Path Selection Method for the Statistical Filtering-Based Sensor Networks Using a Security Evaluation Function

Chung Il Sun and Tae Ho Cho,

Sungkyunkwan University, Suwon 440-740, South Korea

Summary
Many sensor network applications are dependent on the secure operation of sensor networks, and will have serious consequences if the network is compromised or disrupted. Fabricated reports can be injected through compromised nodes, which can lead not only to false alarms but also to the depletion of limited energy resources in battery powered networks. Ye et al. proposed the statistical en-route filtering scheme to detect and drop such fabricated reports during the forwarding process. In this scheme, every node has a limited amount of information that is used to verify against injected false data, the detection power is affected by the selection of routing paths. In this paper, we propose a path selection method to improve the detection power of the statistical filtering. Each node evaluates the detection power of each incoming path from the base station and chooses the most secure path for data delivery against false data injection attacks. We compare our proposed method with the statistical en-route filtering scheme and the simulation results show that our proposed method protects against false data injection attacks.

Key words:
Sensor networks, false data filtering, secure routing path selection.

1. Introduction

Recent advances in micro-electro-mechanical-systems technology, wireless communications and digital electronics have enabled the development of low-cost, low-power and multifunctional sensor nodes [1, 2]. Such a network normally consists of a large number of high density distributed sensor nodes, which are capable of sensing, computing and communicating wirelessly interconnected in an ad-hoc topology [3]. Sensor networks are expected to interact with the physical world at an unprecedented level of universality, and enable a variety of new applications [4, 5]. In many applications, sensor nodes are deployed in open environments and hence are vulnerable to physical attacks, potentially compromising the node's cryptographic keys [6, 7]. False sensing reports can be injected through compromised nodes, which can lead to not only false alarms but also the depletion of limited energy resources in battery powered networks (Fig. 1) [4, 8]. It can also block legitimate reports from passing through it, or record and replay old reports, etc [4]. To minimize damage, fabricated reports should be dropped en-route as early as possible, and the few eluded ones should be further rejected at the base station [1].

Ye et al. proposed the statistical en-route filtering scheme (SEF) [4] to filter out fabricated reports during the forwarding process. In SEF, multiple sensing nodes collaboratively generate a sensing report that contains multiple message authentication codes (MACs). Each MAC is generated by a node using one of its symmetric keys and represents its agreement on the report [9]. As a report is forwarded towards the base station over multiple hops, each forwarding node verifies the MACs carried in the report 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. Therefore, the detection power of SEF is largely affected by the choice of routing path.

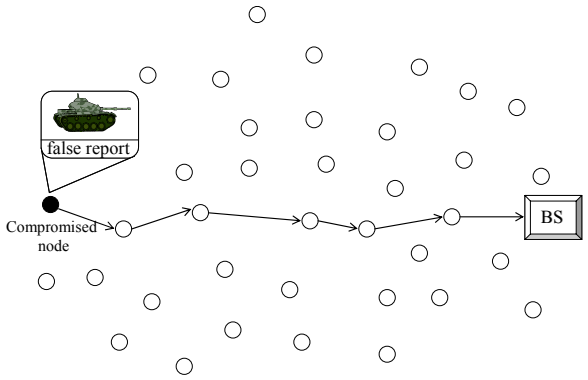

Fig. 1 false data injection attack

In this paper, we propose a path selection method to improve the detection power of SEF. Each message to establish routing paths contains additional information about the keys of the visited nodes. By using this information, the detection power of each incoming path is evaluated by every node. Thus, it can choose the most secure path against false data injection attacks, which can lead to early detection of fabricated reports and thus energy saving.

The remainder of the paper is organized as follows: Section 2 gives a brief description of SEF. Section 3 explains the proposed method. Section 4 reviews the

Manuscript received October 30, 2007
Manuscript received November 20, 2007

simulation results. Finally, the conclusion and future work are discussed in Section 5.

2. Background

2.1 Statistical En-route Filtering scheme

In SEF, the base station maintains a global key pool which is divided into multiple partitions. Each partition has n keys, and each key has a unique key index. Before a sensor node is deployed, the user randomly selects one of the multiple partitions, and randomly chooses a small number of keys from this partition to be loaded into every node [4]. Fig. 2 shows an example of a global key pool with n = 10 partitions, each of which has 10 keys. Five nodes have k = 2 keys randomly selected from one partition.

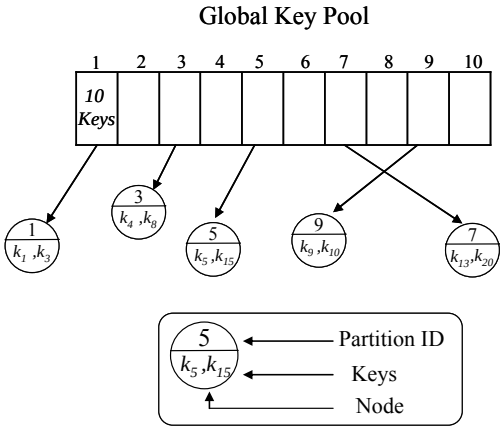

Fig. 2 a global key pool

When real events occur, one of the detecting nodes is elected as the center-of-stimulus (CoS) node to generate a sensing report. Surrounding nodes which detect the same event produce MACs for the event using its stored keys and sends them to the CoS. The CoS generates a sensing report using the collected MACs. This set of multiple MACs acts as the proof that a report is legitimate [4]. Then the CoS forwards the report toward the base station (BS) over multi hops. Each forwarding node verifies the correctness of the MACs carried in the report by using its keys. If fabricated reports are not filtered out by forwarding nodes then the BS serves as the final defense that catches the fabricated reports, because it has complete knowledge of the global key pool [4]. Fig. 3 shows an example of the (a) report generation and (b) en-route filtering in SEF.

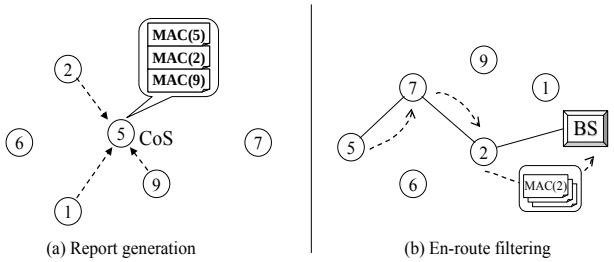

Fig. 3 a report generation and en-route filtering

An adversary can inject a fabricated report with incorrect MACs through a compromised node as shown in Fig. 4(a). However, the fabricated report may be dropped since each forwarding node verifies the correctness of the MACs carried in the report with certain probability (Fig. 4(b)). The probability of detecting incorrect MACs increases with the number of hops the report travels. SEF can detect fabricated reports by an adversary with a fixed number of compromised partitions.

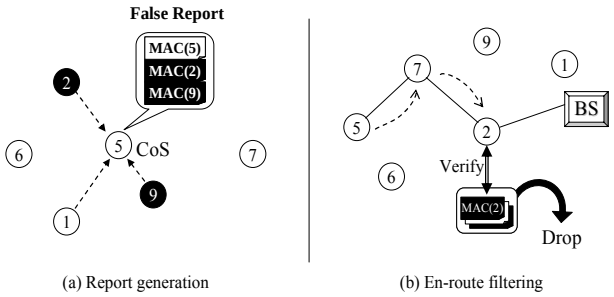

Fig. 4 a fabricated report generation and en-route filtering

3. Path Selection Method

3.1 Assumption

We assume that routing paths are established by flooding a control message. A control message is broadcasted by the BS upon a change of the network topology or the user's request. We also assume that the network uses a single-path routing protocol. To simplify the problem, we further assume that each node chooses a routing path based on the distance from the BS in hop count and the security level to protect against false data injection attacks.

3.2 Overview

In the proposed method, every control message contains additional information about the partition IDs of visited

nodes. The information is used to evaluate the security level of a path. As a control message is flooded through the network over multiple hops, each forwarding node updates the partition ID information of the message. A routing path is chosen by the node using a qualification evaluation function which considers distance and security level.

3.3 Proposed Method

In the proposed method, the BS maintains a global key pool divided into multiple partitions. Each partition has a unique identification number. Each node has some keys from a randomly selected partition in the key pool before it is deployed. These keys are used to generate or verify MACs. After node deployment, routing paths are established by flooding a control message which BS broadcasts.

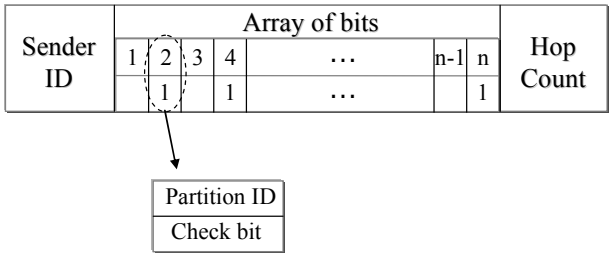

Fig. 5 consist of a control message

In most routing protocols, a control message includes the number of hops from BS and sender ID. In the proposed method, an array of bits is additionally attached into each control message. This array is used to mark the partition IDs of the visited nodes. An example form of a control message is shown in Fig. 5 when the number of partitions in a global key pool is *n*. When a node receives a control message, it stores the sender ID, the hop count from BS, and the partition ID array attached in the message. The stored information is used to evaluate the detection power of the incoming paths by nodes. If the received message is the first instance of the control message, it sets the partition ID of its keys in the partition array of the message and increases the hop count in the message. Then, it forwards the updated control message.

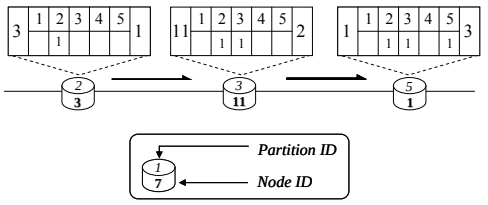

Fig. 6 Flooding control message

Fig. 6 shows how a partition ID array can be updated when a global key pool is divided into five partitions. Node 3, 11, and 1 have some keys loaded from partition 2, 3, and 5, respectively. When node 3 receives a control message shown in Fig. 6, it stores the information attached in the message. If the received message is the first instance of the message, it sets the first bit of the partition ID array in the message (since it loads some keys from partition 2). Then, the node increases the hop count of the message and forwards the updated message. When node 11 receives the message, it stores the information. If the message is the first instance, the node sets second bit of the array and increases the hop count. Then, it forwards the updated message. Node 1 also stores the information and forwards the updated message if necessary.

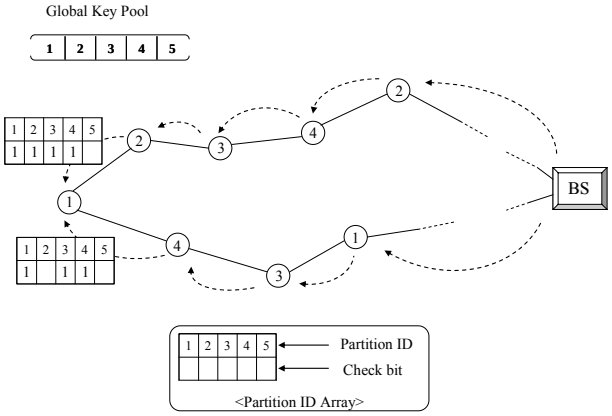

Fig. 7 Evaluation and selection of incoming paths

After the flooding, every node evaluates the detection power of each incoming path based on the stored partition ID array. If all the bits in the array of a path are set, the path will detect most fabricated reports. That is, the path is most secure against false data injection attacks. If a very small number (or none) of the bits are set, most fabricate reports will not be verified by the forwarding nodes. The node may be vulnerable to false data injection attacks. Note that there is a trade-off between detection power and overhead. For a legitimate report, the former path may consume more energy than the latter path because computational overhead is incurred when a node verifies a received report. In Fig. 7, the upper path may be the most secure against false data injection attacks since the numbers of the bits are more filled in the array than the lower path. However, it may consume more energy than the lower path in report forwarding. On the other hand, the lower path is more vulnerable than the upper path. But it may be more energy efficient than the lower path in report delivering.

A path is chosen by an evaluation function that decides the qualification as the path that is both most secure and yet energy conserving, based on the detection power and hop count of a path. An evaluation function can be:

$$Q(p) = D(p) + P(p) \quad (1)$$

Where p is a path, $D(p)$ is the distance of p in hop count, and $P(p)$ is the number of unset bits in the partition ID array received from p. Note that a smaller $Q(p)$ is more qualifiable than a larger one. Each node evaluates the qualification of the incoming paths and decides the routing path with lower qualification than other paths. The qualification of the path is in inverse proportion to $P(p)$. Therefore, the path which has many partition ID array bits is selected by the node as its routing paths and it will increase the detection power of the network against false data injection attacks.

5. Simulation Results

To show the effectiveness of the proposed method, we have compared the original SEF with the proposed method through simulation. Each node takes 16.56, 12.5μJ to transmit/receive a byte and each MAC generation consumes 15μJ [4]. There are 1,000 keys in the global key pool which is divided into 20 partitions. Every node evaluates the qualification of a path using equation (1).

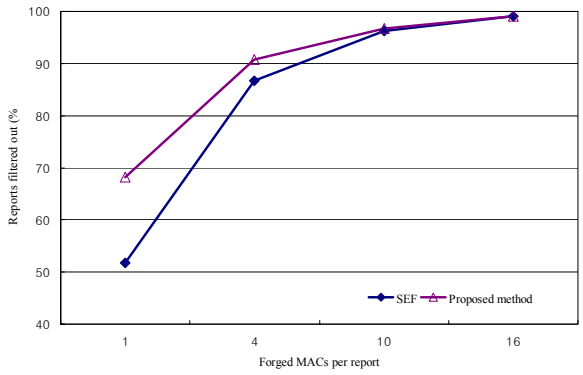

Fig. 8 ratio of the filtered reports

Fig. 8 shows the ratio of filtered fabricated reports when the number of forged MACs in a report is 1, 4, 10 and 16. As shown in the figure, the proposed method can filter out a larger number of fabricated reports during the forwarding process than the original SEF ($P(p) = 0$) since a routing path in the proposed method is chosen based on not only distance but also detection power.

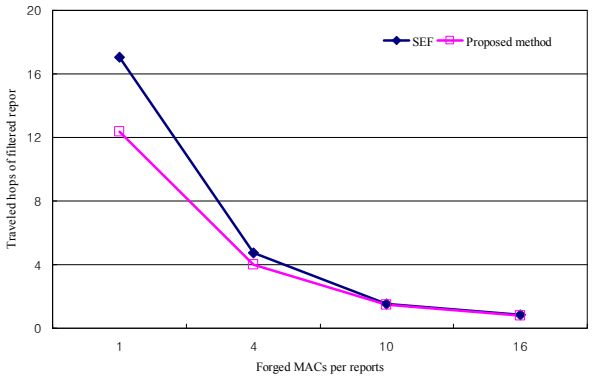

Fig.9 Average number of hops that a filtered report traveled

Fig. 9 shows the average number of hops that a filtered report travels when the number of forged MACs per report was 1, 4, 10 and 16. As shown in the figure, the proposed method can detect fabricated reports earlier than the original SEF since routing paths are chosen with consideration of detection power in the proposed method.

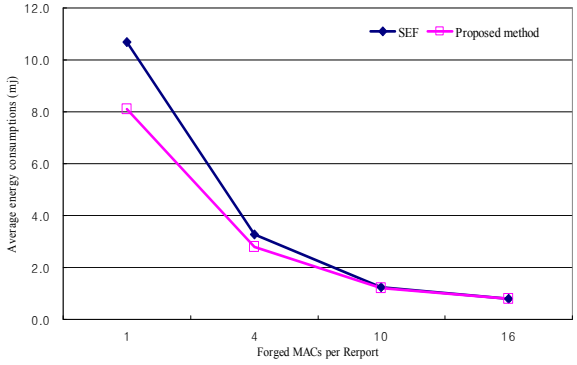

Fig.10 Average energy consumptions per false report

Fig. 10 shows the average energy consumption caused by a fabricated report when the number of forged MACs per report is 1, 4, 10 and 16. As shown in the figure, the proposed method can conserve more energy than the original SEF since it can detect and drop fabricated reports earlier than SEF, before they consume a significant amount of energy (Fig. 8).

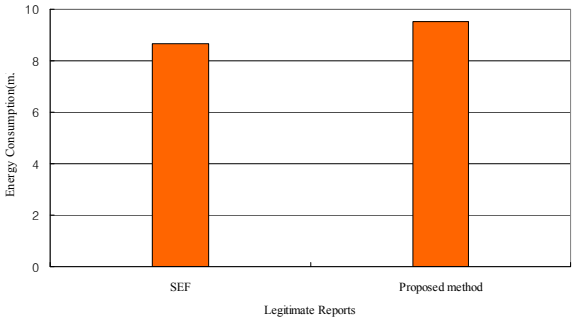

Fig.11 Average energy consumption per legitimate report

Fig. 11 shows the average energy consumption per legitimate report. The proposed method is more inefficient than the original SEF. However, the difference between them is very small. That is, the proposed method can conserve energy better than the original SEF

6. Conclusion

A path selection method for improving the detection power of SEF is presented. In the proposed method, each node can select the safest path against false data injection-attacks using a security evaluate function which evaluates the qualification of incoming paths.

Simulation results show that the proposed method is more effective than SEF in detection of fabricated reports. The result also shows that the proposed method can lower the energy consumption than the existing method. As stated section 3, the choice of routing path represents a trade-off between security level and overhead. Thus, our future research will focus on the adaptive selection of routing paths.

Acknowledgments

This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Advancement). (IITA-2007-C1090-0701-0028)

References

[1] Yang and S. Lu, “Commutative Cipher based En-Route Filtering in Wireless Sensor Networks”, Proc. of VTC, pp. 1223-1227, Sep. 2003.

[2] K. Akkaya and M. Younis, “A Survey on Routing protocols for Wireless Sensor Networks”, Ad hoc Netw., vol. 3, no. 3, pp. 325-349, May 2005.

[3] V. Shah Mansouri, Y. Ghiassi-Farrokhfal, M. MohammadNia-Avval, and B. H. Khalaj, “Using a Diversity Scheme to Reduce Energy Consumption in Wireless Sensor Networks”, Proc. of Broadband Networks, vol. 2, pp. 940-943, Oct. 2005.

[4] F. Ye, H. Luo, and S. Lu, “Statistical En-Route Filtering of Injected False Data in Sensor Networks”, *IEEE J. Sel. Area Comm.*, vol. 23, no. 4, pp. 839-850, Apr. 2005.

[5] Q. Jiang and D. Manivannan, “Routing Protocols for Sensor Networks”, Proc. of CCNC, pp. 63-98, Jan. 2004.

[6] B. Przydatek, D. Song, and A. Perrig, “SIA: Secure Information Aggregation is Sensor Networks”, Proc. of SenSys, pp. 255-265, Nov. 2003.

[7] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An Interleaved Hop-by-Hop Authentication Scheme for filtering of Injected False Data in Sensor Networks”, Proc. of S&P pp. 259-271, 2004.

[8] W. Zhang and G. Cao, “Group Rekeying for Filtering False Data in Sensor Network: A Predistribution and Local Collaboration-based Approach”, Proc. of INFOCOM, pp. 503-514, Mar. 2005.

[9] F. Li and J. Wu, “A Probabilistic Voting-based Filtering scheme in Wireless Sensor Networks”, Proc. of IWCMC, pp. 27-32, Jul. 2006.

Chung Il Sun received his B.S. degrees in computer engineering from Kyungwon University, Korea, in February 2007. He is currently a graduate student in the School of Information and Communication Engineering at Sungkyunkwan University. His research interests include wireless sensor networks, modeling & simulation and security in wireless sensor networks.

Tae Ho Cho received the Ph.D. degree in electrical and computer engineering from the University of Arizona, USA, in 1993, and the 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 School of Information and Communication Engineering, Sungkyunkwan University, Korea. His research interests are in the areas of wireless sensor network, intelligent system, modeling and simulation, enterprise resource planning.