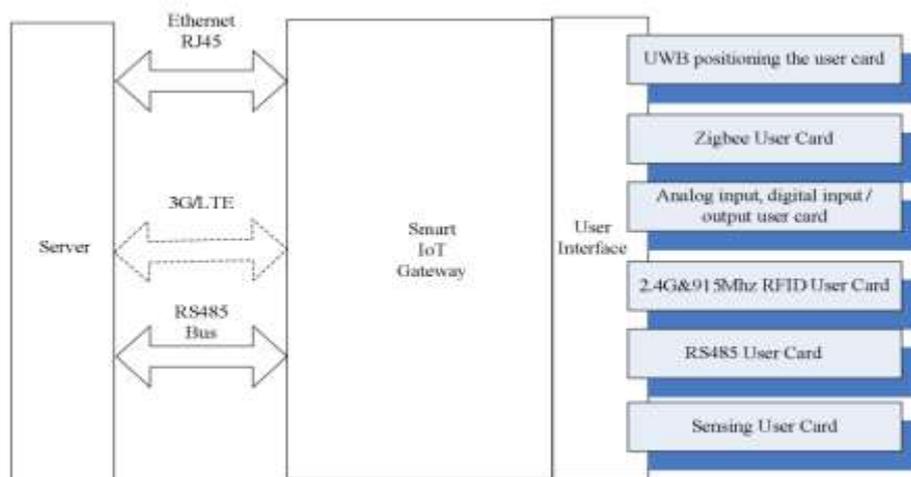


Figure 2. Overview of User Card Slots System

In Figure 2, the server is responsible for the hierarchical data and visual data of the entire system. The smart Internet of Things (IoT) gateway is responsible for the combination of protocol converter and other sensors. In addition, the user interface provides a basic interface for realizing the functional elements of the gateway. The independent protocol converter proposed in this study is shown in Figure 3. Although it can support stable service through the independent protocol converter, it does not support per-message quality of service (QoS) that is important in an actual home network.

2	1	2	2	1	2	1	1	Len-22	2
Preamble Sequence	TYPE	Dest_ID	Source_ID	SN	Len	Pkt_Type	Reserved	*data	CRC16
SHR								Data Payload	CRC
HEAD	payload								FCS

Figure 3. Independent Protocol Converter Structure

The second study considers the environment using private IP addresses. If building a home sensor network environment, there may be times when it is configured as a private IP network. In this study, we propose an effective communications model for a structure where it is difficult to communicate between server and gateway in a private network [6]. The proposed model is shown in Figure 4.

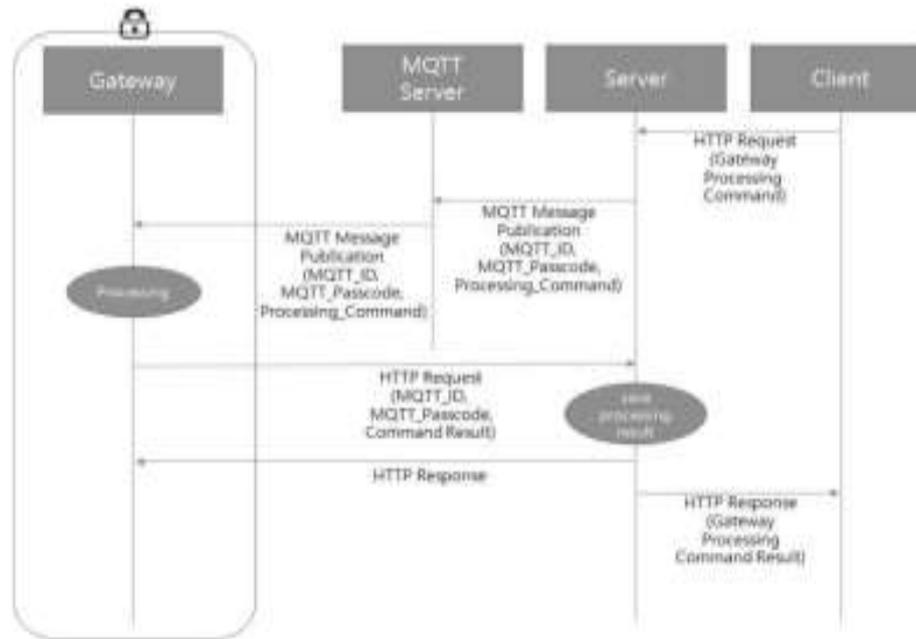


Figure 4. Communication Structure of MQTT/HTTP

As shown in Figure 4, the gateway is configured with private IP and communicates in the following way. When the client sends a Hypertext Transfer Protocol (HTTP) request to the server with a message to be delivered to the gateway, the server publishes the message using MQTT to the gateway. After receiving the message through the MQTT server, the gateway processes the content requested by the received message, transmits an HTTP request to the server, and transmits the result of the MQTT message. The server does not immediately respond to the HTTP request sent by the client, but waits for the processing result of the MQTT message sent to the gateway, and then replies.

Although the bidirectional communication model between the server and the gateway is designed through the method proposed elsewhere [6], the number of requests may be large when used in a home network environment composed of a plurality of sensors. There is a problem that it is not considered.

Research on dynamically discovering sensors has not been done yet. One study [7] focused on the difficulty of dynamically discovering Arduino devices, one of the problems of the existing Device Profile for Web Service (DPWS), and studied how to dynamically discover and register devices at the gateway. This research used the MQTT protocol to dynamically search the sensor in a real home network and access it in a registerable direction. However, the MQTT protocol does not solve the problem of discovery and registration of all sensors because it is applicable only to sensors that perform IP communication. In addition, various studies including 802.15.4 research were preceded[8].

3. A Gateway Design for Smart Home Network Management

In this section, we describe the classification of sensors used in the home network, the content for the selection of the QoS level of each sensor, the reasons for selection, the sensor management method for communications based on IP, and the sensor management method for communications based on non-IP suggests the requirements of the gateway and the overall system configuration. Sensors do not all have the same role, but they work differently depending on the application of each sensor. The transmission method of the sensor can be divided into a sensor that transmits data periodically and a sensor that operates based on an event. In this section, the characteristics of the sensor will be

referred to. The types of communications modules referred to in this section are indicated for currently used sensors. The actual sensor configuration may vary depending on the communications environment, such as how to configure the board, the communication distance, *etc.*, sensor management is very useful in.

Table 1. Classification According to Functional Property of Sensors

Sensor	Temp.	Electric	Gas	Lighting control	Humidity
Group	Temperature & Humidity	Power	Fire	Power	Temperature & Humidity
Sensor	Infrared	Smoke	Sprinkler	Door Lock	
Group	Security	Fire	Fire	Security	

The temperature and humidity sensor groups in Table 1 are sensors that transmit data after periodically measuring the current value. Sensors in the power group are composed of sensors that receive a control message when a threshold value is exceeded, based on periodically measured sensor values such as temperature and humidity, and sensors that receive the control message requested by the user. Fire groups consist of fire-related sensors, such as smoke and gas sensors, and the sensors in that group consist of sensors that can activate sprinklers in the event of an over-threshold event. Finally, the security group can be used to detect an external intruder through infrared sensors and door-lock sensors when the resident goes out.

A home network composed of such a variety of sensor devices can be divided into groups capable of using the MQTT protocol and groups having no Transmission Control Protocol/Internet Protocol (TCP/IP) connection and computational capability. This study categorizes small sensor–device groups that cannot support MQTT as non-IP based sensors and proposes a support method. Among non-IP devices, MQTT-SN [9] is designed for devices capable of supporting the ZigBee protocol [10], but there is a problem in that the protocol is limited to ZigBee. Non-IP–based communications modules include Bluetooth and Z-Wave[11] as well as ZigBee. For sensor management, the keep alive provided by the MQTT protocol cannot be used in ZigBee. Therefore, in this section, we introduce a study on how non-IP-based sensors connect to gateways, how to communicate data, and how to terminate the connection.

A non-IP sensor performs the connection, data transmission, and disconnection between the sensor and the gateway through the process shown in Fig. 5. The sensor transmits a connection frame for connection with the gateway before transmitting its measurement data to the gateway. The connection frame includes a sensor address field, a group field to which the sensor belongs, a sensor for periodically transmitting data, a field for distinguishing whether the sensor operates based on an event, a period value for a sensor transmitting data periodically, and a current battery power–remaining field.

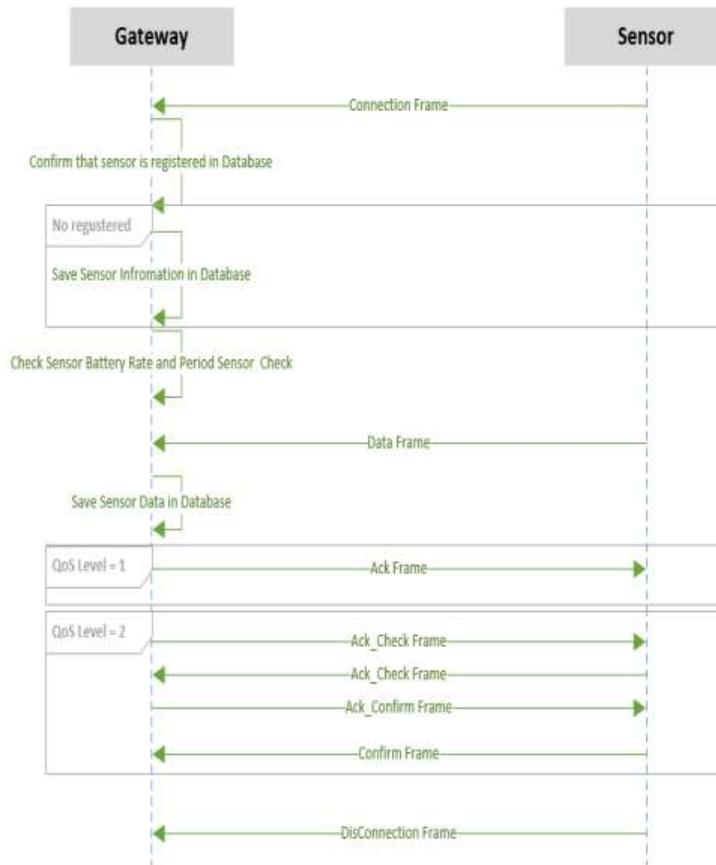


Figure 5. Procedure between Non-IP Device and Gateway

When sending a message from the gateway to the web server:

- If the user wants to query sensor data
- If the user needs to control the sensor
- When user wants to inquire sensor information
- If the user wants to query the sensor error

Usually, you use a method of building a database on a Web server, connecting directly to a database on the Web server. However, this is not a recommended method, given the security considerations. That is, the data of the gateway should be able to be modified by, and inquired into, only by the gateway. In our study, when a Web server requests information, the gateway uses the method of receiving information transmitted from the Web server and connecting directly to its database.

To realize such a function, a unified message structure between the gateway and the Web server is required. In other words, the message sent from the Web server to the gateway must match the message sent from the gateway to the Web server, and the gateway needs to convert the message. By applying these functions, the security of the entire system is improved.

4. Implementation and Discussion

The requirements of the gateway proposed in this study are divided into non-functional requirements and functional requirements. The non-functional requirements are as follows.

- It should be user-friendly.
- The value transferred to the sensor must be transparent.
- Provide a stable service.

Functional requirements can be summarized as shown in Table 2.

Table 2. Functional Requirements

Requirements	Description
Convert and Relay	Converting and delivering messages to wired and wireless network connectivity and platform format.
Security	Should not have direct access to data from outside.
Sensor Management	The gateway must be able to manage the sensor.
Data Management	The sensor data must be retainable.

The structure of the proposed system is shown in Figure 6. For the user interface, the interface is contacted by the user for sensor management and control, and the corresponding interface is provided to the user via the Web. The MQTT client requires brokers and clients to use the MQTT protocol, and it is an entity that performs publish/subscribe.

Socket communications (client) communicates between the user interface and the Web server in HTTP message format. In a communication, it is possible to add and manage a database in the Web server to inquire after sensor configuration management. However, this is a bad method for security problems. The message converter is the part that the Web server handles when a request message arrives, converting it to Web socket format when sending data to the Web server.

In sensor management, the sensors are divided into IP and non-IP sensors, and IP sensors are managed by using the MQTT protocol. Non-IP sensors are managed by the method mentioned above. The data management module is where data from the sensors are stored. The driver interface module requires a communications module driver to communicate with IP and non-IP sensors, and the driver interface provides the corresponding function.

The dotted line in the Figure 6 is the part implemented in this study, and the other part will be implemented and tested in the next study.

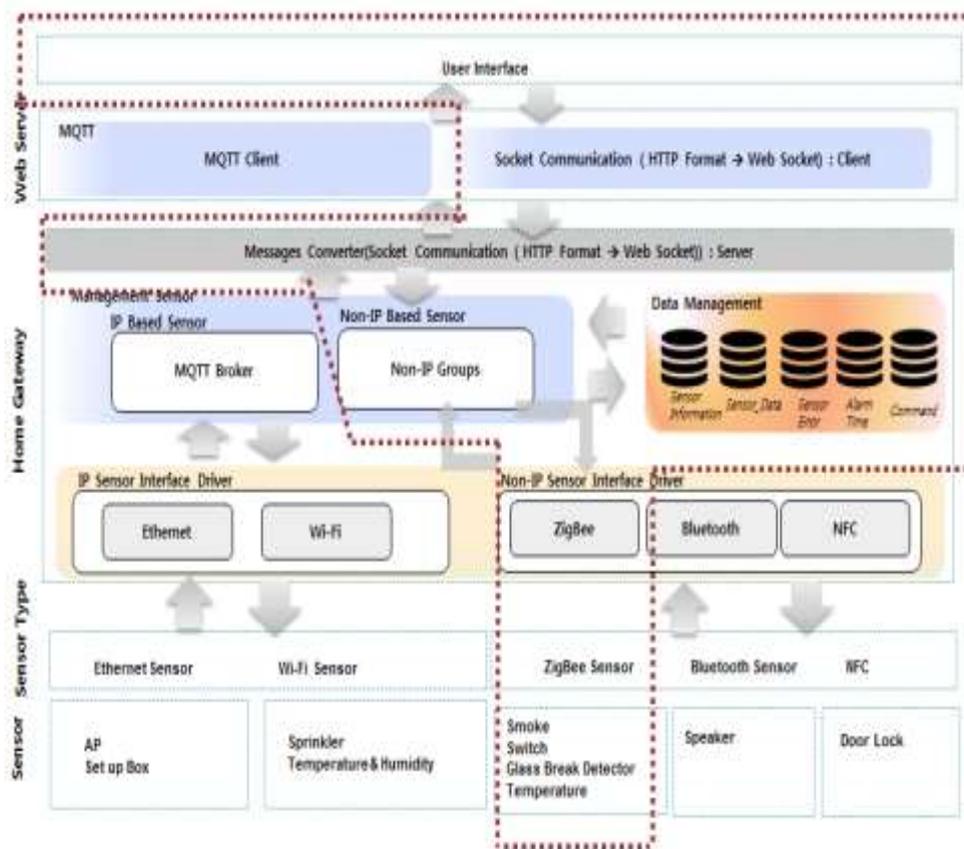


Figure 6. System Overview of Proposed Gateway for Smart Home Network Management

Experimental results will be discussed from the viewpoint of the user, and the results realized by the user interface are explained. Figure 7 shows the Web page that the user first touches before querying the sensor information. If you click each circular icon on the main screen, you can check the information of the sensor. An activated sensor is displayed in red. Inactive sensors are displayed in black and white. By adding an additional GPS sensor, you can see where the actual sensor is. It is provided as a pop-up window when the user clicks the circle icon.

If you want to ask for all the sensor information, you can inquire from the View All Sensors menu. Information about the group to which the sensor belongs, the identifier of the sensor, the address of the sensor, whether the sensor is an event-type sensor or not, and periodic information are provided. Details are shown in Fig. 8. When users want to view data in real time and for a certain period of time, they can inquire about the contents collected in real time by selecting the Check Data item.

Sensor data inquiry can display real-time data and data collected by time period. Figure 9 shows a real-time view of the sensor data. The sensor error inquiry screen and an inquiry screen for alarm information settings according to the sensor battery state can be implemented and used. In addition, a function for actuator sensor control is implemented.



Figure 7. User Interface of Web Service

View All Sensor Information

Group	Sensor ID	Sensor Addr	Sensor Type	Conn_Type	Period	Data Check
Temperature & Humidity	394784917	0013A200409E12BC	Period Sensor	Non_IP	10	Check Data
	sensor0	203.247.239.1	Event	Non_IP	10	Check Data
Fire Group	sensor1	203.247.239.160	Period Sensor	IP Based	10	Check Data
	sensor10	3113A200409E12C1	Period Sensor	Non_IP	22	Check Data
	sensor11	2113A200409E12C1	Event Sensor	Non_IP	22	Check Data
Switch Group	sensor15	203.247.239.112	Period Sensor	IP Based	22	Check Data
	sensor14	203.247.239.12	Period Sensor	IP Based	22	Check Data
	sensor12	2163A200409E12C1	Event Sensor	Non_IP	22	Check Data
Security Group	sensor3	203.247.239.132	Event Sensor	IP Based	20	Check Data
	sensor4	1013A200409E12B1	Event Sensor	IP Based	20	Check Data
	sensor5	1213A200409E12B1	Period Sensor	Non_IP	20	Check Data
	sensor6	203.247.239.22	Event Sensor	IP Based	20	Check Data
	sensor7	203.247.239.44	Period Sensor	IP Based	21	Check Data
	sensor8	203.247.239.56	Period Sensor	IP Based	21	Check Data
sensor9	203.247.239.74	Period Sensor	IP Based	21	Check Data	

Figure 8. View All Sensor Web Design



Figure 9. Real-time Data Query Design

5. Conclusion

In this paper, we study a gateway that can store sensor data and manage multiple sensors in a smart home network environment composed of multiple sensors. In addition, the sensors are classified by how they are used in the actual home network, so they can be managed systematically. When a sensor is connected to the gateway, it adds the remaining battery capacity field and transmits it to the gateway. By managing the sensor based on the collected data, it is possible to have a more stable smart home environment in terms of management. The system developed for this research focuses on non-IP communications sensors and is designed to be easy to use without user training. The structure of the interface provided to the user is implemented so that the user can directly obtain the data of the sensor, control it, and inquire into generated error items.

References

- [1] J. Lee and P. Sunyoung, "Analysis of Home Network Service Acceptance Model Using Extended Technology Adoption Model", *Consumer Culture Research*, vol. 10, no. 4, (2007).
- [2] J. Tae Kim, "Analyses and Security Requirements for Smart Home Network Based on Internet of Things", *International Journal of Reliable Information and Assurance*, vol. 4, no. 2, (2016) December, pp. 25-30.
- [3] J.-H. Huh, S.-M. Je and K. Seo, "Design and Simulation of Foundation Technology for Zigbee-based Smart Grid Home Network System using OPNET Simulation", *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, vol. 5, no. 4, (2015) August, pp. 81-89.
- [4] D. Locke, "Message queuing telemetry transport (mqtt) v3. 1 protocol specification", IBM developer Works Technical Library, (2010).
- [5] J.-Y. Han and S. Lee, "Home Network Gateway Development Supporting Wired-wireless Communication Method", *The Institute of Electronics Engineers of Korea - Telecommunications*, vol. 45, no. 12, (2008), pp. 114-119.
- [6] J. Seul Gi, S. Min Hwan and L. Sang Shin, "A Study on the Communication Method Using MQTT/HTTP Between IoT Server and Gateway Using Private-IP Address", *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, (2016), pp. 1098-1099.
- [7] S.-M. Kim, H.-S. Choi and W.-S. Rhee, "IoT home gateway for auto-configuration and management of MQTT devices", *Wireless Sensors (ICWiSe)*, 2015 IEEE Conference on IEEE, (2015).
- [8] J. Baviskar, A. Mulla, A. Baviskar and J. Desai, "Implementation of 802.15.4 Wireless Sensor Network in Real-time Monitoring and Control System for Green House", *Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology*, vol. 5, no. 5, (2015), pp. 87-105.
- [9] A. Stanford-Clark and H. Linh Truong, "Mqtt for sensor networks (mqtt-sn) protocol specification", *International business machines (IBM) Corporation version 1*, (2013).
- [10] ZigBee Alliance, "Zigbee specification", (2006).
- [11] Z-WAVE alliance, "Z-WAVE public specification", (2017).