Report Verification Technique for Improvement of the Energy Efficiency in a Probabilistic Voting-based Filtering Scheme of WSNs

Sang-hyeok Lim
College of Information and Communication Engineering
Sungkyunkwan University
Suwon 440-746, Republic of Korea

Tae-ho Cho
College of Software
Sungkyunkwan University
Suwon 440-746, Republic of Korea

ABSTRACT
Wireless sensor networks (WSNs) consist of several sensor nodes and base stations and collect information through sensors located over a large area. However, they can easily be compromised by an attacker because of their random placement in an open environment, where individual management is difficult. An attacker can execute a false report injection attack and a false vote injection attack through compromised nodes. The probabilistic voting-based filtering scheme (PVFS) is a scheme to prevent these two kinds of attacks. Before sending the report, the proposed method selects the validation node, judges the validity of the report, and filters it based on a set of threshold values. In this paper, the proposed method detects and filters false reports generated from compromised member nodes of event clusters early and improves both the detection rate of false reports and the energy efficiency of nodes compared with PVFS. It's experiments show that the maximum energy efficiency increased by about 17%, and a nearly 30% increase in detection performance was observed.

Keywords
Wireless sensor networks, False report injection attack, False vote injection attack, Secure routing.

1. INTRODUCTION
WSNs are composed of many sensor nodes and a base station (BS). When an event occurs, the sensor node detects the event and reports it over multiple sensor nodes to the BS [1]. These WSNs are used for data collection and event detection in various fields such as military systems, home networks, and forest fire monitoring [2]. However, many applications have limited computational power and low energy, and they are easily compromised by attackers because they are randomly distributed in an open environment in which it is difficult to individually manage them as they operate independently [3], [4]. Attackers exploit these vulnerabilities to attack WSNs by injecting reports containing false information or false votes. Figure 1 shows these attacks. A false report injection attack is one that injects a report about a non-existent event through the compromised sensor node. It aims to exhaust the energy resources of the nodes on the propagation path and generates a false alarm on the BS. The false vote injection attack injects false votes into a legitimate report, thereby preventing the legitimate report from reaching the BS. Li and Wu proposed a probabilistic voting-based filtering scheme (PVFS) [5] to prevent such attacks. In PVFS, all nodes constitute a network that exploits cluster-based organization. When a cluster head (CH) recognizes an event, it generates a report on that event, and the member nodes judge the authenticity of the report and generate their own message authentication codes (MACs), alternatively referred to as votes in PVFS.

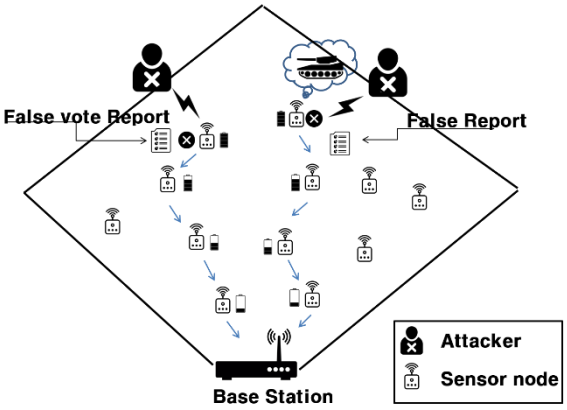

Figure 1: False Report and False Vote Injection Attacks.

CH randomly selects votes and inserts them into the report. Verification nodes on the path use MAC and threshold values to defend against attacks. An attacker can attempt a false report injection attack and false vote injection attack through the compromised member node. But, the existing PVFS does not address this type of attack. This paper uses CH verification code that identifies the source of the report to deal effectively with such an attack. This code reveals the origin of the report and provides early detection of false reports generated from the compromised member node. The composition of this paper is as follows. In Section 2, related works are described. In Section 3, the problems associated with existing schemes and the proposed method are described in detail. Section 4 describes the experimental environment and results. Finally, Section 5 discusses conclusions and future work.

2. RELATED WORK
This section describes false report attacks and false vote injection attacks on WSNs. PVFS, a defense mechanism against those attacks, is also described.

2.1 False report attack
A false report attack is an attack that injects a false report on an event that does not exist in the network [6], [7]. This is also called a false positive attack (FPA). In the absence of a defense system, false reports can arrive at the BS, trigger false alarms, and cause unnecessary energy consumption. The attacker attaches a false MAC to the report. This false MAC is generated using the MAC of the node itself and the s-1 false keys. Thus, false reports contain a large number of false votes. DEF, SEF, CCEF, IHA, and BECAN are examples of defense schemes against such false report attacks [8],[9],[10],[11],[12].

2.2 False vote injection attack

A false vote injection attack is one that prevents a legitimate report from reaching the BS. This is usually called a false negative attack (FNA). The compromised member node makes a false vote in a legitimate report, so that the wrong information is written in the report. Because of this, the false MAC-injected report contains a small number of false votes. A false vote in the legitimate report will cause the verification node to regard the report as false and drop it during path verification. This attack causes the BS to lose important information.

2.3 PVFS

To cope with false report injection and false vote injection attacks in wireless sensor networks, the proposed PVFS uses the true threshold value (Tt) and false threshold value (Tf) to detect and filter false reports and false vote injection reports at validation nodes. Figure 2 shows the report generation and verification node selection process.

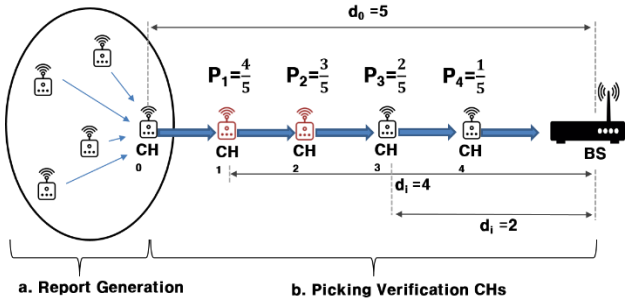

Figure 2: Report Generation and Verification Node Selection Process.

In the network configuration phase, the nodes are divided into cluster units, and the CHs responsible for report generation are selected for each cluster. The verification nodes are probabilistically selected from among the CHs to verify reports. The probability p uses the distance d_0 between the BS and the event cluster, and the distance d_i represents the distance between the BS and the CH_i. The verification node selection process is shown in Figure 2-b. Figure 3 shows the Key allocation step in which the BS divides the key pool into N partitions and delivers them to each CH. Each partition contains L keys, where L is equal to the size of the cluster. The CH uses one of the keys in the partition as its own and distributes the remaining L-1 keys to the member nodes. A key is allocated to the member nodes according to the partition of the key pool.

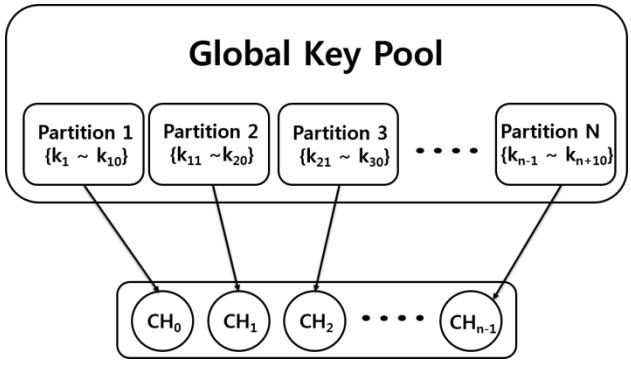

Figure 3: Key Distribution Process.

The node selected as the verification node stores the keys of the member nodes of the event reporting cluster one by one. In the report generation step, CH generates a report on an event and broadcasts it to member nodes. The member nodes confirm this, and if the report is judged to be normal, the MAC created by its own key is transmitted to the CH. CH extracts a predetermined number of MACs received from member nodes and adds them to the report. In the report verification process, the verifying nodes compare their own key-index with those in the report. If they have the same key-index, they determine the MAC of the report if the MAC value generated by the same key is different. Then, the vote is regarded as a false vote, and the false count is increased. In the filtering process, if the false count reaches the threshold value, the report is judged to be false and is immediately dropped. If the true count value reaches the threshold value, the report is considered legitimate and is sent to the BS without further validation.

3. PROPOSED METHOD

This section presents the problems associated with the present PVFS and describe the proposed method for solving these problems.

3.1 Problem statement

PVFS prevents false report attacks generated from compromised CHs and false vote injection attacks generated from compromised member nodes.

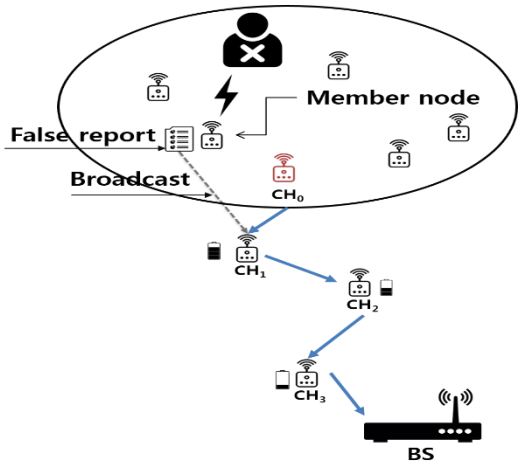

Figure 4: False Report Generated from a Member Node.

In PVFS, it assumes that all false reports are generated from CH. However, when the sensor field is divided into clusters, there is a high probability that the node the attacker has compromised is a member node. Also, there is a high probability that a compromised member node will perform a false report injection attack. A false report generated from a compromised member node is delivered to the BS through the same path as a false report generated from the CH, causing a false alarm and wasting energy of the WSNs. This process is shown in Figure 4. Therefore, early detection of false reports generated from member nodes will help improve the overall network lifetime and detection rates. In the proposed scheme, the code that identifies whether or not the report generation node is CH is added to the report to prevent these attacks early and improve security and energy efficiency.

3.2 System overview

Figure 5 shows the operation of the proposed method. In the initial network configuration, the CHs on the path send their node ID values to the BS. Based on this, the BS creates a CH_MAC necessary for authentication of the report and distributes it to CHs. The CH of the event cluster senses the event, writes the report, attaches s randomly selected votes, and adds the CH_MAC received from the BS. The composition of the final report is shown in Figure 6. During the delivery of the report, the verification node compares its own CH_MAC with the CH_MAC of the report. If the value is different or does not exist, the validation node regards it as a false report generated from a compromised member node and drops it immediately.

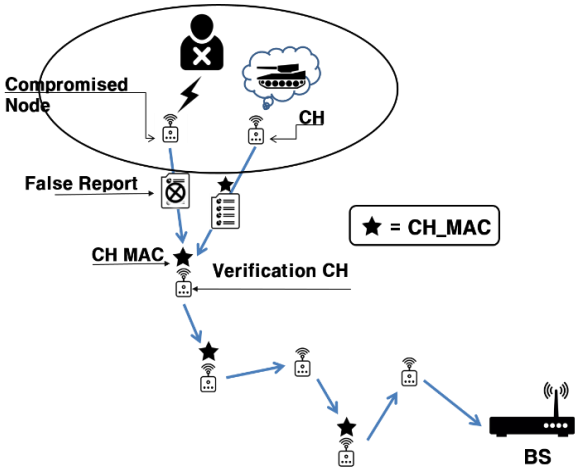

Figure 5: Filtering Process of the Proposed Scheme.

If the CH_MAC is correct, it considers the report generated from the CH and starts to compare other MACs. If the same key index is detected, it verifies the MAC. The next full cycle follows the existing PVFS.

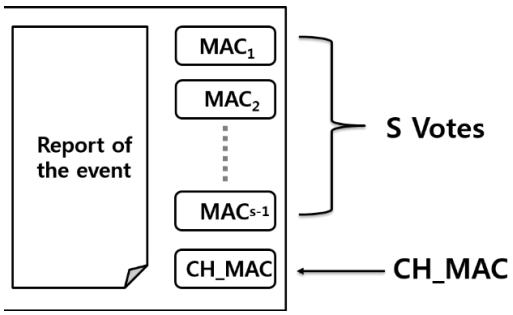

Figure 6: Report Composition of the Proposed Scheme.

The probability that a compromised node from an attacker is a member node is proportional to the number of nodes (L) constituting the cluster. The proposed scheme is applicable only when the compromised node from the attacker is a member node. If the compromised node is CH, the attacker will obtain the CH_MAC information, and the protection scheme follows the existing PVFS. Calculation of the total energy consumption of the network is shown in Equation 1. The algorithm of the proposed scheme is shown in Figure 7. C.P means energy consumption in pvfs and C.P.S means energy consumption on proposed scheme.

$$E_{consume} = \frac{1}{L}(C.P) + \frac{L-1}{L}(C.P.S) \qquad (1)$$

Equation 1: Total Amount of the Energy Consumption

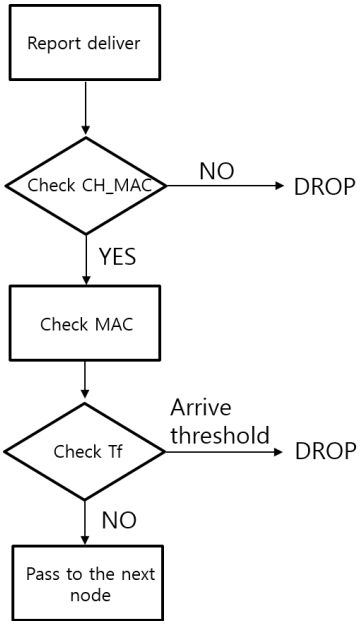

Figure 7: Flowchart of Proposed Scheme

4. EXPERIMENTAL RESULTS

This section describes the simulation environment and the obtained results.

4.1 Experimental Environment

This section shows the simulation results of energy efficiency and security in the proposed method compared with PVFS. This paper assumes the following experimental environment to demonstrate the efficiency of the proposed method [7]. Relevant values are provided in the tables below.

Table 1: Parameters Used in the Experiments

Parameter	Value
Field size	1000 x 1000(m^2)
Number of nodes	100-4000
Number of experiments	1000
L	10
S	5
Tt	5
Tf	1-3

Table 2: Energy Consumption and Data Size of the Experiments

Parameter	Value
MAC calculation	15 µJ
Energy consumption of transmitting	16.25 µJ
Energy consumption of receiving	12.5 µJ
Packet size	24 byte
Size of MAC	1 byte
Size of CH_MAC	1 byte

4.2 Experimental Results

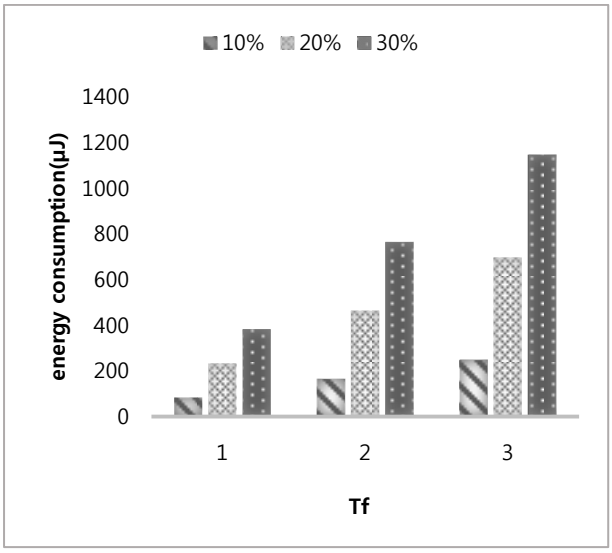

Figure 8: Energy Consumption Gap by Attack Rate.

Figure 8 shows the difference in energy consumption of the proposed scheme and PVFS according to attack rate and Tf. Higher attack rates and larger Tf values result in larger differences in energy consumption. In the existing PVFS, the total energy consumption increases as the attack rate increases. As the Tf increases, the cost of filtering false reports increases. On the other hand, in the proposed method, filtering by CH_MAC is independent of the Tf value, but it is affected by the attack rate. When the proposed scheme is applied to the experimental environment with s = 5, L = 10, and Tt = 3, energy savings of up to 1145 μJ and an energy efficiency of about 17% can be obtained when the attack rate is 30%.

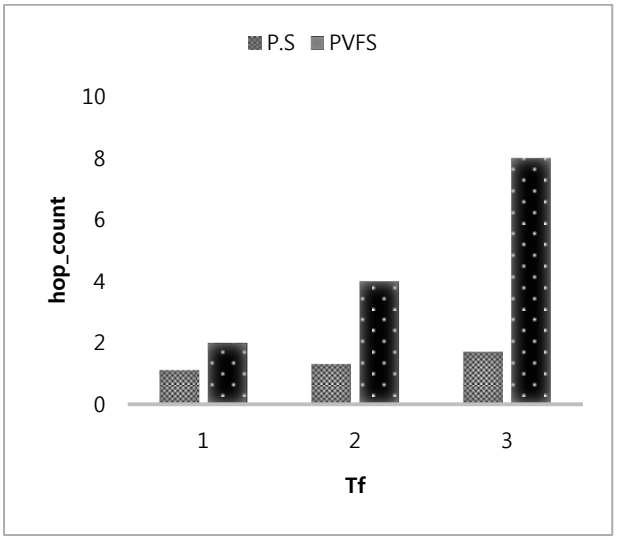

Fig 9: Hop Count Difference for Different Tf Values.

Figure 9 shows the differences in filtering performance according to Tf value for PVFS and the proposed method. In PVFS, larger Tf values result in a larger number of hops traversed until false reports are dropped.

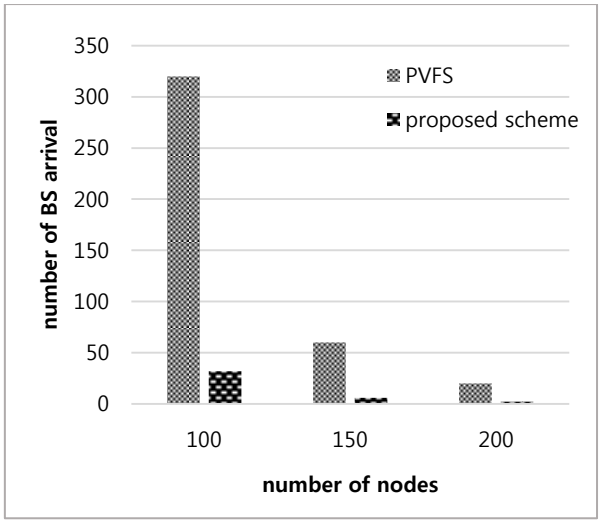

Fig 10: Filter Failure Rate by Number of Nodes.

Figure 10 shows the false report detection failure rate according to the number of nodes installed in the field. The experiment calculated the number of false reports reaching the BS when a total of 1000 events were generated. When the number of nodes is less than 200, the PVFS shows poor filtering performance. The reason for this is that, when the number of nodes is insufficient, the selected verification nodes of the PVFS are not suitable for filtering. On the other hand, in the proposed scheme, most of the verification is unaffected by the number of nodes because it is an immediate filtering method, even if only one verification node is used instead of the probabilistic filtering performed in the verification node.

5. CONCLUSIONS

WSNs are sometimes placed in an open field and are easily compromised due to the limited resources of the sensor nodes and vulnerable to security attacks. Therefore, a protocol is needed to defend against attacks, and it is essential to consider energy resources when applying a protocol to WSNs. The proposed method aims to increase the detection rate of false reports and the energy efficiency of the whole network by using CH_MAC for report verification in the existing PVFS. Future work will further incorporate a technique dealing with false vote injection attacks, thereby increasing energy efficiency and preventing both false report injection attacks and false vote injection attacks, which are the main objectives of PVFS. Normally, as the detection rate increases, energy consumption is reduced, so these tasks are expected to significantly reduce energy consumption.

6. ACKNOWLEDGMENTS

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science, and Technology (No. NRF-2015R1D1A1A01059484).

7. REFERENCES

[1] Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6 (2004): 53-57.

[2] Zhang, Wensheng, and Guohong Cao. "Group rekeying for filtering false data in sensor networks: A predistribution and local collaboration-based approach." INFOCOM 2005. 24th Annual Joint Conference of the

IEEE Computer and Communications Societies. Proceedings IEEE. Vol. 1. IEEE, 2005.

[3] Al-Karaki, Jamal N., and Ahmed E. Kamal. "Routing techniques in wireless sensor networks: a survey." IEEE wireless communications 11.6 (2004): 6-28.

[4] Perrig, Adrian, John Stankovic, and David Wagner. "Security in wireless sensor networks." Communications of the ACM 47.6.

[5] Li, Feng, and Jie Wu. "A probabilistic voting-based filtering scheme in wireless sensor networks." Proceedings of the 2006 international conference on Wireless communications and mobile computing.ACM, 2006.

[6] Yu, Zhen, and Yong Guan. "A dynamic en-route scheme for filtering false data injection in wireless sensor networks." SenSys. Vol. 5. 2005.

[7] 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.

[8] Yang, Hao, and Songwu Lu. "Commutative cipher based en-route filtering in wireless sensor networks." Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. Vol. 2. IEEE, 2004.

[9] Zhu, Sencun, et al. "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.

[10] Lu, Rongxing, et al. "BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks." IEEE transactions on parallel and distributed systems 23.1 (2012): 32-43.

[11] 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.

[12] Jeba, S. A., and B. Paramasivan. "An evaluation of en-route filtering schemes on wireless sensor networks." *International Journal of Computer Engineering & Technology (IJCET)* 3 (2012): 62-73.