International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249 – 8958 (Online), Volume-9 Issue-4, April 2020

Fuzzy-based Dynamic Security Parameters Determination Method to Improve Energy Efficiency

Ye-lim Kang, Tae-ho Cho

Abstract*: Fine dust is a harmful substance that floats in the atmosphere. It is not filtered well in the bronchus and causes health problems when it accumulates in the body. Fine dust that is present in the air outside can flow into buildings through windows and other openings, adversely affecting indoor air quality. It has negative health effects on people who live indoors. As attention to problems associated with fine dust gradually rises, the importance of continuously managing the quality of indoor air through air purification rises. Therefore, recently, research and development into systems to periodically purify indoor air are being carried out. This paper introduces an air purification system, a Wireless Sensor Networks (WSNs)-based Internet of Things (IoT) air purification system. In the WSNs-based IoT air purification system, the IoT air purifier is controlled based on event information that the WSNs senses, so it is important to maintain the security of the event information. To this end, a WSNs security protocol, Interleaved Hop by hop Authentication (IHA), is used in this system. IHA is a security protocol in which sensor nodes and a Base Station (BS) detect and drop false reports if the number of compromised sensor nodes does not exceed a security threshold. That is, because the false report injection attack that the number of compromised sensor nodes exceeds security threshold can't defend by IHA, it is detected and defended through Data Calibration. However, considerable energy of the sensor nodes is unnecessarily consumed in the process of forwarding false reports. Thus, this paper proposes a method of decreasing and increasing security thresholds dynamically according to the network situation using fuzzy logic. This proposed scheme has the advantages of improvements in both the overall energy efficiency and network lifetime in WSNs.

Keywords* : Security, *Wireless Sensor Networks, Internet of Things, Interleaved Hop-by-hop Authentication, False report injection attack,

I. INTRODUCTION

Fine dust is particulate material that floats in the atmosphere. Fine dust particles smaller than 10 μm in diameter are called PM10, and particles less than 2.5 μm in diameter (PM2.5) are called ultrafine particles [1]. Fine dust is mainly from car exhaust or burning of fuel, and smaller particles of fine dust are more harmful to the human body [2]. When outdoor fine dust, which is harmful to the human body, flows into a building, fine dust is mixed into the indoor air, and the quality of the indoor air is worsens, with negative effects on human health. Therefore, in response to health problems related to breathing polluted indoor air, the importance of periodically purifying and managing indoor air is being recognized increasingly, and research and development into air purification systems is ongoing. This paper introduces a recently developed air purification system, WSNs-based IoT air purification system.

A WSNs consists of thousands of sensor nodes and a BS [3]. Sensor nodes detect an event, and the BS receives information about the event from many connected sensor nodes. The BS then provides the user with the event information. WSNs are used in various fields, such as healthcare, military, and household appliances and devices. They are also useful for monitoring phenomena occurring in real time. The IoT is the network of devices such as refrigerators, smartphones and air conditioners that communicate through the internet and have built-in sensors and communication functionality [4-5]. The IoT is useful for controlling devices. A WSNs-based IoT system fuses WSNs and the IoT where the IoT device is controlled based on the event information sensed by the WSNs.

In the WSNs-based IoT air purification system, it is important to maintain the security of the event information sensed by the WSNs, so an IHA security protocol is used [6-7]. A false report injection attack where the number of compromised sensor nodes is less than the security threshold does not have an effect on executing normal operation of the IoT air purifier because false reports are detected early and dropped through en-route filtering in IHA [8]. However, in a false report injection attack where the number of compromised sensor nodes exceeds the security threshold, en-route filtering in IHA doesn't operate, so false reports are transmitted from the BS to the IoT air purifier, detected and dropped by Data Calibration[9]. However, in the process of transmitting false reports, the overall network lifetime of the WSNs is decreased by excessive energy consumption by the sensor nodes. In this paper, a method for dynamically adjusting the security threshold by considering energy and security according to the network situation using fuzzy logic is proposed to solve this problem [10-11]. The proposed scheme improves energy efficiency and security because of using a method for decreasing or increasing the security threshold according to the network situation.

Revised Manuscript Received on April 25, 2020.
* Correspondence Author
Ye-lim Kang, Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, Republic of Korea.
Tae-ho Cho*, Department of Computer Science and Engineering,

Compared to existing IHA, the proposed scheme shows, on average, a 5.53% improvement in the energy efficiency in a false report injection attack where the number of compromised sensor nodes is less than the security threshold. In addition, the proposed scheme shows an average improvement in energy efficiency of 25.28% in a false report injection attack where the number of compromised sensor nodes exceeds the security threshold. Thus, on the whole, energy is saved.

The composition of this paper is as follows. Chapter 2 describes IHA, Security threshold, Fuzzy logic, Fine dust, and IoT. Chapter 3 describes the proposed scheme. In Chapter 4, the performance of the proposed scheme is proven through experimental results. In Chapter 5, the conclusions are described.

II. RELATED WORKS

A. Interleaved Hop-by-hop Authentication

It is easy for an attacker to compromise sensor nodes because WSNs use wireless communication and are deployed in an open environment. The attacker compromises sensor nodes, acquires keys and generates a report using the keys. In a false report injection attack, the attacker injects the report into the WSNs. To defend against a false report injection attack, IHA was proposed by Zhu, Sencun, et al. IHA is a security protocol in which sensor nodes and the BS can verify the authenticity of the report using a Message Authentication Code (MAC) if the number of sensor nodes compromised by the attacker doesn't exceed the security threshold. The steps involved in IHA consist of 4 steps as follows.

i.Node Initialization and Deployment

The key server preloads individual keys in all sensor nodes. Each sensor node acquires an authentication key using an individual key and forms pairwise keys with neighborhood nodes located within one hop.

ii.Association Discovery

BS hello and Cluster Acknowledgement are initial steps for finding the association nodes of each sensor node. In BS hello, each sensor node finds an upper association node located within security threshold+1. In Cluster Acknowledgement, each sensor node finds a lower association node located within security threshold+1.

iii.Report Endorsement

If an event is generated, the Cluster Head (CH) node generates a report including pairwise MACs and individual MACs and transmits it to the BS.

iv.En-route Filtering

A forwarding node that receives the report from a CH verifies the report using pairwise keys and checks the number of pairwise MACs. If the number of pairwise MACs is right, each forwarding node generates MAC using a pairwise key shared with a lower association node and verifies pairwise MACs of the report. If the verification of pairwise MACs ends, the verified MAC is dropped in the report. Finally, the forwarding node generates a MAC using a pairwise key shared with an upper association node and transmits a report adding the MAC to the report. All forwarding nodes repeat this process when they transmit the report.

v.BS verification

If the report is transmitted to the BS, the BS verifies MACs using individual keys shared with all sensor nodes. If verification of MACs ends, the BS approves the report.

B. Security threshold

The security threshold of IHA is the number of MACs included in the report. If the security threshold increases, the verification count of MACs increases so the security is reinforced. However, the problem is that much more energy is consumed by the sensor nodes because the size of the report increases. On the other hand, if the security threshold decreases, the verification count of MACs decreases so security is weakened. However, the advantage is that energy is saved by the sensor nodes. Therefore, regulating the security threshold by properly considering security and energy usage according to the network situation is important when using IHA.

C. Fuzzy logic

Fuzzy logic takes a logic value between 0 and 1 rather than either 0 or 1 and deals with the ambiguity of the real world, reflecting people's language. For example, in the sentence "The height of that student is 170 cm. Is the student tall?" the sentence is ambiguous because tall height isn't defined; thus, it is called a fuzzy sentence. To use fuzzy logic, a fuzzy set is defined first, and input and output values through fuzzification should be converted into a membership function. The fuzzy set represents the degree to which each object belongs to a certain group in the membership function rather than representing that each object is definitely in a certain group. A set expressing the membership function together with a corresponding object is called a fuzzy set. Furthermore, each rule about input values through a fuzzy inference rule is examined and the calculation is operated to draw output values. Lastly, fuzzy output values drawn through defuzzification are converted into correct values. The Center of Gravity Method and Mamdani's inference method are methods of defuzzification [12].

D. Fine dust

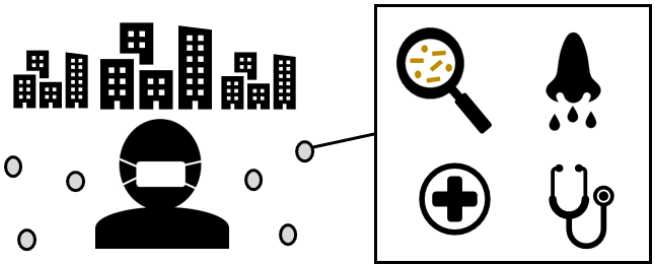

Fig. 1 Fine dust

Fine dust is particulate pollutants less than 10 μm in diameter (PM10) floating in the atmosphere. It is mainly generated by exhaust from cars or burning of fuel. Fine dust that has a particle size less than 2.5 μm in diameter is called PM2.5, or ultrafine particles. The smaller the particles, the worse it affects people's health. If fine dust flows indoors, it accumulates in the bronchus of people who live indoors and can cause infections such as pneumonia.

In particular, PM10 is a main cause of various respiratory diseases. Therefore, research and development into indoor air purification systems are actively progressing.

E. Internet of Things

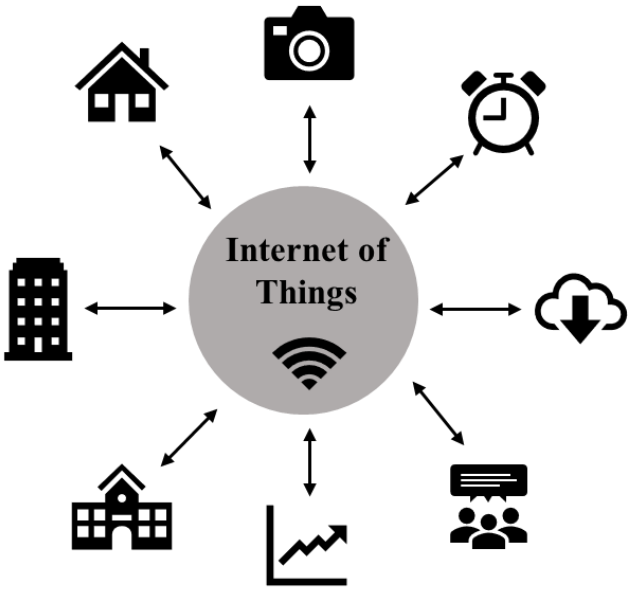

Fig. 2 Internet of Things

IoT is the technology connects appliances and devices with built-in sensors and communication modules, such as refrigerators, air conditioners, and clocks, on the internet through wireless communication. Internet-connected devices determine run of the device using data that are transferred between devices. Devices apply an artificial intelligence algorithm and they can provide the user with many services. IoT devices are internet-connected, so they are a main target of various types of security attacks such as hacking. Recently, research on this security threat has emerged as a new issue.

III. PROPOSED SCHEME

A. Problem Statement

In IHA, if the security threshold is increased, the verification count of MACs also increases by the security threshold so that security is reinforced. However, the energy of sensor nodes is unnecessarily consumed so there is a disadvantage that the overall lifetime of the network decreases. On the other hand, if the security threshold decreases, the verification count of MACs also decreases by the security threshold so security is weakened, but the overall lifetime of the network increases. In existing IHA security and energy are not adjusted according to the network situation because a fixed security threshold is used. Therefore, it is important to adjust security and energy, setting up a proper security threshold according to the network situation.

B. Assumption

For Data Calibration of the IoT air purifier, we assume that enough data is accumulated in the IoT air purifier. The BS needs to know Energy of each sensor node, Hop Count, False Traffic Ratio (FTR), and the number of compromised sensor nodes to dynamically adjust the security threshold. Thus, we assume that the BS asks each sensor node to know the corresponding values.

C. Proposed Scheme

I. Fuzzy System

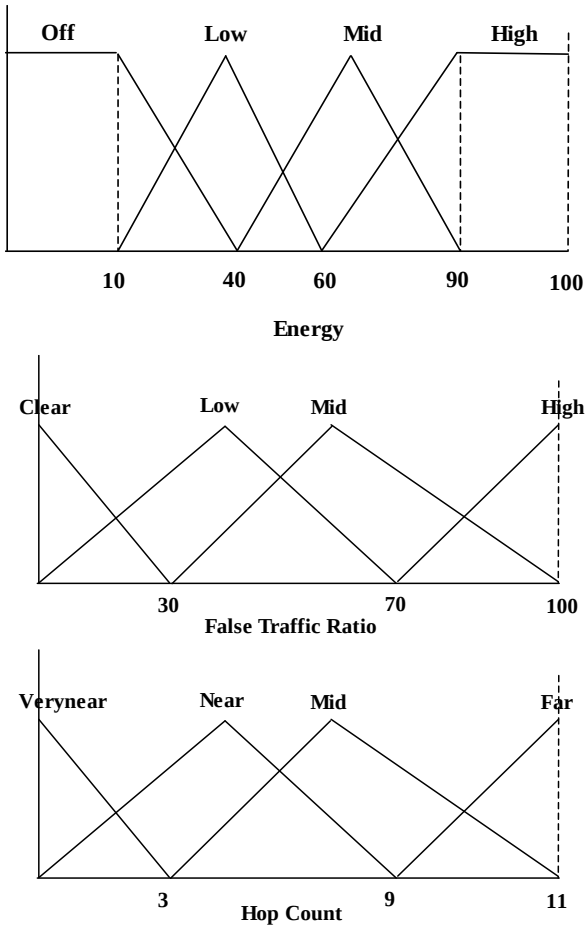

Fig. 3 Fuzzy input membership function

In this paper, in a WSNs-based IoT air purification system, the method used to determine the security threshold by using the fuzzy system was proposed to determine an efficient security threshold according to the network situation. The BS and IoT air purifier use various input factors, such as Energy of the sensor node, FTR, Hop Count into the fuzzy system and output proper security threshold. The output of the fuzzy system, security threshold is output in the form of Down, Maintain, Up. Lastly, the BS and IoT air purifier decide which number to increase or decrease security threshold checking output of the fuzzy system and either the number of compromised sensor nodes or the current security threshold. Lastly, the BS and IoT air purifier determine how to increase or decrease the security threshold by checking the output of the fuzzy system and either the number of compromised sensor nodes or the current security threshold. The fuzzy input membership function is shown in Fig. 3.

II. Fuzzy Rule

i. False report injection attack where the number of compromised sensor nodes is less than the security threshold, occurance of a normal event

- RULE 58: IF (Energy IS High) AND (FTR IS Mid) AND (HopCount IS Mid) THEN (Threshold IS Maintain);
- RULE 59: IF (Energy IS High) AND (FTR IS Mid) AND (HopCount IS Far) THEN (Threshold IS Maintain);
- RULE 60: IF (Energy IS High) AND (FTR IS High) AND (HopCount IS Verynear) THEN (Threshold IS Down);
- RULE 61: IF (Energy IS High) AND (FTR IS High) AND (HopCount IS Near) THEN (Threshold IS Down);

ii. False report injection attack where the number of compromised sensor nodes exceeds security threshold.

- RULE 36: IF (Energy IS Mid) AND (FTR IS Low) AND (HopCount IS Verynear) THEN (Threshold IS Maintain);
- RULE 37: IF (Energy IS Mid) AND (FTR IS Low) AND (HopCount IS Near) THEN (Threshold IS Maintain);
- RULE 38: IF (Energy IS Mid) AND (FTR IS Low) AND (HopCount IS Mid) THEN (Threshold IS Up);
- RULE 39: IF (Energy IS Mid) AND (FTR IS Low) AND (HopCount IS Far) THEN (Threshold IS Up);

III. Operation process

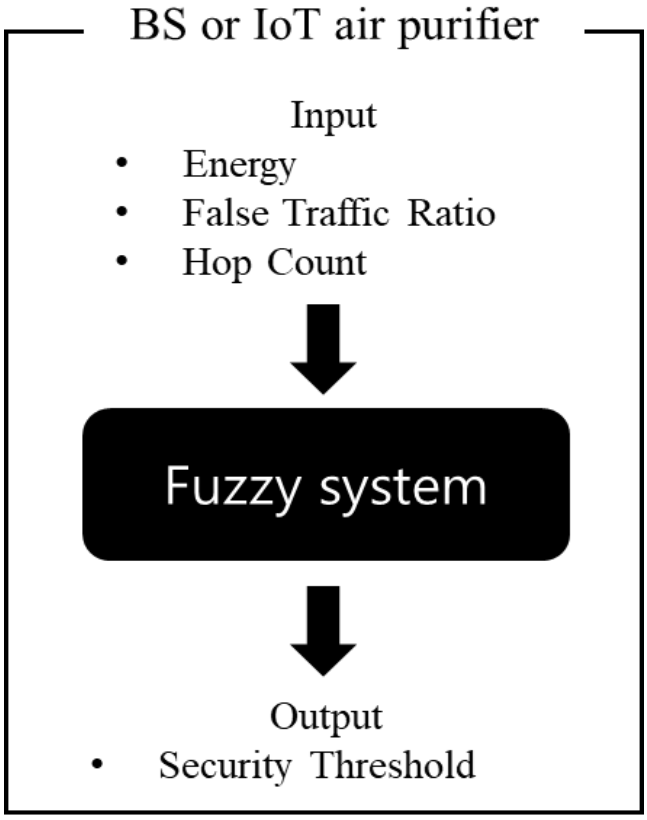

Fig. 4 Fuzzy system

Fig. 4 shows that the BS or IoT air purifier puts Energy, False Traffic Ratio, and Hop Count into the fuzzy system as input factors and outputs the proper security threshold according to the network situation.

If a normal event occurs, the BS acquires the output from the fuzzy system, either Down or Maintain. If Down is the output, the fuzzy system decides how much to decrease the security threshold by referring to the current security threshold. If Maintain is the output, the current security threshold is fixed.

If a false report injection attack occurs where the number of compromised sensor nodes is less than the security threshold, the false report is detected and dropped by either sensor nodes or BS. Then, the BS executes the fuzzy system. Down or Maintain is output by the fuzzy rules. If Down is output, the fuzzy system decreases the security threshold, referring to the number of compromised sensor nodes, and remains secure with improved energy efficiency. If Maintain is output, the current security threshold is fixed.

If a false report injection attack occurs where the number of compromised sensor nodes exceeds the security threshold, the false report is transmitted to the IoT air purifier through the BS, is detected and dropped by Data Calibration. If the false report is detected by the IoT air purifier, the fuzzy system is executed and either Up or Maintain is output. If Up is output, the fuzzy system reinforces the security by increasing the security threshold and improves the energy efficiency. If Maintain is output, the current security threshold is fixed.

IV. CHANGE OF SECURITY THRESHOLD

When the fuzzy system is executed by the BS or IoT air purifier and the security threshold is reset, the BS and IoT air purifier change the security threshold referring to the number of compromised sensor nodes of the current attacked cluster or the current security threshold and reset pairwise keys of association nodes.

V. PERFORMANCE EVALUATION

A. Experimental environment

Table- I: Experimental environment

Parameter		Value
Field Size		1000 m x 1000 m
Cluster Size		50 m x 50 m
Number of Nodes		2000
Number of Cluster Head Nodes		400
MAC Size		1 byte
Energy Consumption [13]	Transmission	16.25 µJ (per 1 byte)
	Reception	12.5 µJ (per 1 byte)

	Report Generation	70 µJ
	MAC Generation	15 µJ
	MAC Verification	75 µJ
Security Threshold		2-4

B. Experiment results

- False report injection attack where the number of compromised sensor nodes is less than the security threshold

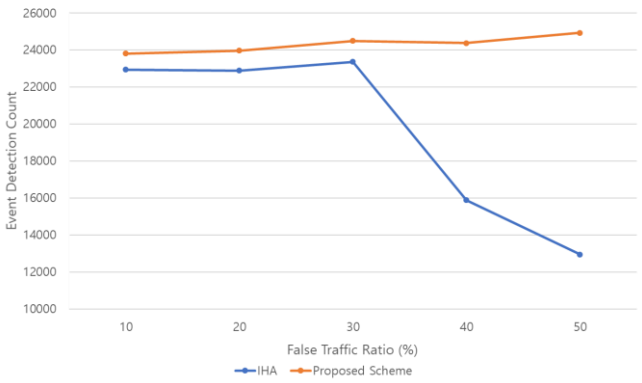

Fig. 5 Event Detection Count according to FTR

Table- II: Event Detection Count according to FTR

FTR	Event Detection Count
60	11140
70	9591
80	8362
90	7352
100	6679

Fig. 5 and Table- II show event detection counts according to FTR in a false report injection attack where the number of compromised sensor nodes is less than the security threshold. To compare existing IHA with the proposed scheme, we generated events at random positions until there was one sensor node with 10% or less remaining and analyzed the event detection count according to FTR. The existing IHA uses a fixed security threshold and in the proposed scheme, the existing security threshold is decreased or maintained according to the network situation determined by the fuzzy system. Because the proposed scheme uses a dynamic security threshold, it saves energy compared to the existing IHA so the event detection count increases.

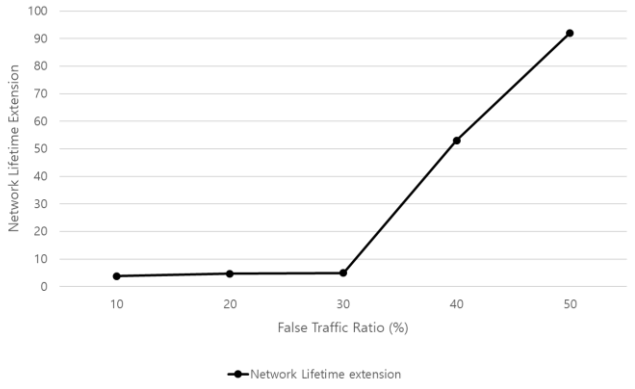

Fig.6 Network Lifetime Extension according to FTR

Table- III: Network Lifetime Extension according to FTR

FTR	Network Lifetime Extension
60	1.9
70	3.1
80	1.6
90	1.5
100	1.3

Fig. 6 and Table- III show network lifetime extension according to FTR in a false report injection attack where the number of compromised sensor nodes is less than the security threshold. To compare the existing IHA with the proposed scheme, we generated events at random positions until there was one sensor node with 10% or less remaining energy. We analyzed the network lifetime extension according to FTR. Because the proposed scheme uses a dynamic security threshold, it properly adjusts security and energy according to the network situation, saving total energy comparing to the existing IHA. Therefore, network lifetime extension increases. It can be seen that the proposed scheme shows, on average, 16.85% network lifetime extension compared to the existing IHA.

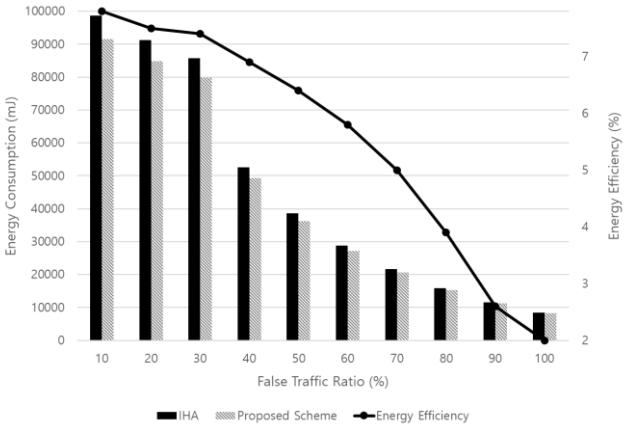

Fig. 7 Energy Consumption according to FTR

Fig.7 shows total the energy consumption according to FTR in a false report injection attack where the number of compromised sensor nodes is less than the security threshold. To compare the existing IHA with the proposed scheme, we generated 6591 - 22945 events at random positions and analyzed the total energy consumption according to FTR. Energy consumption decreases as FTR increases. If a false report that the number of compromised sensor nodes is less than the security threshold is injected into the network, the false report is filtered early on by sensor nodes. At this time, the proposed scheme properly saves energy according to the network situation by decreasing or maintaining the security threshold, and security is maintained. Therefore, the proposed scheme is energy-efficient compared to the existing IHA. Through this, it can be seen that the proposed scheme shows an average improvement in energy efficiency of 5.53% compared to the existing IHA.

- False report injection attack where the number of compromised nodes exceeds the security threshold

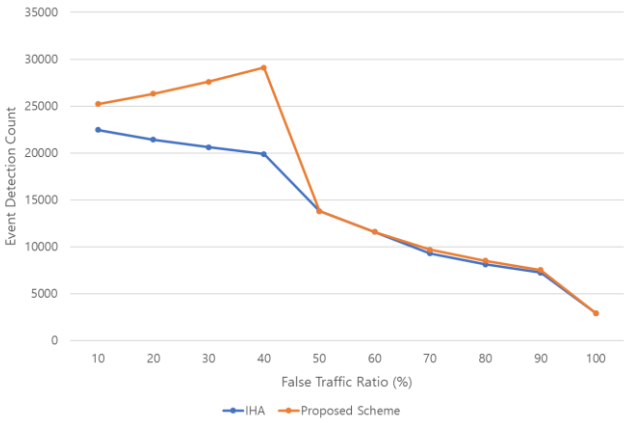

Fig. 8 Event Detection Count according to FTR

Fig. 8 shows total event detection count according to FTR in a false report injection attack where the number of compromised nodes exceeds the security threshold. The existing IHA doesn't perform en-route filtering in a false report injection attack where the number of compromised nodes exceeds security threshold. Thus, the false report is transmitted to the BS and the false report isn't filtered early on. However, in the proposed scheme, the security threshold dynamically increases or maintains according to the network situation as determined by the fuzzy system, so this attack is caught early and security is reinforced. The total energy use is decreased and the event detection count increases.

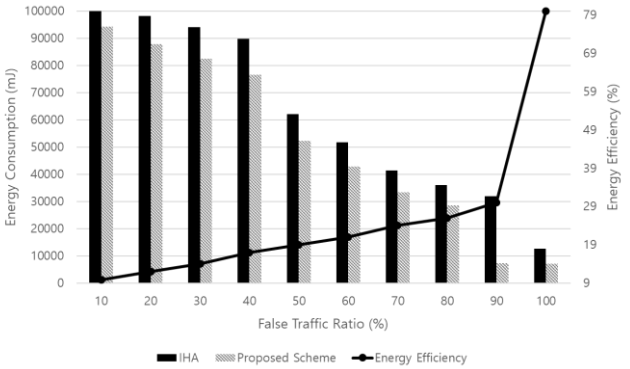

Fig. 9 Energy Consumption according to FTR

The total energy consumption according to FTR in a false report injection attack where the number of compromised nodes exceeds the security threshold is as shown Fig9. To compare existing IHA with the proposed scheme, we generated 2933-22481 events at random positions and analyzed total energy consumption according to FTR. As the FTR increases, energy consumption decreases and energy efficiency increases. The proposed scheme shows that the energy efficiency is improved by 25.28%, on average, compared to the existing IHA.

VI. CONCLUSION

Air purification systems applying existing IHA use a fixed security threshold. In this network situation, if a false report injection attack occurs where the number of compromised sensor nodes is less than the security threshold, the false report can be detected and dropped through en-route filtering. However, in a false report injection attack where the number of compromised sensor nodes exceeds the security threshold, en-route filtering of IHA does not operate, so the false report is transmitted to the IoT air purifier through the BS. There are problems that interrupt normal operation of an IoT air purifier, and the network lifetime decreases because the energy of sensor nodes is consumed unnecessarily. To solve this problem, in this paper, a method was proposed for determining appropriate security thresholds for the network situation. This proposed scheme has an advantage that if the BS or IoT air purifier detects a normal event or false report injection attack, the energy efficiency of the network is improved by decreasing or increasing the security threshold in response to execution of the fuzzy system, and security is adjusted. However, the proposed scheme has a disadvantage of additional overhead, with increased cost of message processing.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2018R1D1A1B07048961)

REFERENCES

1. Kang, Dongmug, and Jong-Eun Kim. "Fine, ultrafine, and yellow dust: emerging health problems in Korea." Journal of Korean medical science 29.5 (2014): 621-622.
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. Akyildiz, Ian F., et al. "A survey on sensor networks." IEEE Communications magazine 40.8 (2002): 102-114.
4. 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.
5. Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.
6. Zhu, Sencun, et al. "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004. IEEE, 2004.
7. Zhu, Sencun, et al. "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks." ACM Transactions on Sensor Networks (TOSN) 3.3 (2007): 14.
8. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).
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. Zadeh, Lotfi Asker. "Fuzzy sets as a basis for a theory of possibility." Fuzzy sets and systems 1.1 (1978): 3-28.
11. Lee, Chuen-Chien. "Fuzzy logic in control systems: fuzzy logic controller. II." IEEE Transactions on systems, man, and cybernetics 20.2 (1990): 419-435.
12. Mamdani, Ebrahim H., and Sedrak Assilian. "An experiment in linguistic synthesis with a fuzzy logic controller." International journal of man-machine studies 7.1 (1975): 1-13.
13. Ye, Fan, et al. "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on Selected Areas in Communications 23.4 (2005): 839-850.

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.