International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Detection of False Report Injection At Wsns Based on Data Calibration in Iot Environment

Ye-lim Kang, Tae-ho Cho

Abstract*: Unlike ordinary dust, fine dust has a small particle size and is thus not well-filtered out of the human nose or bronchus. It accumulates in the human body where it can generate various respiratory and bronchial illnesses. If this fine dust is introduced into a room from the outside, the indoor air is worsened which has negative effects on the health of the people there. The continuous management of indoor air through air purification is necessary to protect the health of students, office workers, and others who spend most of the day indoors. Various air purification systems exist for this purpose, and research and development are actively progressing. This paper discusses an indoor air purification system that uses Internet of Things (IoT) based on Wireless Sensor Networks (WSNs). In such a system, false reports are generated when the number of sensor nodes compromised by an attacker exceeds the security threshold. The WSNs security protocol, Interleaved Hop-by-hop Authentication (IHA), cannot defend against such false reports, resulting in abnormal behavior of the IoT air cleaner. Therefore, a false report detection scheme that uses sensing data is proposed in this paper. When fine dust occurs, the WSNs and IoT air cleaner sense fine dust at the same time. The IoT air cleaner, which has normally received the WSNs event report, calculates the average and the deviation about the cumulative fine dust sensing data values of the WSNs and the IoT. Then, it compares the deviation for the current event with the deviation for the previous event to calculate the variation of deviation. If the variation of deviation is within a predetermined error range, it is determined that a normal event occurs. Otherwise, it is determined that the false report injection attack occurs and it is prevented from running abnormal behavior of it. In conclusion, this scheme not only improves security by preventing the IoT air cleaner from running abnormally, but also contributes to improved energy efficiency in the WSNs.

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

I. INTRODUCTION

Fine dust is defined to be less than 10 um in diameter and is generated by artificial processes such as the burning of fuel [1]. Since fine dust is not discharged in a human's bronchi, it accumulates in the body where it can cause various respiratory diseases [2]. If this dust is introduced indoors, carbon dioxide accumulates and the indoor air becomes polluted, which can seriously affect the health of the people there. Therefore, there are many systems that automatically purify indoor air by sensing fine dust to manage indoor air quality. Research and development are also actively underway. This paper discusses an indoor air purification system that uses WSNs-based IoT to maintain a pleasant indoor environment by efficiently controlling indoor fine dust. WSNs consist of hundreds to thousands of sensor nodes and a base station (BS) [3]. The sensor nodes detect an event, generate an event report and transmit it to the BS. Then the BS forwards the received event report to the user. IoT is a technology that connects the internet to physical objects through embedded sensors and wireless communication functions [4-5]. Objects that can be connected to the internet are known as IoT devices, and include common household items such as washers, cameras, and refrigerators. The behavior of an IoT device is determined based on its interactions with other connected devices.

A combination of a WSNs and IoT is called a WSNs-based IoT system. A WSNs is deployed throughout a large region to detect events and an IoT device executes behaviors based on the event information it receives. Because they use wireless communication, WSNs can be deployed in an open environment and are vulnerable to false report injection attacks [6]. WSNs implement a security protocol called IHA to defend against such attacks. In the IHA scheme, sensor nodes and the BS can detect false reports if the number of sensor nodes compromised by the attacker does not exceed the security threshold (T) [7-8]. However, when the number of sensor nodes compromised by the attacker exceeds T, a false report is generated and forwarded to an IoT air cleaner through the BS. This causes the IoT air cleaner to run abnormally and be unable to correctly manage indoor air quality. Thus, people may be exposed to bad air and develop health problems such as respiratory disease. In this paper, to prevent an IoT air cleaner from running abnormally, we propose a security scheme to detect false report injection attacks using sensing data. If an IoT air cleaner receives an event report from the WSNs, it begins data calibration, which verifies that the data detected by its own fine dust sensor and the sensing data of the WSNs are within a predetermined error range. If the data calibration result is within the predetermined error range, the IoT air cleaner runs normal behavior. On the other hand, the IoT air cleaner does not run command if the result of data calibration is not within the predetermined error range.

Manuscript published on November 30, 2019.
* 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, Sungkyunkwan University, Suwon, Republic of Korea.

Data calibration can prevent physical failure of the fine dust sensor in the IoT air cleaner, as well as abnormal behavior. The proposed scheme shows an energy improvement of up to 38% and a false report filtering ratio of 100% compared to IHA.

As a result, energy is saved and security is improved.The remainder of this paper is as follows. In Section 2, false report injection attack, IHA, IoT, and fine dust are explained. In Section 3, the proposed scheme is introduced. In Section 4, the performance of the proposed scheme is described through experimental results. Section 5 contains our conclusions and future works.

II. RELATED WORK

A. False report injection attack

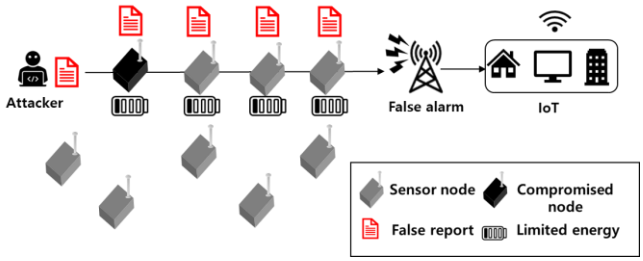

Fig. 1. False report injection attack

Fig. 1 shows a false report inject attack, which is a security attack that can occur in WSNs. The attacker compromises sensor nodes and injects a false report about an event that did not occur into the sensor node. When the false report injected by the attacker is forwarded to the BS, the sensor nodes unnecessarily consume energy, which contributes to the shortening of the lifetime of the WSNs. Finally, when the BS receives the false report, a false alarm occurs in the BS. Therefore, WSNs apply various security protocols, such as Probabilistic Voting-based Filtering Scheme, Dynamic En-route scheme for Filtering false data injection, and IHA, to defend against false report injection attacks [9-10].

B. Interleaved Hop-by-hop Authentication (IHA)

The IHA is a security protocol used in WSNs. It uses for sensor nodes and a BS to verify the authenticity of an event report using a message authentication code (MAC). The protocol consists of node initialization and deployment, association discovery, report endorsement, en-route filtering and BS verification.

i. Node initialization and deployment

The key server preloads a unique ID and an individual key shared from the BS to all sensor nodes. Each node acquires an authentication key using a preloaded individual key and establishes the pairwise key with one-hop neighbor nodes [11].

ii. Association discovery

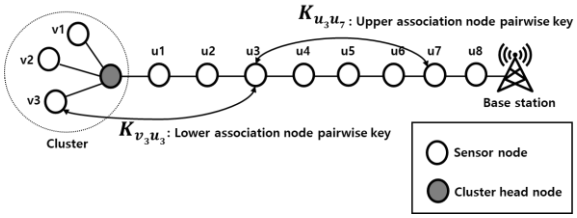

Fig. 2. Association discovery

Fig. 2 illustrates the association discovery step used to find the association nodes for each sensor node. For the setup of the initial path, all sensor nodes perform a base station hello to find an upper association node and cluster acknowledgement to find a lower association node.

iii. Report endorsement

If an event occurs, member nodes of the cluster generate a MAC using an authentication key and the pairwise key. The nodes then generate an endorsement message that includes the MACs and transmit it to a Cluster Head (CH) node. A CH node authenticates the endorsement message using the pairwise key shared with member nodes of the cluster and transmits the event report to the BS after generating the event report that includes all MACs.

iv. En-route filtering

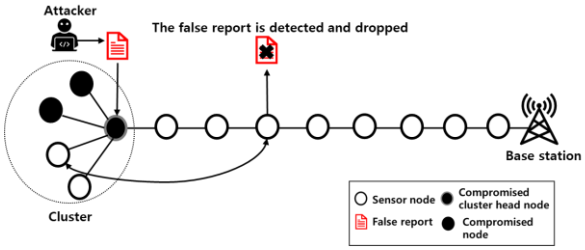

Fig. 3. En-route filtering

Fig. 3 shows en-route filtering being used to verify an event report. The node receiving the event report from the CH node verifies the event report using the pairwise key shared with the child node. It also checks whether the number of pairwise MACs in the event report is correct. If the number of pairwise MACs is correct, the sensor node generates a MAC using the pairwise key shared with a lower association node and verifies whether a MAC in the event report and the generated MAC are equal. If the verification succeeds, the verified MAC is removed from the event report, the sensor node generates a MAC using the pairwise key shared with an upper association node, then adds the MAC to the event report, and transmits the event report to the BS.

v. BS verification

If the event report is forwarded to the BS, the BS verifies the individual MACs in the event report using an authentication key. If the verification succeeds, the event report is authenticated. Otherwise, the event report is dropped.

C. Internet of Things (IoT)

IoT is an environment in which objects are connected through wireless communication and interact to make decisions, thus providing a user with intelligent service. Since an IoT device contains an embedded sensor or wireless communication module, it can determine its own behavior based on data detected by the sensor or data forwarded from other IoT devices.

Retrieval Number: D9746118419/2019©BEIESP
DOI:10.35940/ijrte.D9746.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Because IoT is connected to the Internet, it is convenient to manage the collected information and control the IoT devices. The user can operate the IoT device in a manner appropriate to the situation by setting conditions that determine its behavior. As IoT technology has evolved, it has become possible to construct systems that can more accurately control IoT devices in various environments, such as in the home and medical field.

D. Fine dust

Fine dust occurs naturally, but is usually created artificially by processes such as the burning of fuel. Fine dust includes various contaminants stuck to the dust core which weaken people's immunity and adversely affect their health by causing various respiratory diseases. If fine dust from outdoors is introduced indoors, contaminants such as carbon dioxide can accumulate, worsening the indoor air. As many people spend most of the day indoors, it is increasingly important to be able to easily manage indoor air quality by controlling fine dust. Therefore, there exist various IoT-based air purification systems that purify the air when the amount of fine dust exceeds a certain threshold.

III. PROPOSED SCHEME

A. Problem statement

If the number of compromised sensor nodes exceeds T, IHA cannot defend against the false report injection attack since the en-route filtering function of IHA does not work in this case. The undetected false report is forwarded to an IoT air cleaner through the BS. Then, the IoT air cleaner runs abnormally and the indoor air is not correctly purified. Therefore, it is necessary to be able to judge the authenticity of event reports for correct operation of the IoT air cleaner.

B. Assumptions

We assume that enough normal data from the IoT air cleaner has accumulated so that a correct comparison of the sensing data values is possible. It is assumed that the IoT air cleaner must assure the integrity of the sensing data for correct data calibration.

C. Proposed scheme

i. Data calibration

$$n^{th}\ Average = \frac{1}{\alpha} \cdot (E_{n-\alpha} + \cdots + E_{n-1}) = \frac{1}{\alpha} \cdot \sum_{k=n-\alpha}^{n-1} E_k \quad (1)$$

$$n^{th}\ Deviation = E_n - n^{th}\ Average \quad (2)$$

$$The\ variation\ of\ Deviation = n^{th}\ Deviation - (n-1)^{th}\ Deviation \quad (3)$$

Fig. 4. Data calibration

Fig. 4 shows the data calibration step. If fine dust is present, the WSNs and the IoT air cleaner sense fine dust at the same time. The IoT air cleaner receiving the event report from the WSNs verifies that the data from both the WSNs and the IoT air cleaner are within a predetermined error range. After computing the average and deviation of the accumulated fine dust data from the WSNs and the IoT air cleaner, the IoT air cleaner computes the variation of the deviation by comparing the deviation of the current event with the deviation of a previous event. Additionally, the IoT cleaner determines whether the variation of deviation is within a predetermined error range. If the variation of deviation is within the predetermined error range, it is determined that a normal event has occurred. Otherwise, it is determined that an attack has occurred.

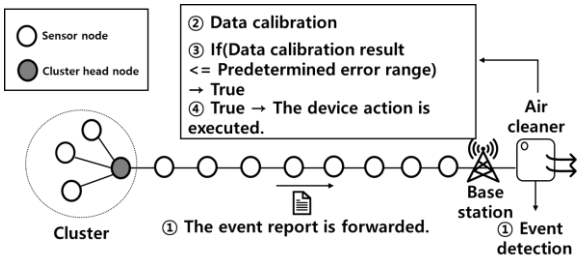

Fig. 5. Data Calibration when a normal event occurs

Fig. 5 shows the data calibration step for a situation in which a normal event occurs. The IoT air cleaner receiving the event report from the WSNs performs data calibration. If the variation of deviation in the WSNs and the IoT air cleaner is within a predetermined error range, the data calibration result is True. Therefore, the IoT air cleaner runs its normal behavior.

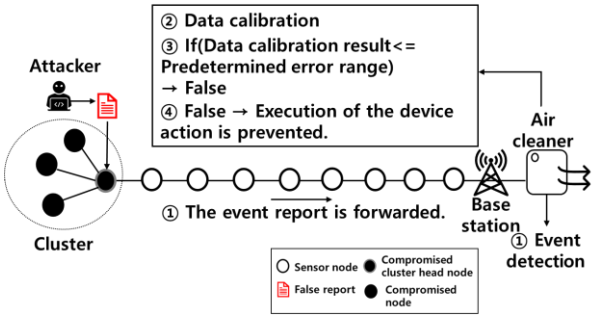

Fig. 6. Data Calibration when a false report injection attack occurs

Fig. 6 shows the data calibration step for a situation in which a false report injection attack occurs. In this case, the number of sensor nodes compromised exceeds T. The data calibration result is False because the variation of deviation in the WSNs exceeds the predetermined error range. Therefore, the IoT air cleaner detects the false report and is prevented from running abnormal behavior.

Dynamic security threshold setup

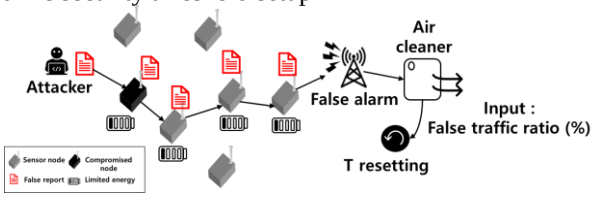

Fig. 7. Dynamic Security Threshold setup

Fig. 7 Shows the process through which the IoT air cleaner broadcasts T by resetting it based on the False Traffic Ratio (FTR). When the IoT air cleaner detects a false report through data calibration, it drops the false report and resets T based on the FTR. If the FTR is over 10%, the IoT air cleaner resets T to be larger than the current value and broadcasts the new value. En-route filtering operates if the sensor nodes reset T. As a result, early detection of false reports is possible and IHA is improved.

ii. Association node pairwise key resetting

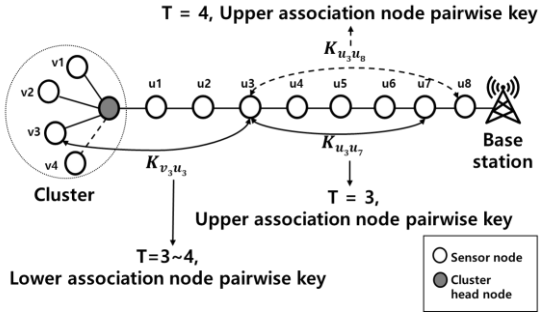

Fig. 8. Association node pairwise key resetting

Fig. 8 shows the process through which sensor nodes reset by the new T value reestablish the pairwise keys of the association nodes.

IV. PERFORMANCE EVALUATION

A. Experimental environment

Table- I: Parameters used in experimental environment

Parameters	Value
Field Size	1,000 m x 1,000 m
Cluster Size	50 m x 50 m
Number of Nodes	2,000
Number of CH nodes	400
Number of Events	1,000
MAC Size	1 byte
Energy consumption of transmitting	16.25 µJ (per 1 byte)
Energy consumption of receiving	12.5 µJ (per 1 byte)
Energy consumption of Report Generation	70 µJ
Energy consumption of MAC Generation	15 µJ
Energy consumption of MAC Verification	75 µJ
Security Threshold (T)	3-4

The experimental environment was as follows. Two thousand nodes were randomly deployed in a 1,000 x 1,000 (m^2) sensor field, 400 of which were CH nodes. The BS was located at (x, y = 1,000, 1,000). The energy needed to transmit 1 byte was 16.25 µJ, and the energy needed to receive 1 byte was 12.5 µJ [12]. The energy needed to generate a report was 70 µJ. The energy needed to generate a MAC was 15 µJ, and the energy needed to verify a MAC was 75 µJ. The size of a MAC was 1 byte, and the size of the original report was 12 bytes. Table 1 shows the parameters used in the experimental environment.

B. Experimental results

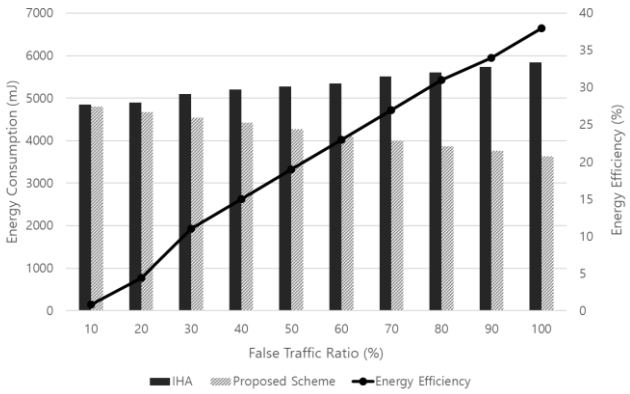

Fig. 9. Energy Consumption and Energy Efficiency according to FTR

Fig. 9 shows the energy consumption and energy efficiency with respect to the FTR for a situation in which a false report injection attack occurs when the number of compromised sensor nodes exceeds T. To compare IHA with the proposed scheme, we analyzed the total energy consumption and energy efficiency and generated 1,000 events at random locations. False report filtering did not work in this case because IHA uses a fixed value for T. Thus, as the FTR increases, the energy consumption of IHA increases. Because the proposed scheme uses a dynamic T, the false report filtering function operates correctly. Therefore, in the proposed scheme, as the FTR increases, energy consumption decreases. In addition, as the FTR increases, the energy efficiency increases. In comparison with IHA, the proposed scheme showed an energy improvement of up to 38% when the FTR was 100%.

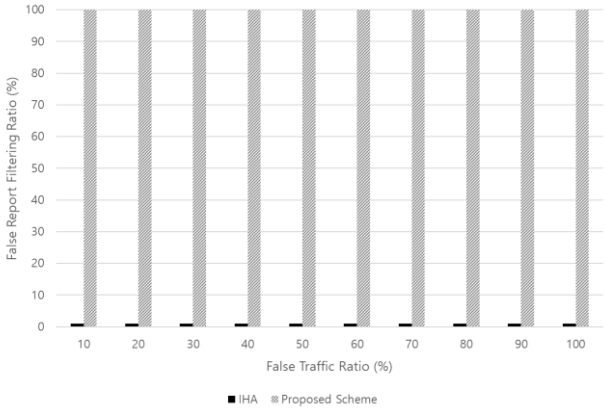

Fig. 10. False Report Filtering Ratio according to FTR

Fig. 10 shows the false report filtering ratio with respect to the FTR for a situation in which a false report injection attack occurs when the number of compromised sensor nodes exceeds T. To compare IHA with the proposed scheme, we analyzed the total false report filtering ratio and generated 1,000 events at random locations. False report filtering did not work because IHA uses a fixed value for T. Thus, the false report filtering ratio was 0%. In the proposed scheme, since T is reset from the fixed T to an increased value, false report filtering is restored. In this case, the false report filtering ratio was 100%. When the FTR was 100%, the average filtering hop of IHA was 8 hops, while the average filtering hop of the proposed scheme was 4.2 hops. As a result, the average filtering hop of the proposed scheme improved by up to 90% compared to IHA. This shows that the security of the proposed scheme is improved over that of IHA.

V. CONCLUSION AND FUTURE WORKS

Because false report filtering does not operate in an indoor air purification system using existing IHA schemes if the number of compromised sensor nodes exceeds T, a false report can be forwarded to the IoT air cleaner. This can cause abnormal behavior. In addition, the overall network lifetime is reduced because energy of the sensor nodes is unnecessarily consumed in the process of forwarding false reports to the IoT air cleaner.

Retrieval Number: D9746118419/2019©BEIESP
DOI:10.35940/ijrte.D9746.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

In this paper, we propose a method for detecting false reports by verifying if the fine dust data sensed by the WSNs and the IoT air cleaner are within a predetermined error range to solve these problems. Through precise data calibration based on two values, one sensed by the fine dust sensor in the IoT air cleaner and one sensed by the WSNs, the IoT air cleaner can detect a false report injection attack. In conclusion, security is improved and proper air purification is achieved.In the future work, in case in which a false report injection attack occurs in the WSNs-based IoT indoor air purification system, we will research the security scheme that can detect and defend against the false report injection attacks by dynamically adjusting security threshold of WSNs using fuzzy logic.

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. Wang, Yong, Garhan Attebury, and Byrav Ramamurthy. "A survey of security issues in wireless sensor networks." (2006).
7. 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.
8. 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.
9. Li, Feng, Avinash Srinivasan, and Jie Wu. "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks." IJSN 3.3 (2008): 173-182.
10. Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." Proceedings of the 3rd international conference on Embedded networked sensor systems. ACM, 2005.
11. Zhu, Sencun, Sanjeev Setia, and Sushil Jajodia. "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks." ACM Transactions on Sensor Networks (TOSN) 2.4 (2006): 500-528.
12. sef : 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.