

Key Re-Dissemination for Maintaining Detection Power in Sensor Networks

Jin Myoung Kim, Soo Young Moon, and Tae Ho Cho

*School of Information and Communication Engineering
Sungkyunkwan University, Suwon 440-746, Republic of Korea
{kjm77, moonmous, taecho}@ece.skku.ac.kr*

Abstract— In many wireless sensor network (WSN) applications, sensor nodes are deployed in unattended environments, and hence are vulnerable to physical attacks, potentially compromising the node's cryptographic keys. Sensor nodes are subject to compromise physically and surreptitious use by an adversary. The adversary can capture them to inject an incorrect data into the sensor field in order to reduce network life time. Ye et al. proposed the statistical en-route filtering scheme to detect and drop such false reports during the forwarding process. However if the number of filtering keys exposed to adversary is larger than or equal to the size of threshold, the forward nodes can not filter out a fabricated report. Also the base station can not filter the report. In this paper, we propose key dissemination method for maintaining detection power in statistical filtering based WSNs. Via simulation; we show the proposed method is better than existing one in terms of remaining energy and the number of fabricated reports which are not filtered out by forwarding nodes and the base station.

Keywords— security; sensor network; filtering scheme; injection attack

I. INTRODUCTION

Wireless sensor networks (WSNs) have emerged as an innovative class of networked embedded systems due to the union of ever smaller, less costly embedded processors and wireless interfaced with micro-sensors based on micro-mechanical systems (MEMS) technology [1], [2]. WSNs are composed of small autonomous devices or sensor nodes, that are networked together [3], [4].

In many applications, sensor nodes are deployed in open outdoor environments, and hence are vulnerable to physical attacks, potentially compromising the node's cryptographic keys [5]. False sensing reports can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resource in battery powered networks [5].

Ye et al. [6] proposed the statistical en-route filtering scheme (SEF) to filter out forged reports during the forwarding process. In the SEF, multiple sensing nodes collaboratively generate a sensing report that contains

multiple message authentication codes (MACs) so that each MAC is generated by a node using one of its symmetric keys, and represents its agreement on the report [7]. As a report is forwarded towards the base station over multiple hops, each forwarding node verifies the MACs carried in the report, checking if it has any of the keys used to generate those MACs. If it does not have any of those keys, the report is forwarded without verification.

In these schemes, a false report is filtered out by intermediate forwarding nodes. However, by attacker, if enough nodes are compromised and filtering keys (FK) are exposed then intermediate nodes can not detect false report. Hence network lifetime and usability is reduced.

In this paper, we propose filtering key re-dissemination method to maintain the filtering power. We detect a compromised node and find exposed filtering keys to re-assign new keys to legitimate nodes.

The remainder of this paper is organized as follows: Section 2 gives a brief description of SEF and motivation. Section 3 explains the proposed method. Section 4 presents the simulation results. Finally, section 5 the conclusions and future work.

II. RELATED WORK AND MOTIVATION

A. Statistical En-Route Filtering

SEF is the first scheme that addresses false data injection attacks in the presence of compromised nodes and it focuses on the detection of false event reports, which are known as false positive attacks, injected by compromised nodes. In SEF, the base station maintains a global key pool, which is divided into multiple partitions and every node loads a small number of keys from a randomly selected partition in the global key pool before it is deployed.

When real events occur, one of the detecting nodes is elected as the center-of-stimulus (CoS) node to generate a sensing report. The surrounding nodes, which detect the same event, produce MACs for the event, using their stored keys, and sends them to the CoS which generates a sensing report using the collected MACs. This set of multiple MACs acts as the proof that a report is legitimate [7] after which points the CoS forwards the report toward the base station over multiple hops.

Each forwarding node verifies the correctness of the MACs carried in the report by using its keys. When the base station receives a report, it can verify all the MACs carried in the report because it has complete knowledge of the global key pool [7].

The figure 1 shows a fabricated report generation and en-route filtering in case that the size of threshold is 3 and each node has 2 filtering keys. In the figure, gray node 4 is compromised by an adversary.

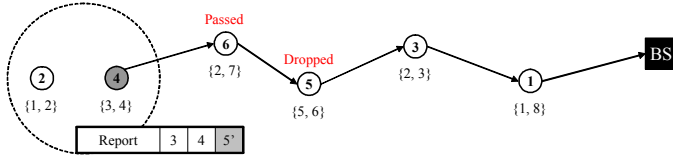


Figure 1. Fabricated report that is generated by compromised node 4 with forged key 5' is dropped by forwarding node 5.

Since the size of the threshold is three, the compromised node 4 generates the forged key 5' in order to generate a fabricated report. The fabricated report is forwarded towards the base station over multiple hops. During the forwarding process, the fabricated report is dropped by forwarding node 5 since the forwarding node can verify the fabricated report using its own filtering key 5.

B. Motivation

In the SEF, for a fabricated report, a detection power is largely affected by the size of threshold. If the number of exposed filtering keys is larger than or equal to the size of the threshold, both forwarding nodes and the base station cannot verify the fabricated report generated by the adversary. Figure 2 shows the example of the worst case.

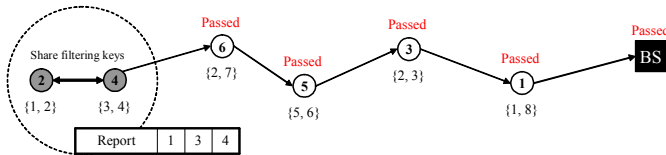


Figure 2. The fabricated report generated by compromised node 2 and 4 with the filtering key 1, 2 and 3 cannot be filtered out by forwarding nodes and the base station

In above figure, two gray nodes 2 and 4 are compromised and white nodes 1, 3, 5 and 6 are forwarding nodes. Let us assume that compromised nodes can share filtering keys. In case threshold is 3, the compromised node 2 and 4 share filtering keys and can generate a fabricated report. The fabricated report is not verified by forwarding nodes during the forward process. Also the base station cannot verify the report since the report contains correct MACs using valid filtering key 1, 3 and 4.

In this paper, we propose filtering key dissemination method to maintain the filtering power. For this, we detect exposed filtering keys and distribute new filtering keys to

legitimate nodes. Also we determine the re-keying period by considering a threshold, amount of energy consumption by an injection attack and the number of the exposed keys.

III. PROPOSED METHOD

In this section, we simply illustrate the operation of our proposed method and then provide more detailed explanation for each operation.

A. Models and Assumptions

The assumptions in our paper are as follows. The sensor field is large and in a harsh environment with no infrastructure, so the sensor nodes are vulnerable to security threats. Sensor nodes are given limited energy, computing power, and memory whereas the sink node can use enough resources. The base station knows location information of all sensor nodes and directly sends a message to each node.

Figure 3 shows our network environments where the white circles and gray circles imply legitimate sensor nodes and compromised nodes respectively.

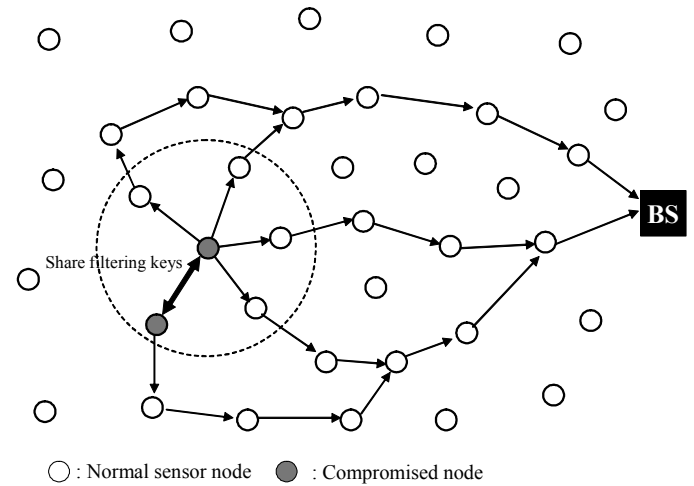


Figure 3. Network environments in proposed method

In the network, we assume that compromised nodes located within transmission range can share filtering keys when they generate a fabricated report. Also compromised node can send the fabricated report to neighbor nodes.

B. Detection and Notification

In the network, when the sensed report is sent to the base station, the report is forwarded towards the base station and verified by forwarding nodes. If a compromised node generates a fabricated report and sends it to the base station, the report is filtered out by forwarding nodes or the base station. That the report is filtered out implies that compromised node exists in the network. Therefore, the forwarding node which detects the fabricated report drops the report and generates a notification report to send information of the compromised node to the base station.

The notification report is generated using the forwarding node's filtering keys, as shown in figure 4. For the

compromised node, the base station collects notification reports and determines a key re-dissemination.

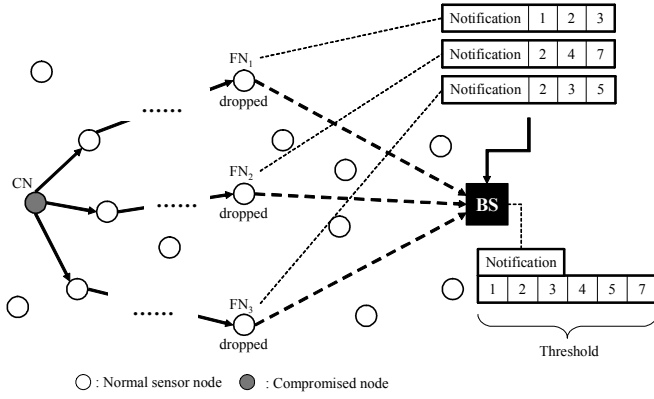


Figure 4. A fabricated report by generated compromised node (CN) is dropped by forwarding nodes FN1, FN2 and FN3. The forwarding nodes generate a notification report using their filtering keys and send it to the base station over the multiple hops.

In figure 4, the base station gathers MACs from the notification reports and determines that CN is compromised node if the number of the MACs is larger than or equal to the size of the threshold.

Next section, we will explain a re-keying and a key revocation. Also we will demonstrate a re-keying period by considering the size of the threshold, exposed keys, and amount of energy consumption by compromised nodes.

C. Re-Keying and Revocation

As shown in motivation session, if an adversary gets N filtering keys (N is bigger or equal to the size of threshold), forwarding nodes can not filter out fabricated report.

Exposed keys by adversary have to be revoked to maintain a filtering mechanism in the network. To revoke exposed filtering keys, the base station generates new filtering keys and sends them to legitimate nodes. Each node revokes the exposed key and save a new filtering key.

When the generated filtering keys are sent to legitimate nodes, these keys have to be encrypted to protect the keys from the adversary. Therefore, the base station encrypts the new keys using filtering key of each node. The transmission of the filtering key is as follows:

$$BS \rightarrow SN_i : E(SN_{i,FK}, FK) \quad (1)$$

In (1), $E(K, \dots)$ is symmetric encryption function using key K . $SN_{i,FK}$ is the filtering key of the node SN_i where the $SN_{i,FK}$ is not exposed to the adversary. BS and SN is the base station and a sensor node respectively.

D. Re-Keying Period

Threshold, i.e. used in CoS, determines the size of the MAC included in a report. If the size increases, the filtering probability increases for fabricated report. But energy

consumption for the report transmission is increased because of the increase of the report size.

If a legitimate node is captured by adversaries, they can get filtering keys and those are used to generate a fabricated report. If the number of filtering keys exposed to the adversary is bigger or equal to the size of threshold, forwarding nodes can not filter out the fabricated report. The base station also can not filter out the report because the compromise node generates the fabricated report using valid filtering keys. Therefore, to determine the period, we define an evaluation function as following:

$$F = \alpha \cdot Security + (1 - \alpha) \cdot Energy Efficiency$$

$$= \alpha \cdot \frac{EK}{T} + (1 - \alpha) \frac{ECCNs}{EECCNs + ECRK} \quad (2)$$

In (2), alpha value is design factor where the value is more or equal to 0 and less or equal to 1. T and EK are the size of the threshold, i.e. used in CoS, and the number of exposed keys respectively. $ECRK$ is energy consumption needed for re-keying and $EECCNs$ is estimate of energy consumption by compromised node's injection attack. If F is more or equal to 1 then the base station generates and distributes new filtering keys to legitimate nodes.

IV. SIMULATION RESULTS

To show the effectiveness of the proposed method, the original SEF scheme is compared with proposed method through simulation studies. The sensor network in the simulation environment consists of 400 nodes over a field of $100 \times 400m^2$ size. The nodes are assumed to be uniformly distributed in the field and the base station is located at the center of the field. Each node takes $16.56\mu J/12.5\mu J$ to transmit/receive a byte, and each MAC generation consumes $15\mu J$ [4]. The size of a MAC is 1 byte, and the report size is 12 bytes. There are 100 keys in the global key pool, which is divided into 10 partitions.

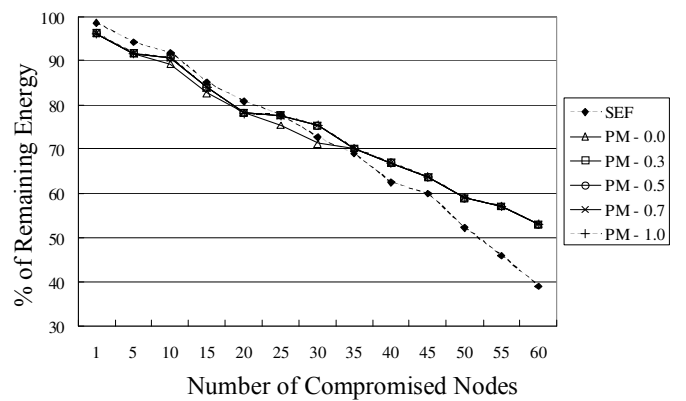


Figure 5. For the alpha value is 0.0, 0.3, 0.5, 0.7 and 1.0, comparison of proposed method (PM) and SEF in terms of the percentage of remaining energy

Figure 5 shows the percentage of the remaining energy for the increase of compromised nodes. In this figure, the compromised nodes send a fabricated report to the base station five times. In our proposed method, forwarding nodes drop the fabricated report and send notification reports to the base station. So, for the fabricated report, our proposed method requires more energy than SEF first stage. But if the number of compromised nodes increase, our method is better than SEF in terms of remaining energy.

Figure 6 shows an increase of exposed keys for compromised nodes and filtering power. In the figure 6, the histograms and the graph of broken line imply the number of exposed keys and the number of fabricated reports which can not be verified by forwarding nodes and the base station respectively.

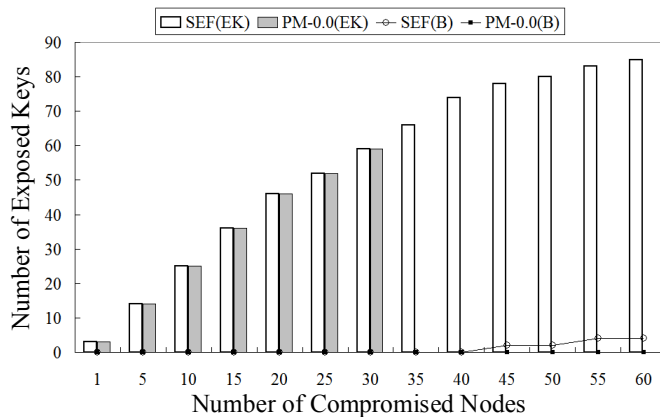


Figure 6. For an increase of compromised nodes, an increase of exposed keys (EK) and fabricated reports that can not be filtered out by forwarding nodes and the base station.

Existing method does not manage for the exposed keys. So, compromised nodes can generate fabricated reports that cannot be dropped by forwarding nodes and the base station. Moreover, adversaries easily perform the injection attack using exposed keys and filtering scheme cannot filter out for the fabricated report any longer.

V. CONCLUSION AND FUTURE WORKS

Statistical en-route filtering is the first scheme that addresses the false data injection attacks. In the scheme, to protect the injection attack, a report generated by CoS includes MACs that are generated by neighbor nodes using their filtering keys. The number of MACs is determined by the size of threshold. But if the number of the exposed filtering keys to an adversary is larger than or equal to the size of the threshold then the filtering scheme is broken.

In this paper, we propose key dissemination method to maintain the filtering power. We detect exposed filtering keys and distribute new filtering keys to legitimate nodes. Also we determine the re-keying period by considering a threshold, amount of energy consumption by compromised node's injection attack and the number of the exposed keys.

In future research, we will improve the evaluation function to get an optimized re-keying period. We will also research partial re-keying technique to reduce energy consumption.

ACKNOWLEDGMENT

This work was supported by National Research Foundation of Korea Grant funded by the Korean Government (No. 2009-0076504).

REFERENCES

- [1] R. D. Pietro, L. V. Mancini, and S. Jajodia, "Providing secrecy in key management protocols for large wireless sensors networks," *AdHoc Networks*, vol. 1, pp. 455-468, 2003.
- [2] Lin Yuan and Gang Qu, "Design Space Exploration for Energy Efficient Secure Sensor Network," *IEEE ASAP*, pp. 88-97, 2002.
- [3] Mohamed Eltoweissy, Ashraf Wadaa, Stephan Olariu and Larry Wilson, "Grop Key management scheme for large-scal sensor networks," *AdHoc Network*, vol. 3, pp. 668-688, 2005.
- [4] Laurent Eschenauer and D. Virgil Gligor, "A Key Management Scheme for Distributed Sensor Networks," *CCS'20*, 2002.
- [5] B. Przydatek, D. Song, and A. Perring, "SIA: Secure Information Aggregation in Sensor Networks," *ACM in Proc. Of SenSys*, pp. 255-265, 2003.
- [6] F. Ye, H. Luo, and S. Lu, "Statistical En-route Filtering of Injected False Data in Sensor Networks," *IEEE Journal of Sel. Area Comm.*, vol. 23, no. 4, pp. 839-850, 2005.
- [7] F. Li and J. Wu, "A Probabilistic Voting-based Filtering scheme in Wireless Sensor Networks," *Proceeding of IWCMC*, pp.27-32, July, 2006.