A METHOD FOR DETECTING FALSE POSITIVE AND FALSE NEGATIVE ATTACKS USING SIMULATION MODELS IN STATISTICAL EN-ROUTE FILTERING BASED WSNS

Su Man Nam[1] and Tae Ho Cho[2]

[1]College of Information and Communication Engineering,
Sungkyunkwan University, Suwon 16419, Republic of Korea
[2]College of Software,
Sungkyunkwan University, Suwon 16419, Republic of Korea

ABSTRACT

In wireless sensor networks, adversaries compromise sensor nodes to damage the network though potential threats such as false positive and false negative attacks. The false positive attacks cause energy drain and false alarms, and false negative attacks generate information loss. To address the false positive attacks in the sensor network, a statistical en-route filtering (SEF) detects the false report in intermediate nodes. Even though the scheme detects the false report against the false positive attack, it is difficult to detect false MACs in a legitimate report against the false negative attack in the SEF-based WSN. Our proposed method effectively detects the false positive and false negative attacks in the sensor network through a simulation model. The experimental results indicate that the proposed method increase detection power while maintaining the energy consumption of the network against the false positive and false negative attacks.

KEYWORDS

Wireless Sensor Networks, Network Security, Simulation models, Statistical En-route Filtering Network Protocols

1. INTRODUCTION

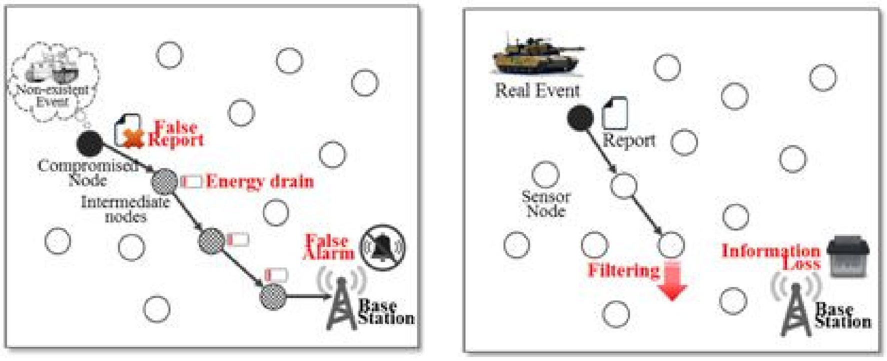
Wireless sensor networks (WSNs) are being applied in diverse application fields such as habitat monitoring field, and surveillance field, and military field[1]. A WSN consists of a base station and the large number of sensor nodes in a sensor field[2]. The base station collect data, analyzes the data, and provides the data information to users. For forwarding the data to the base station, the sensor nodes includes the data collection module, the date processing module, communication module, and so on. Although the sensor network has many advantages such as easy monitoring in the wide fields, intelligence surveillance, safety tracking in energy areas, the sensor network is subject to potential attacks because the sensors are energy-constrained.

Figure 1 shows false positive[3] and false negative [4]attacks in the sensor network. In Figure 1(a), the compromised node can inject false reports to cause energy drain and false alarms. In Figure 1(b), the compromised node can insert a false message authentication code (MAC) in a legitimate report to filter out the report in an intermediate node.

A statistical en-route filtering (SEF) was proposed through the MACs verification in a report to address the false positive attack. In the SEF, as an event is generated, a node collects MACs from

DOI : 10.5121/avc.2016.3302

its neighbors and generate a report with the collected MACs. Intermediate nodes verify the MACs to filter out the false report. When an intermediate node detects a false MAC, it immediately drops the report. Although the SEF effectively detects false MACs against the false positive attack, it is difficult to detect the legitimate report including the false MACs against the false negative attack because the report is dropped as the false MAC of the report is verified.



(a) False positive attack (b) False negative attack

Figure 1.False positive and false negative attacks

In this paper, our proposed method effectively detects false positive and false negative attacks through simulation models. To detect both of the attacks, the proposed method collects data from the sensor nodes and analyzes the data based on its history data in the base station. Therefore, the proposed method effectively detects the false data against the false positive and false negative attacks.

This paper is organized as follows: in Section 2, we describe background and motivation of the proposal. Section 3 introduces our proposed method in detail, and Section 4 provides the analysis and experimental results. Finally, the conclusions and future works are discussed in Section 5.

2. BACKGROUND

2.1. STATISTICAL EN-ROUTE FILTERING (SEF)

The SEF is a countermeasure method of the sensor network that detects false reports through MACs verification in a report against the false positive attack. The SEF consists of three phases: key assignment and report generation, en-route filtering, and base station verification. In the first phase, the base station generates a global key pool including *n* non-overlapping partitions (PIDs). It produces m unique keys per each PID.

The base station has a global key pool with *n* PIDs including each of 100 keys. The base station randomly assigns the keys of each of partition to each sensor nodes before deploying the nodes. The sensor nodes are then deployed in the sensor field. When an event occurs, a center-of-stimulus (CoS) node, which one of the detecting nodes is elected, broadcasts an event data (including the event location, the detection time, event type) to the detecting nodes. The nodes then generate each message authentication nodes (MACs) using their keys after checking an error range of the event data. They transmits the MACs to the CoS node, and the CoS node collects them.

In the second phase, the CoS node forwards a report to its next-hop node after attaching the MACs in the report. When an intermediate node receives the report, the node checks whether its keys match one of key indexes in the report and verifies the MAC of the matched key. If the intermediate node detects a false MAC, the node immediately filters out the report. On the other hand, if the keys are not matched, the intermediate node forwards the report to the next-hop node.

In the third phase, when the report arrives at the base station, the base station verifies all of MACs in the report using its keys of the global key pool. When a false MAC is detected in the report, the base station drops the report.

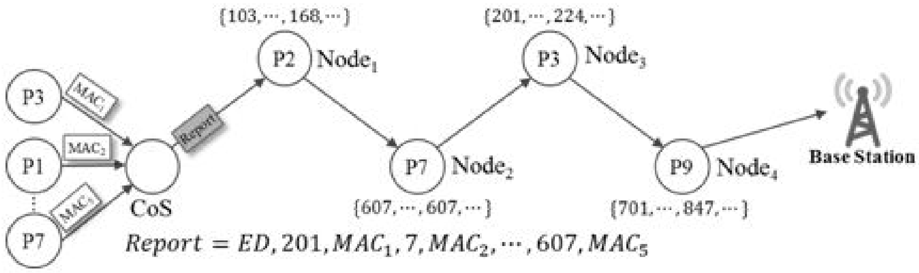


Figure 2. An example of report generation and en-route filtering

Figure 2 shows an example of a report generation and en-route filtering in a phase from a CoS node to the base station. After generating an event and broadcasting the event data, the CoS node collects MACs from its neighboring nodes. The MACs are generated in the nodes by a key of each PID. The CoS node generates a report including event data and the MACs $(MAC_1, MAC_2, \cdots, MAC_5)$). After the report pass through Node$_1$ without MAC verification, Node$_2$ verifies MAC$_5$ as the report arrives at it. Since the MAC is normal, Node$_2$ continually forwards the report toward the base station. When the base station receives the report, it verifies all of MACs again.

2.2. Motivation

In a sensor network, adversaries can easily compromise sensor nodes because the node has limited hardware resource. The compromised nodes causes serious damage to the network such as false positive and false negative attacks. The false positive attack results in energy drain in intermediate nodes and false alarm in the base station and the false negative attack causes information loss in the base station. In order to address the false positive attack, the SEF detects false reports through MACs verification in intermediate nodes. Although the SEF detects the false report against the false positive attack, it is difficult to discover a legitimate report including a false MAC against the false negative attack. Our proposed method detects the false positive and false negative attacks through the simulation models, which collects the data of the sensor network and analyzes the data. Thus, the proposed method effectively detects false data using the simulation models against the both of them.

3. Proposed Method

3.1. Assumption

We assume that the sensor network is composed of a base station and a large number of sensor nodes (e.g. Berkeley MICA2 motes [8]). The initial paths is established through directed diffusion [9] and minimum cost forwarding algorithms [10]. Every node forwards reports into the base station along their path.

3.2. METHOD DETAILS

The proposed method simultaneously detects false positive and false negative attacks through the simulation models in the sensor network.

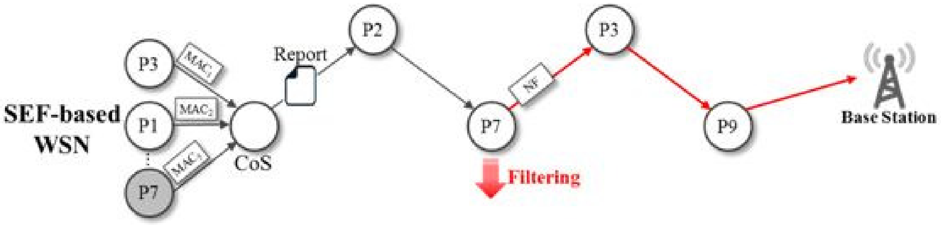


Figure 3. Overview of the proposed method

Figure 3 shows an overview of the proposed method. After an event occurs, a CoS node collects MACs from its neighbors, include a compromised node for injecting the false negative attack. The CoS node forwards the report with a false MAC. The report is filtered out in an intermediate node.The intermediate node transmits a notification message including attack information. When the base station receives the message, it executes simulation models for detecting the compromised node with the past history data. Thus, the proposed method effectively detects the compromised nodes against the two attacks.

3.3. DETAILED PROCEDURES

The proposed method uses three phases (key assignment and report generation, en-route filtering, and base station verification)of the SEF. We add simulation verification for detecting the compromised nodes against false positive and negative attacks.

3.3.1. KEY ASSIGNMENT AND REPORT GENERATION

Before deploying the sensor nodes, the base station assigns keys of a partition to every node after they establish their routing path using the directed diffusion and the minimum cost forwarding algorithm from each source sensor to the base station. When an event occurs, a CoS node broadcasts the event data to its neighbors. The neighboring nodes generate their MACs and transmit each MAC to the CoS node. After receiving the MACs, the CoS node attaches the MACs in a report and forwards the report to the next-hop node.

3.3.2. EN-ROUTE FILTERING

After an intermediate node receives the report forwarded from the CoS node, the node verifies a MAC in the report as it has a matched key. If the MAC is normal, the intermediate node forwards the report to its next-hop node; if the MAC is error, the node immediately filters out the report. The intermediate node transmits a notification message including attack information to the base station.

3.3.3. BASE STATION VERIFICATION

When the base station receives the report, it verifies all MACs of the report using its keys in the global key pool. If the MACs are normal, the report is provided to users; if a false MAC is detected, the report wipes the report.

3.3.4. Simulation verification

The proposed simulation models analyze the collected data as it receives the notification message from an intermediate node.The simulation models are implemented for treatment accuracy of the vast data with time values. The models maintain the same sensor network structure. A representative model is as shown in Figure 4.

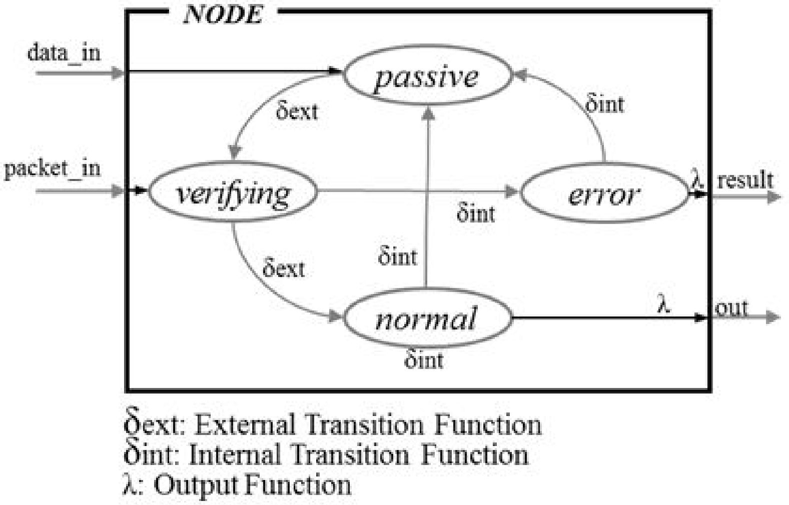


Figure 4. simulation model

As shown in Figure 4, as the model receives data from the sensor node, it verifies that the data is whether normal or error for detecting compromised node against the false positive and false negative attack.

For example, if a compromised node injects a false MAC in a legitimate report for a false negative attack, SEF may drop the legitimate report through the MAC verification in an intermediate node. After dropping the report, the intermediate node transmits a notification message to the base station. When the message is received in the base station, the NODE model verifies the message information based on its past history data. When the model receives the information of the attacks, it transfers states *passive→verifying→error*. Thus, the proposed method detects the compromised node using back tracking in the simulation models against the false positive and negative attacks.

4. Simulation Results

We performed a simulation in order to evaluate the proposed method as compared to SEF. The sensor field consists of 1000 sensor nodes. A routing path of each sensors was established based on the minimum cost forwarding algorithm. Each sensor node forwards reports toward the base station via multiple hops. Each node used 16.25 μJ per byte to transmit, 12.5 μJ per byte to receive. The node consumed 15 μJ per byte to generate, and 75 μJ to verify a MAC in intermediate nodes. The size of each report was 36 bytes. We randomly generated 300 events. There was no packet loss in the experiment. For false positive and negative attacks, 10 compromised nodes were randomly selected and 10 probability are generated in the sensor field.

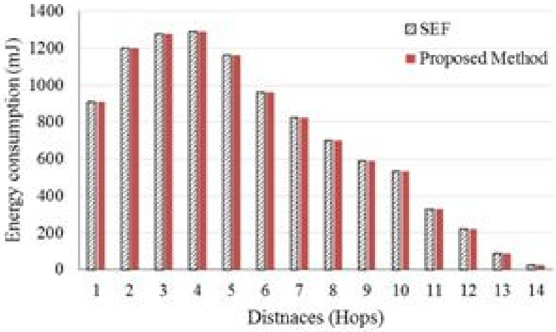


Figure 5. Energy consumption in two methods

Figure 5 shows energy consumption per distance in SEF and the proposed method. As showed in Figure 5, the proposed method's energy consumption is equal to the energy consumption of SEF.

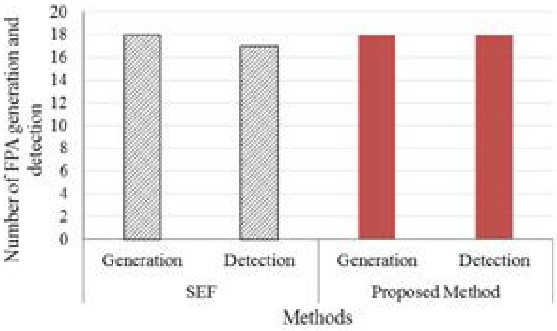


Figure 6. Number of generating and detecting false positive attacks

Figure 6 shows the number of generation and detection of false positive attacks. Since SEF probabilistically detects false reports, the number of detected reports in the SEF was reduced as compared to our proposed method. On the other hand, the proposed method detects false data through the simulation models against the false positive attack. Thus, the proposed effectively method detects all of the false data through the simulation models.

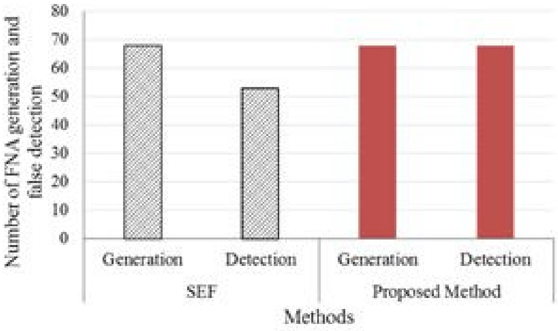


Figure 7. Number of generating and detecting false negative attacks

Figure 7 shows the number of generation and detection of the false negative attacks. The proposed method detects false MACs in legitimate reports through the simulation model. Although SEF drops 53 reports for the false report, the reports were be dropped with false detection. Therefore, the proposed method effective detects the false MACs in the legitimate reports against the false negative attacks.

5. Conclusion and Future Works

WSNs is vulnerable to the false positive and false negative attacks since the network has the limited hardware resource. SEF detects false reports through MAC verification in the sensor network. Even though the method addresses the false report against the false positive attack, it is difficult to detect false negative attack. The proposed method effectively detects the false positive and false negative attacks through the simulation model. As shown in the experimental results, the proposed method simultaneously detects the two attack while maintaining the energy. Therefore, the proposed method effectively detects the false data against the false positive and false negative attacks without no additional energy consumption of the sensor network.

Acknowledgements

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-2015R1D1A1A01059484)

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam & E. Cayirci, (2002) "A survey on sensor networks",Communications Magazine, IEEE, Vol. 40 pp 102-114.

[2] K. Akkaya & M. Younis, (2005) "A survey on routing protocols for wireless sensor networks",Ad Hoc Networks, vol. 3, pp 325-349.

[3] F. Ye, H. Luo, S. Lu & L. Zhang, (2005) "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal On, vol. 23, pp 839-850.

[4] F. Li, A. Srinivasan & J. Wu, (2008) "PVFS: A Probabilistic Voting-based Filtering Scheme in Wireless Sensor Networks," International Journal of Security and Network, vol. 3, pp 173-182.

[5] M. Baldauf, S. Dustdar & F. Rosenberg, (2007) "A survey on context-aware systems," International Journal of Ad Hoc and Ubiquitous Computing, vol. 2, pp 263-277.

[6] ZhiGang Li, XingShe Zhou, Huaifeng Qing & Shining Li, (2008) "Model and implementation of context-aware sensor networks," in Information Science and Engineering, 2008. ISISE '08. International Symposium On, pp 16-19.

[7] S. M. Nam and T. H. Cho, (2016) "Context-Aware Architecture for Probabilistic Voting-based Filtering Scheme in Sensor Networks," IEEE Transactions on Mobile Computing, to be submitted (TMC-2016-05-0332).

[8] MICA2. Available: http://bullseye.xbow.com:81/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf.

[9] C. Intanagonwiwat, R. Govindan & D. Estrin, (2000) "Directed Diffusion: A scalable and robust communication paradigm for sensor networks," Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, pp 56-67.

[10] F. Ye, A. Chen, S. Lu &L. Zhang, (2001) "A scalable solution to minimum cost forwarding in large sensor networks," in Computer Communications and Networks, 2001. Proceedings. Tenth International Conference On, p. 304-309.

AUTHORS

Su Man Nam received his B.S. degree in Computer Information from Hanseo University, Korea, in February 2009 and his M.S. degree in Electrical and Computer Engineering from Sungkyunkwan University in 2013. He is currently a doctoral student in the College of Information and Communication Engineering at Sungkyunkwan University, Korea. His research interests include wireless sensor networks, security in wireless sensor networks, and modeling & simulation.

Tae Ho Cho received a Ph.D. degree 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, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor networks, intelligent systems, modeling & simulation, and enterprise resource planning.