International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-10 Issue-6, August 2021

Simulation of a Fine Dust Value-Based False Data Detection System to Improve Security In WSN-Based Air Purification IoT

Ye-lim Kang, Tae-ho Cho

Abstract*: Fine dust refers to harmful substances floating in the air. It is divided into PM 2.5 and PM 10, and has the characteristic that the particles are small enough to be invisible to the naked eye. When fine dust enters a room, it can enter the human body through the bronchi and cause lung or respiratory diseases. To solve the health problems caused by fine dust, research and development about various air purification systems are progressing. In this paper, we introduce a Wireless Sensor Networks (WSNs)-based Internet of Things (IoT) air purification system. This WSNs-based IoT air purification system refers to a system in which an IoT air purifier and a window are automatically controlled based on fine dust values detected by sensor nodes. Therefore, because it is important to maintain the integrity of the fine dust values, SSL/TLS, an encryption protocol, is applied to this system. However, the existing SSL/TLS has a problem in which, if an attacker attempts a false data injection attack, the symmetric key itself used to encrypt and decrypt the data is stolen, so it cannot be detected. To solve this problem, in this paper we propose a Discrete Event System Specification (DEVS) model based on Data Calibration that verifies whether the fine dust values detected by sensor nodes and an IoT air purifier is within a preset error range. If the fine dust value is not within the preset error range, it is detected as false data, filtered, and not stored in the database. Because this proposed scheme verifies the integrity of the fine dust values, it not only raises the accuracy of collected sensing data, but also prevents abnormal operation of an IoT air purifier and a window in advance. Therefore, the security of the WSNs-based IoT air purification system is improved.

***Keywords*: Internet of Things; Wireless Sensor Networks; Security; Discrete Event System Specification.**

I. INTRODUCTION

Fine dust refers to particulate matter floating in the atmosphere and is mainly generated when exhaust gas from factories, automobiles, or fossil fuels are burned [1]. Fine dust is classified into PM 10 with 10um in diameter or less and PM 2.5 with 2.5 um in diameter or less. PM 2.5 is classified as ultra-fine dust. In other words, since the particles are so small that they are invisible to the naked eye, they can remain in the atmosphere for a long time and then enter the body and cause various diseases [2]. Therefore, there is a problem that when fine dust is introduced indoors, it may adversely affect the health of people who spend most of the day indoors. To solve health problems that may be caused by fine dust, recently, research and development of air purification systems that purify indoor air by filtering fine dust is being actively conducted. In this paper, we introduce the WSNs-based IoT air purification system, one of such technologies [3-6]. WSNs is a network environment in which if sensor nodes detect an event, they send event information to the Base Station (BS) and the BS provides a user with useful services by using it. The IoT is a network environment that not only sends and receives data through the Internet by attaching sensors and communication functions to various objects, but also provides people with convenient functions.

A network that combines WSNs with IoT is called a WSNs-based IoT system, and whether or not to execute an operation of an IoT device is determined based on event information detected by sensor nodes. Because it is important to maintain the integrity about sensing data in this network environment, SSL/TLS, an IoT security protocol, is used [7-8].

However, in the WSNs-based IoT system, when a false data injection attack occurs, the symmetric key is stolen by the attacker, so the existing SSL/TLS cannot filter false data and can possibly execute abnormal operations of the IoT device. To solve this problem, in this paper, we propose a DEVS model based on Data Calibration that verifies whether sensing data values detected by sensor nodes and IoT are within the preset error range [9-11]. If the sensing data values detected by sensor nodes and IoT are out of the preset error range, this is a method of filtering out false data. Compared to the existing system using SSL/TLS, the proposed scheme has the advantage of not only strengthening the security of the system by preventing the execution of abnormal operation of the IoT, but also increasing the accuracy of the collected data, which is useful for the development of a knowledge system.

The structure of this paper is as follows. Chapter 2 describes IoT, false data injection attacks, SSL/TLS, and DEVS, and Chapter 3 describes the proposed scheme. Chapter 4 verifies the performance of the proposed scheme through simulation. Chapter 5 draws the conclusions.

Manuscript received on August 18, 2021.
Revised Manuscript received on August 24, 2021.
Manuscript published on August 30, 2021.
* Correspondence Author
Ye-lim Kang, Student, Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea. Email: missye7322@skku.edu
Tae-ho Cho*, Professor, Department of Computer Science and Engineering, Sungkyunkwan University, Suwon, Republic of Korea. Email: thcho@skku.edu

II. RELATED WORK

A. Internet of Things (IoT)

IoT refers to an environment in which objects in the real world are connected to the Internet to provide convenient functions to users and to exchange data in real time. This does not simply mean that objects in the real world are connected to the Internet, but rather that objects automatically exchange data and communicate without human intervention to provide intelligent services to users. For example, when the user wakes up from bed, the light
turns on automatically and
the vacuum cleaner
automatically starts
cleaning. In addition, when the user is ready to go out and leaves home, all lights and gas lights in the house are turned off. In this way, objects can automatically perform all functions without human manipulation or intervention, so users can enjoy their daily life conveniently. IoT can also accumulate received data and use it for services to be provided to users in the future.

B. False Data Injection Attack

An attacker writes false data using the stolen symmetric key and injects this false data into an IoT device [12]. The false data injected into the IoT device is transmitted to the other IoT devices and can cause abnormal operation. For example, if an attacker injects false data that is different from the fine dust value actually detected by sensors into the IoT purifier, the false data is transmitted to the IoT window and can cause incorrect Open or Close operations.

C. SSL/TLS

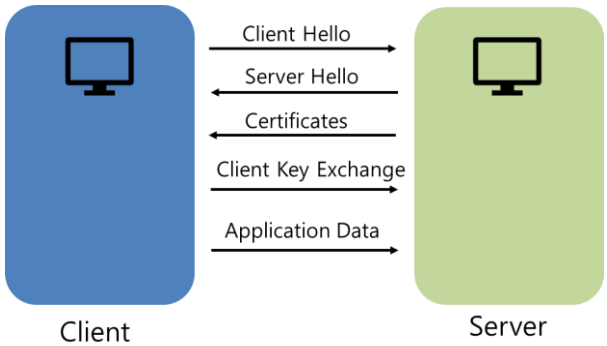

Fig. 1 SSL /TLS

Fig. 1 presents SSL/TLS. SSL/TLS is an encryption protocol that transmits data by encrypting plain text to safely transmit data between a client and a server. This protocol is a connection-oriented protocol that negotiates security by performing mutual authentication between a client and a server through a handshake. The client and the server generate a symmetric key used to encrypt data through the handshake, and when the handshake is finished, the client and the server encrypt data using the generated symmetric key and transmit it.

D. Discrete Event System Specification (DEVS)

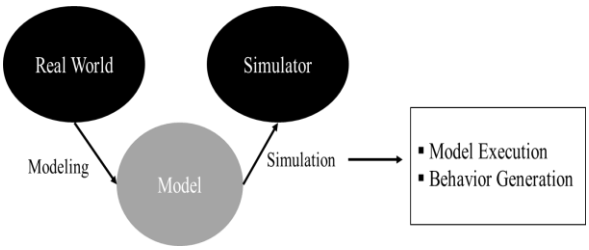

Fig. 2 DEVS

Fig. 2 presents DEVS. An attacker writes false data using the stolen symmetric key and injects this false data into an IoT device [12]. The false data injected into the IoT device is transmitted to the other IoT devices and can cause abnormal operation. For example, if an attacker injects false data that is different from the fine dust value actually detected by sensors into the IoT purifier, the false data is transmitted to the IoT window and can cause incorrect Open or Close operations.

$$M = <X, S, Y, \delta int, \delta ext, \lambda, ta>$$

Coupled Models play a role in determining the message delivery path between models and can implement a complex system by connecting various atomic models to form a Coupled Model. This Coupled Model is composed of a set of component names, a basic component of the model, a set of influence models, an output transformation, and a tie-breaking function.

$$N = <X, Y, D, \{Md \mid d \in D\}, EIC, EOC, IC, select>$$

III. PROPOSED SCHEME

A. Problem Statement

The existing SSL/TLS has a problem in which an IoT device can perform an abnormal operation when a false data injection attack occurs. To defend against this problem, in this paper, we propose a Data Calibration-based DEVS model that filters false data by verifying whether sensing data detected by sensors and IoT is within a preset error range.

B. Assumption

We assume that a sufficient amount of normal data is accumulated in a Data Calibration-based DEVS model proposed in this paper.

C. Proposed Scheme

Chapter 3 is structured as follows. Section 3.3.1 of this paper explains the System Entity Structure (SES) of the Broadcast Model (BM) – (WSNS based IoT) WI model, and Section 3.3.2 describes the structure of the BM-WI model and the State Transition Diagram and Timing Diagram of each atomic model.

I. Model Design

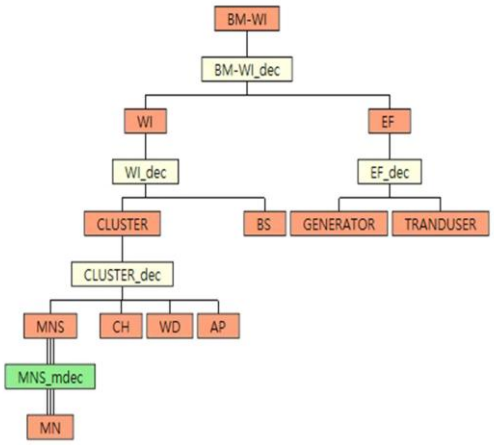

Fig. 3 SES of the BM-WI model

The WSNs-based IoT air purification system can perform a normal indoor air purification operation using the Data Calibration-based DEVS model. However, if an attacker injects false data into the IoT air purifier, an incorrect fine dust value is transmitted to the IoT Window and the air purification operation is not executed properly. To solve this problem, a Data Calibration-based DEVS model is proposed in this paper in which the operation execution of the IoT device is determined after checking whether the sensing data values are normal. The proposed scheme of the BM-WI is verified through DEVS simulation. Fig. 3 presents the SES of the BM-WI model.

II.Model Definition

In this paper, objects existing in the real world were modeled and simulated to verify the performance of the proposed scheme. The WI model consists of a Cluster model that acts as a cluster of WSNs and a BS model that provides users with useful services by receiving event reports. The Cluster model consists of an MN model that acts as member nodes, a Cluster Head (CH) model that acts as a cluster head, a WD model that acts as an IoT window, and an AP model that acts as an IoT air purifier.

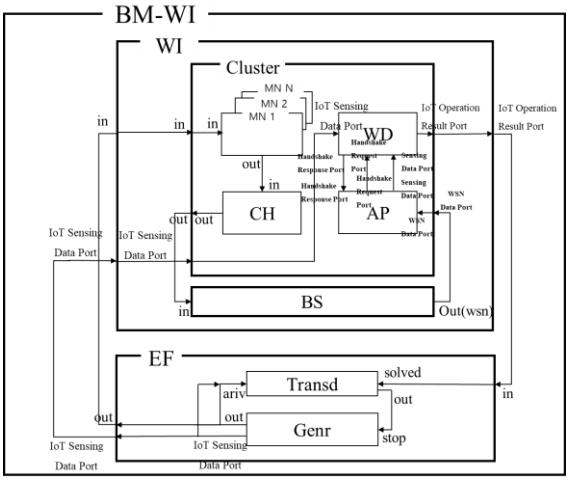

Fig. 4 The structure of the BM-WI model

Fig.4 shows the structure of the BM-WI, WSNs-based air purification IoT Model. The BM-WI consists of multiple coupled models, atomic models, and packets of all models are transmitted through input and output ports. In the EF model, the GENR model randomly generates events and the TRANSD model measures the processing results of the BM-WI model. The MN model transmits sensing data values with attached Message Authentication Code (MAC) to the CH model to maintain the integrity of the transmitted message. The CH model verifies the MACs using the pairwise key shared with the MN model. If MAC verification succeeds, the CH model transmits MAC and sensing data values of the WSNs to the BS model. The BS model verifies the MACs using the individual key shared with the CH model. If MAC verification succeeds, the BS model transmits sensing data values of the WSNs to the AP model through the out port.

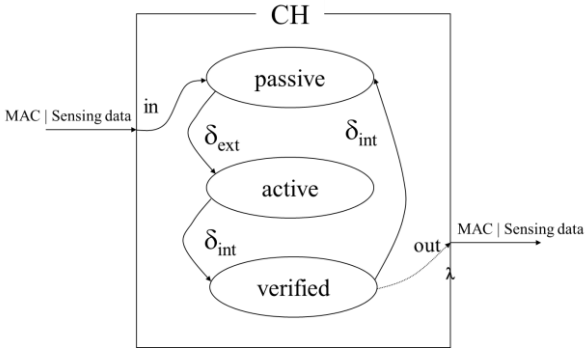

Fig. 5 State Transition Diagram of the CH model

Fig. 5 shows the state transition diagram of the CH model. The CH model has passive, active, and verified states. The CH model to receive event information from the MN model through the in port changes to the active state. Finally, the CH model transmits the current event information of the WSNs to the BS model through the out port.

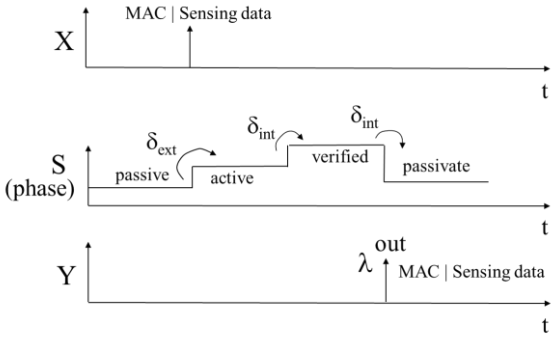

Fig. 6 Timing Diagram of the CH model

Fig. 6 shows the timing diagram of the CH model. In the CH model, Input(X) is transmitted through the in port and switches to the active state. Then it verifies the MAC using the pairwise key shared with the MN model.

If it succeeds in MAC verification, it switches to the verified state and the Output(X) is transmitted to the BS model through the out port. The content of the transmitted message is the MAC and the sensing data value of the WSNs.

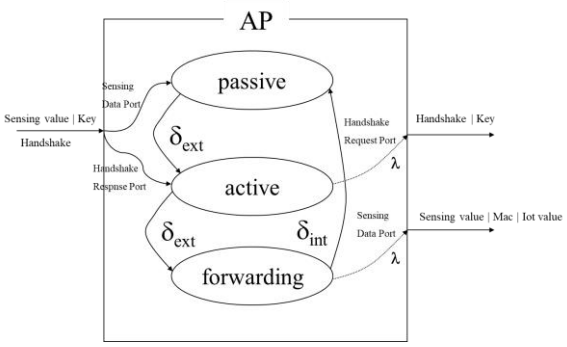

Fig. 7 State Transition Diagram of the AP model

Fig. 7 shows the state transition diagram of the AP model. The AP model has passive, active, and forwarding states. First, if the AP model receives a message from the BS model through the Sensing Data Port, it switches to the active state and transmits a handshake message and a symmetric key to the WD model through the Handshake Request Port. Second, if it receives a handshake message from the WD model through the Handshake Request Port, it switches to the forwarding state and transmits the sensing data to the WD model through the Sensing Data Port.

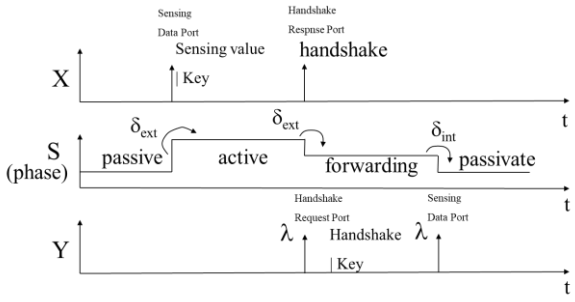

Fig. 8 Timing Diagram of the AP model

Fig. 8 shows the timing diagram of the AP model. First, the AP model switches to the active state if Input(X) is transmitted through the Sensing Data Port and prepares a handshake by transmitting a handshake request message and a symmetric key to the WD model through the Handshake Request Port. Second, if the AP model receives a handshake response message from the WD model through the Handshake Request Port, it verifies whether the content of the message is a handshake response message. If the handshake response message is correct, the AP model switches to the forwarding state and transmits to the WD model after encrypting data using the symmetric key through the Sensing Data Port.

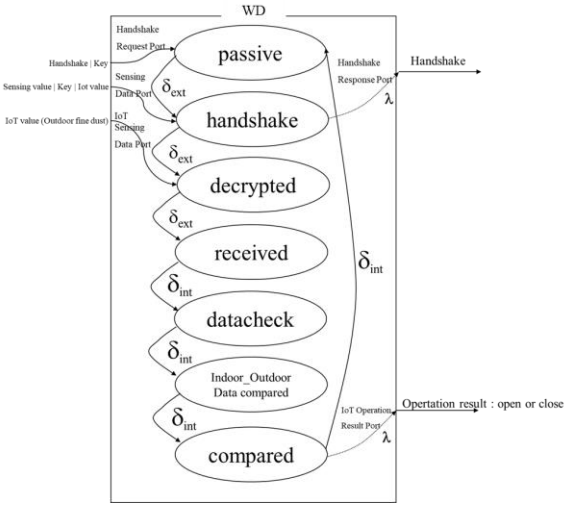

Fig. 9 State Transition Diagram of the WD model

Fig. 9 shows the state transition diagram of the WD model. The WD model has passive, handshake, decrypted, received, datacheck, Indoor_Outdoor Data compared, and compared states. If the WD model receives a handshake request message and the symmetric key from the AP model through the Handshake Request Port, it switches to the handshake state and transmits a handshake response message to the AP model through the Handshake Response Port. Also, if the WD model receives a sensing data value (indoor fine dust value) detected by sensor nodes from the AP model through the Sensing Data Port, it switches to the decrypted state. If the WD model receives a sensing data value of IoT through the IoT Sensing Data Port, it switches to the received state. If the WD model switches to the datacheck state, it checks whether the sensing data values of the WSNs and IoT is within the preset error range. If the sensing data value is within the preset error range, the WD model determines the Open or Close operation of the IoT Window by comparing the indoor fine dust value with the outdoor fine dust value detected by the WD model. Finally, the Open and Close operations of the IoT Window are printed through the IoT Operation Result port.

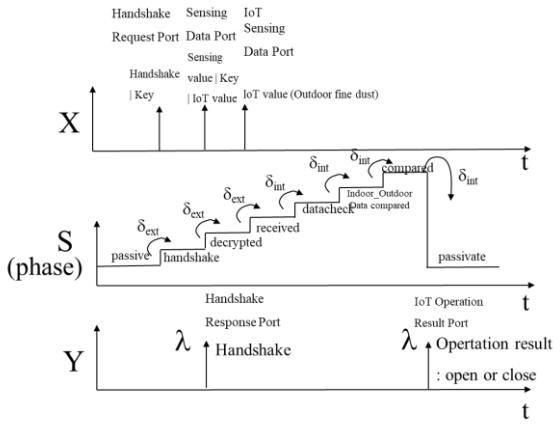

Fig. 10 Timing Diagram of the WD model

Retrieval Number: 100.1/ijeat.F30770810621
DOI:10.35940/ijeat.F3077.0810621
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

Fig. 10 shows the timing diagram of the WD model. All inputs of the WD model are transmitted through Handshake Request Port, Sensing Data Port and IoT Sensing Data Port. First, the WD model receives Input(X) through the Handshake Request Port. The WD model acquires a pairwise key shared with the AP model and switches to the handshake state after checking whether the handshake message is correct. Also, the handshake response message is transmitted to the AP model through the Handshake Response Port. Second, the WD model receives Input(X) from the AP model through the Sensing Data Port and the content of Input(X) is the sensing data values of the WSNs encrypted by the symmetric key. Therefore, if decryption of data succeeds using the symmetric key, the state is switched to the decrypted state. Third, if the WD model receives sensing data values of IoT through the IoT Sensing Data Port, the state is switched to the received state. Fourth, it switches from the received state to the datacheck state and checks whether the sensing data values of the WSNs and IoT are within the preset error range. If the indoor fine dust is within the preset error range, the IoT window determines whether to open or close by comparing the outdoor fine dust value with the indoor fine dust value. Finally, it outputs whether the IoT window is open or closed through the IoT Operation Result Port.

IV. EXERPERIMENTAL RESULTS

Table- I: The security comparison of security protocols

Type of attacks	Security Protocol		
	IHA	*SSL/TLS*	*Proposed Scheme*
False report injection that the number of compromised nodes exceeds security threshold	No[a]	No	Yes
False report injection that the number of compromised nodes is less than security threshold	Yes	No	Yes
False data injection	No	No	Yes
IoT abnormal behavior	Yes	Yes	Yes
Security method	Authentication	Authentication	Integrity check of data

Table 1 shows the performance of IHA, the SSL/TLS and the proposed scheme. To compare the performance of the IHA, SSL/TLS and the proposed scheme, an event was generated 1000 times and the security was analyzed accordingly. When a false data injection attack occurs, the symmetric key is stolen by the attacker, and multiple false data is generated using it. Since the existing SSL/TLS encrypts and decrypts using a symmetric key, it cannot be protected, and thus there is a problem in that it may cause an abnormal operation of the IoT device. However, the proposed scheme verifies whether the fine dust value detected by the WSNs and IoT is normal using the DEVS model based on Data Calibration, so it is possible to filter false data as well as determine whether to execute an operation based on the sensing data. There is an advantage in that it is possible to prevent the execution of an abnormal operation of the IoT device. Therefore, it can be seen that the security is strengthened in the proposed scheme as compared to the existing SSL/TLS. When a false report injection attack occurs, the attacker compromises the sensor node to steal the authentication key and injects the false report into the network. Existing IHA can detect false report injection attacks that the number of compromised nodes is under the security threshold. However, since a false report injection attack that the number of compromised nodes goes beyond the security threshold cannot be detected, it can be delivered to the IoT device through the BS and cause abnormal behavior. However, since the proposed method checks the integrity of the sensing data, it is possible to filter out false data as well as prevent abnormal behavior of IoT devices.

V. CONCLUSION

In the WSNs-based air purification IoT system, if a false data injection attack occurs, the existing SSL/TLS encryption/decryption symmetric key is stolen, so it cannot filter false data, and can also cause abnormal behavior of IoT devices. This problem causes the security of the whole system to be weakened. In order to solve this problem, the proposed scheme uses the Data Calibration-based DEVS model to prevent false data injection attacks that cannot be defended by the existing SSL/TLS, so that it is possible to prevent abnormal operation of the IoT devices. Therefore, it is possible not only to strengthen the overall security of the WSN-based air purification IoT system, but also to utilize the normal data accumulated in the DEVS model to develop an intelligent knowledge system. However, it has a disadvantage in the additional processing cost for verifying the integrity of the sensing data.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2021R1A2C2005480)

REFERENCES

1. Kang, Dongmug, and Jong-Eun Kim. "Fine, ultrafine, and yellow dust: emerging health problems in Korea." Journal of Korean medical science
2. Chang, Sei, and Kisik Jeong. "A Mobile Application for Fine Dust Monitoring System." 2017 18th IEEE International Conference on Mobile Data Management (MDM). IEEE, 2017.
3. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006)
4. Akyildiz, Ian F., et al. "A survey on sensor networks." IEEE Communications magazine 40.8 (2002): 102-114.
5. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.
6. Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 (2015): 2347-2376.
7. E. Rescorla, SSL and TLS: Designing and Building Secure Systems. Addison-Wesley Reading, 2001.
8. Wagner, David, and Bruce Schneier. "Analysis of the SSL 3.0 protocol." The Second USENIX Workshop on Electronic Commerce Proceedings. Vol. 1. No. 1. 1996.

9. Ye-lim Kang and Tae-ho Cho.“Detection of False Report Injection At Wsns Based on Data Calibration in Iot Environment.” International Journal of Recent Technology and Engineering (IJRTE) 8.4(2019): 8956-8960.
10. Bernard P. Object-oriented simulation with hierarchical, modular models: inteligent agents and endomorphic systems. Academic pres, 2014.
11. Concepcion, Arturo I., and Bernard P. Zeigler. "DEVS formalism: A framework for hierarchical model development." IEEE Transactions on Software Engineering 14.2 (1988): 228-241.
12. Lin, Jie, et al. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." IEEE Internet of Things Journal 4.5 (2017): 1125-1142.

AUTHORS PROFILE

Ye-lim Kang received her B.S. degree in Information and Communication Engineering from Sungkyul University, Korea, in February 2018. She is currently a master student in the Information and Communication Engineering at Sungkyunkwan University, Korea. Her research interests include internet of things, artificial intelligence, wireless sensor network and network security.

Tae-ho Cho received his Ph.D. in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical Engineering from Sungkyunkwan University, Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Computing at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, intelligent systems, modeling and simulation, and enterprise resource planning.