Energy-Efficient Security Threshold Determination Method for the Enhancement of Interleaved Hop-By-Hop Authentication

Ye Lim Kang[1], Tae Ho Cho[*2]
Department of Electrical and Computer Engineering
Sungkyunkwan University
Suwon, Republic of Korea

***Abstract*—Wireless sensor networks allow attackers to inject false reports by compromising sensor nodes due to the use of wireless communication, the limited energy resources of the sensor nodes, and deployment in an open environment. The forwarding of false reports causes false alarms at the Base Station and consumes the energy of the sensor nodes unnecessarily. As a defense against false report injection attacks, interleaved hop-by-hop authentication was proposed. In interleaved hop-by-hop authentication, the security threshold is a design parameter that influences the number of Message Authentication Codes; the sensor nodes must verify, based on the security requirements of the application and the node density of the network. However, interleaved hop-by-hop authentication fails to defend against false report injection attacks when the number of compromised sensor nodes exceeds the security threshold. To solve this problem, in this paper we propose a security scheme that adjusts the security threshold according to the network situation using an evaluation function. The proposed scheme minimizes the energy consumption of the sensor nodes and reinforces security.**

Keywords*—Component; wireless sensor networks; false report injection attack; network security; interleaved hop-by-hop authentication

I. Introduction

Wireless Sensor Networks (WSNs) are densely deployed with many sensor nodes and use wireless communication [1]. WSNs are used in various applications that require real-time observation, such as fire detection and enemy movement detection [2]. For this reason, it is important to transmit accurate information to the Base Station (BS).

Security is an essential consideration in WSNs. WSNs are extremely vulnerable to false report injection attacks, due to their use of wireless communication, their deployment in open environments, and the limited energy resources of the sensor nodes [3-4]. In a false report injection attack, an attacker injects a false report into a WSN by compromising certain sensor nodes. The BS causes false alarms upon receiving false reports. In addition, the forwarding of false reports unnecessarily consumes the energy of the sensor nodes. Therefore, false reports must be detected early and dropped before they arrive at the BS.

As a defense against false report injection attacks, Z. Sencun, S. Sanjeev, J. Sushil., N. Peng proposed Interleaved Hop-by-hop Authentication (IHA) [5-6]. IHA is a security protocol in which sensor nodes detect and drop false reports during transmission if the number of compromised nodes does not exceed a certain Security Threshold (T). IHA is used when strong security is desired because it involves two-step report verification with one-hop neighbors and T+1-hop neighbors. However, IHA does not defend against false report injection attacks when the number of compromised nodes exceeds T.

In this paper, we propose a security scheme that determines a suitable T according to the network situation by means of an evaluation function. The BS resets T according to the network situation and alters the number of Message Authentication Codes (MACs) to be included in the report. By resetting T, it is possible to defend against false report injection attacks when the number of compromised nodes exceeds T. As a result, the proposed scheme improves the total energy efficiency of the network and reinforces security.

The composition of this paper is as follows. In Section 2, false report injection attacks and IHA are described. In Section 3, the proposed scheme is described. Section 4 illustrates the performance of the proposed scheme through experimental results. In Section 5, conclusions are drawn.

II. Related Work

A. False Report Injection Attacks

Fig. 1 depicts a false report injection attack in a WSN. An attacker compromises sensor nodes and obtains an authentication key. Then, the attacker generates a false report about an event that did not occur using the acquired authentication key. This causes a false alarm at the BS, and the sensor nodes consume energy unnecessarily during the transmission of false reports. There are various security protocols to defend against such attacks, including Dynamic En-route Filtering (DEF) and Probabilistic Voting-based Filtering (PVFS) [7-8].

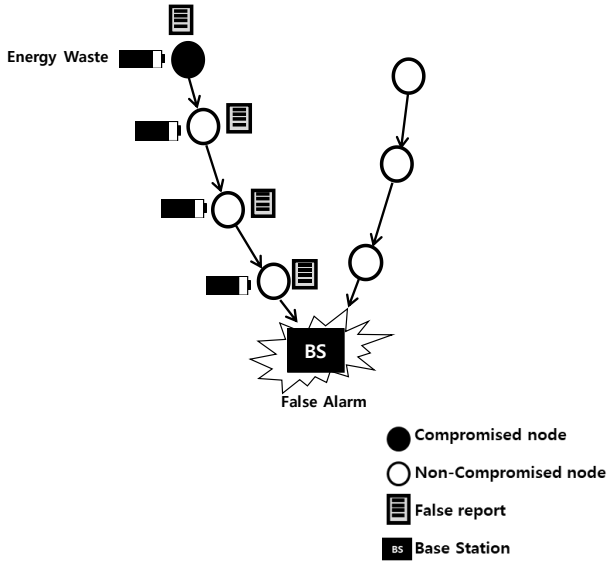

Fig. 1. False Report Injection Attack

B. IHA

1) Node Initialization and Deployment

The key server is located at the BS and distributes and manages keys. The key server preloads unique integer IDs and individual keys onto all nodes. After node deployment, all the nodes discover one-hop neighbor nodes and establish pairwise keys with them [9-10].

2) Association Discovery

Fig. 2 displays the Association Discovery step, in which all nodes discover the IDs of association nodes. For the initial path setup, there are association discovery steps, such as BS Hello and Cluster Acknowledgement [11]. The BS Hello step allows the node to discover an upper association node. The BS broadcasts a Hello message. The node receiving the Hello message discovers the ID of a T+1-hop upper association node within the path. The Cluster Head (CH) receiving the Hello message allocates T+1 IDs to the cluster nodes. The Cluster Acknowledgement (ACK) step allows the node to discover a lower association node. After the BS Hello step, the CH transmits ACK toward the BS. The node receiving ACK discovers the ID of a T+1-hop lower association node.

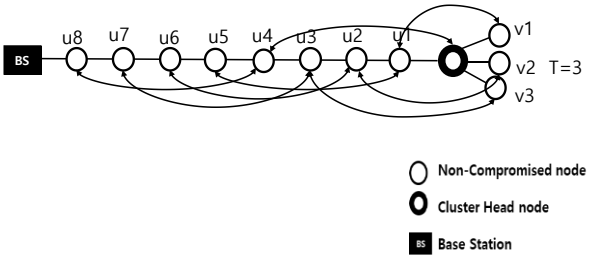

Fig. 2. Association Discovery

3) Report Endorsement

If an event occurs, the cluster nodes generate an endorsement message including the MAC, and transmit it toward the CH. The CH authenticates the endorsement message using pairwise keys shared with the cluster nodes. If the endorsement message is authenticated, the CH generates an event report including the MAC, and transmits it toward the BS.

4) En-route Filtering

Fig. 3 depicts en-route filtering in IHA. The node receiving a report from the CH verifies the report using a pairwise key shared with its downstream node. Then, the node checks the number of pairwise MACs within the report. The node verifies the last MAC within the pairwise MAC list of the report using the pairwise key shared with its lower association node. If the verification succeeds, the last MAC is eliminated from the pairwise MAC list. The node generates a MAC using the pairwise key shared with its upper association node and adds it to the beginning of the pairwise MAC list of the report. Then, the report is transmitted to the next node. All forwarding nodes repeat the same process.

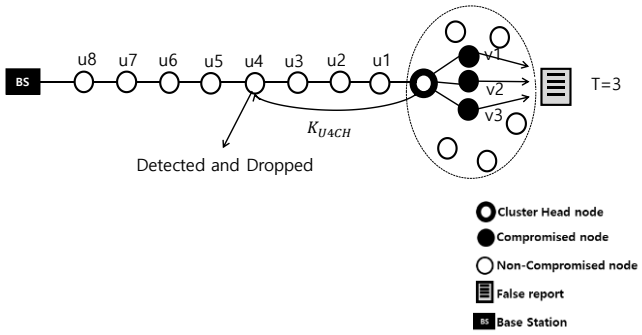

Fig. 3. En-route Filtering

5) BS Verification

If a report arrives at the BS, the BS verifies the compressed individual MACs [12]. The BS computes T+1 MACs about the event using the authentication keys of the nodes in the ID list of the report. Then, the BS determines whether or not these MACs match the individual MACs within the report. If the verification succeeds, the report is authenticated. However, if the verification fails, the report is discarded.

III. PROPOSED SCHEME

A. Problem Statement

IHA is an effective security protocol that defends against false report injection attacks. However, it has several problems.

1) IHA loses en-route filtering during false report injection attacks when the number of compromised nodes exceeds T. The event data of a false report that the number of compromised nodes exceeds T are false, but the report is composed of normal MACs. There are not methods to detect and drop such reports before the BS receives them.

2) In IHA, if the node receives a report, the node goes through a verification process with its T+1-hop neighbor node in addition to its one-hop neighbor node. IHA has powerful security, but the energy of the sensor nodes is consumed much more than with other security protocols.

To solve these problems, we propose the following solutions

3) The network administrator presets standard range of event data values of a normal report. The BS judges that a received report is false if it deviates from the standard range of a normal report set by the network administrator.

4) The BS minimizes the energy consumption of the sensor nodes as much as possible by determining the suitable T according to the network situation.

B. Assumptions

- We assume the energy of the sensor nodes is not limited.
- We assume the BS is not compromised.

C. Proposed Scheme

1) Factors Considered to Determine T

Fig. 4 demonstrates that after the BS resets T based on the False Traffic Ratio (FTR), Residual Energy of the Node (REN), and Max Hop Count (MHC), it broadcasts T. The evaluation function is executed whenever the number of received reports is 100. The BS performs the evaluation function considering the cluster in which the FTR is the largest and the REN is the smallest among the clusters in which the false report injection attack has occurred. The evaluation function is not executed if T is changed from the initially set T to a new T. The node detecting the false report deletes the false MAC without discarding the false report, and forwards the false report to the BS by adding the pairwise MAC of its upper association node. The BS can determine the number of compromised nodes and their IDs using this received false report. The BS determines the value to which it should reset T according to the number of compromised nodes. T should be reset to a value equal to the number of compromised nodes or greater than the number of compromised nodes. If all the nodes receive a broadcasting message to reset T from the BS, all the nodes will stop transmitting false reports after detecting them. Once T is reset, all the nodes operate by detecting and dropping false reports, as in existing IHA.

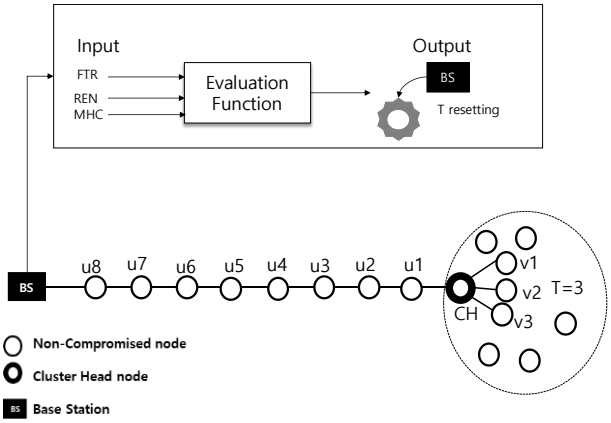

Fig. 4. Interleaved Hop-by-hop Authentication Using the Evaluation Function

Evaluation function (1) determines whether to reset T based on the FTR, REN, and MHC of Path (P).

$$\mathrm{T(p)} = \frac{FTR(p)}{FTR(p) + MHC(p)} + REN(p) \qquad (1)$$

Table 1 displays the output according to the inputs of the evaluation function. If the FTR is 0-10% and the REN is 0-100%, the BS resets T to a value smaller than the initially set T through the evaluation function. Then, the BS broadcasts T. At this time, the execution condition of the evaluation function is that the number of compromised nodes is smaller than the initially set T. This minimizes unnecessary energy consumption by the sensor nodes.

If the FTR is 11-100% and the REN is 0-100%, the BS resets T to a value greater than the initially set T through the evaluation function. Then, the BS broadcasts T. At this time, the execution condition of the evaluation function should be the situation of a false report injection attack when the number of compromised nodes exceeds the initially set T. In other words, the BS restores en-route filtering by resetting T to a value greater than the initially set T. Therefore, false reports are dropped before they arrive at the BS. Thus, it is possible to defend against attacks that cannot be defended against by the existing IHA.

Determining the suitable T involves adjusting T differently in various network situations, such as attack situations.

TABLE I. EVALUATION FUNCTION

Input			Output	
FTR(%)	**REN(%)**		**T**	
0~10	0~10	**MHC**	0~10	Down
	11~21		11~21	
	22~100		22~100	
11~100	0~10		0~10	Up
	11~21		11~21	
	22~100		22~100	

2) Reassociation Setup of Nodes

The BS broadcasts the new T to all the nodes when T is reset as a result of the evaluation function. Fig. 5 depicts the process in which all the nodes reset T+1 association node pairwise keys with the new T. For example, if T is changed from 3 to 4, node u3 resets its upper association node pairwise key from K_{u3u7} to K_{u3u8}.

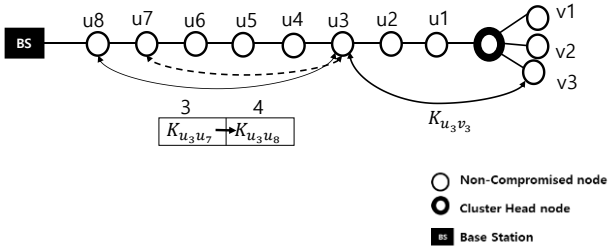

Fig. 5. Reassociation Setup

IV. PERFORMANCE EVALUATION

A. Experimental Environment

The experimental environment is as follows: 2000 nodes are randomly deployed in the sensor field, which is 1000 x $1000m^2$ in size, and 2000 events are generated. The BS is positioned at (x, y = 1000, 1000) of the sensor field. The energy required to transmit 1 byte is 16.25 μJ, and the energy required to receive 1 byte is 12.5 μJ [13]. The energy required to verify a MAC is 75 μJ, and the energy required to generate a

MAC is 15 μJ [14]. The size of a MAC is 1 byte and the size of the original report is 12 bytes. The size of the Hello Message is 30 bytes [15]. The initial energy resource of the nodes is 1 J.

B. Experimental Results

Fig. 6 displays the total energy consumption of the network according to the FTR in the situation of a false report injection attack when the number of compromised nodes is less than T. To demonstrate the energy efficiency of the proposed scheme, we generated 2000 events at random positions and analyzed the total energy consumption of the sensor nodes. As the FTR increases, the total energy consumption decreases. IHA maintains the initially set T. In the proposed scheme, the BS changes its broadcast value from the initially set T to the reduced T if the FTR is 0-10% and the REN is 0-100%.

Comparing IHA and the proposed scheme, when the FTR is 100%, the energy efficiency is improved by up to 27.17%, as shown in Fig. 6.

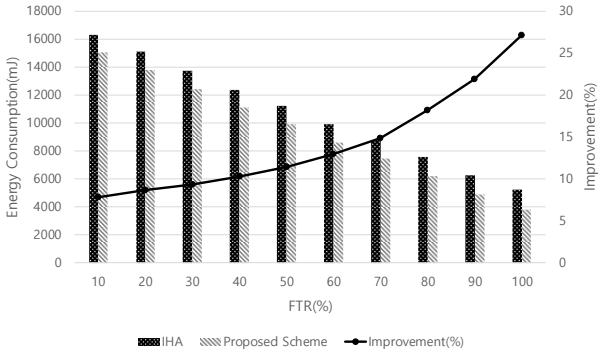

Fig. 6. Energy Consumption versus the FTR when the number of compromised nodes is less than T.

Fig. 7 displays the total energy consumption of the network according to the FTR in the situation of a false report injection attack when the number of compromised nodes exceeds T. IHA maintains the initially set T. In the proposed scheme, when the FTR is 11-100% and the REN is 0-100%, the BS changes its broadcast value from the initially set T to the increased T. Comparing IHA and the proposed scheme, when the FTR is 90%, the energy efficiency increases by up to 24.18%, as shown in Fig. 7.

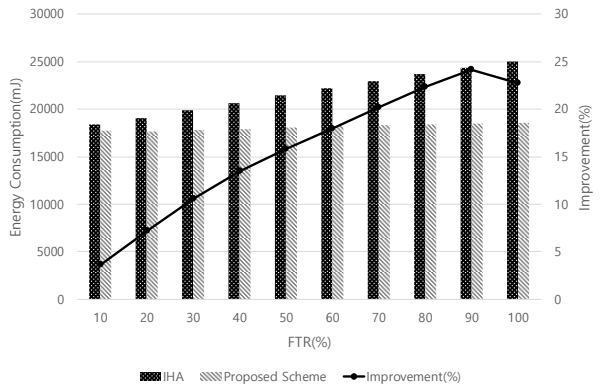

Fig. 7. Energy Consumption versus the FTR when the number of compromised nodes exceeds T.

Fig. 8 displays the number of dropped false reports according to the FTR in the situation of a false report injection attack when the number of compromised nodes exceeds T. To demonstrate the security of the proposed scheme, we generated 2000 events at random positions and analyzed the number of dropped false reports. IHA maintains 0% en-route filtering, while the proposed scheme progressively improves en-route filtering as the FTR increases. Thus, the security of the proposed scheme is better than that of IHA.

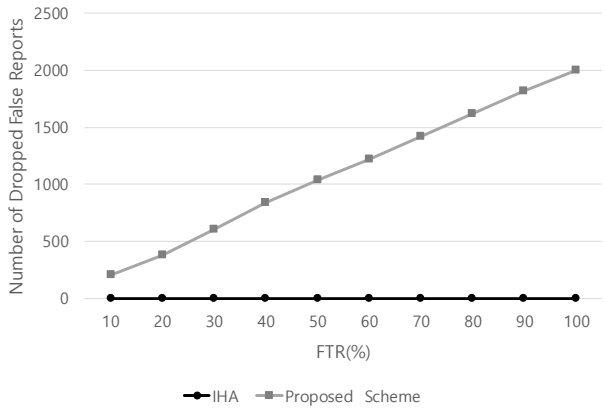

Fig. 8. Number of Dropped False Reports versus the FTR

V. Conclusions

WSNs are vulnerable to false report injection attacks. IHA is an effective security protocol to defend against false reports. However, with IHA, it is impossible to defend against false report injection attacks when the number of compromised nodes exceeds T. In this paper, we proposed a WSN security scheme that adjusts T according to the network environment. When sensor nodes detect a false report that the number of compromised nodes is less than T, the BS reduces T and prevents unnecessary energy use by the sensor nodes through the evaluation function. The BS broadcasts an increased value of T when the sensor nodes detect a false report that the number of compromised nodes exceeds T. Therefore, en-route filtering is restored, security is enhanced compared to the existing IHA, and unnecessary energy wasting by the sensor nodes is prevented because false reports are discarded in advance. However, in the node initialization deployment step, all the nodes have many keys, so much of the memory of the sensor nodes is consumed. Therefore, in the proposed scheme, costs increase because expensive sensor nodes must be used. Through this experiment, we have demonstrated the performance improvement of the proposed scheme compared with IHA.

Acknowledgment

This research was supported by the MISP (Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW) (2015-0-00914) supervised by the IITP (Institute for Information & communications Technology Promotion)" (2015-0-00914)

References

[1] A. Ian F., S. Weilian, S. Yogesh, C. Erdal, "A survey on sensor networks." IEEE communications magazine 40.8 (2002): 102-114.

[2] A. K .Jamal N., and K. AHMED E. "Routing techniques in wireless sensor networks: a survey." IEEE wireless communications 11.6 (2004): 6-28.

[3] Jeba, S. A., and B. Paramasivan. "False data injection attack and its countermeasures in wireless sensor networks." European Journal of Scientific Research 82.2 (2012): 248-257.

[4] K. Chris, and W. David. "Secure routing in wireless sensor networks: Attacks and countermeasures." Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on. IEEE, 2003.

[5] Z. Sencun, S. Sanjeev, J. Sushil., N. Peng, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks." Security and privacy, 2004. Proceedings. 2004 IEEE symposium on. IEEE, 2004.

[6] Z. Sencun, and N. Peng. "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks." ACM Transactions on Sensor Networks (TOSN) 3.3 (2007): 14.

[7] Y. Zhen, and G. Yong. "A dynamic en-route filtering scheme for data reporting in wireless sensor networks." IEEE/ACM Transactions on Networking (ToN) 18.1 (2010): 150-163.

[8] L. Feng, S. Avinash and W. Jie. "PVFS: a probabilistic voting-based filtering scheme in wireless sensor networks." International Journal of Security and Networks 3.3 (2008): 173-182.

[9] Z. Sencun, S. Sanjeev, and J. Sushil. "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks." ACM Transactions on Sensor Networks (TOSN) 2.4 (2006): 500-528.

[10] B. Carlo, S. Alfredo De, H. Amir, K. Shay, V. Ugo, Y. Moti, "Perfectly-secure key distribution for dynamic conferences." Annual international cryptology conference. Springer, Berlin, Heidelberg, 1992.

[11] W. Yong, A. Garhan, and R. Byrav. "A survey of security issues in wireless sensor networks." (2006).

[12] B. Mihir, G. Roch, and R. Phillip. "XOR MACs: New methods for message authentication using finite pseudorandom functions." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1995.

[13] P. Dongjin, and C. Taeho. "A Fuzzy Rule-based Key Re-Distribution Decision Scheme of Dynamic Filtering for Energy Saving in Wireless Sensor Networks." International Journal of Information Technology and Computer Science (IJITCS) 9.4 (2017): 1-8.

[14] Y. Fan, L. Haiyun, L. Songwu, Z. Lixia, "Statistical en-route filtering of injected false data in sensor networks." IEEE Journal on Selected Areas in Communications 23.4 (2005): 839-850.

[15] R. Sajjad, Q. Hassaan Khaliq, K. Syed Ali, R. Veselin, R. Muttukrishnan, "A1: An energy efficient topology control algorithm for connected area coverage in wireless sensor networks." Journal of Network and Computer Applications 35.2 (2012): 597-605.l