

Hop by Hop On Demand Path Selection Method for Sensor Networks

Soo Young Moon, Tae Ho Cho

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

Abstract— Due to the nature of wireless sensor networks (WSNs) such as battery usage, limited computation capability and wireless communication, there are many threats in WSNs. Among these, false report attacks exploit compromised nodes to forge and inject false reports into a network so that they waste valuable energy of sensor nodes and confuse a user. Statistical en route filtering scheme is one of filtering schemes that detect and remove false reports. In the scheme, routing paths of event reports affect the filtering rate. We propose a hop by hop on demand path selection method to increase the filtering rate. Simulation results show that the proposed method enhances the filtering rate of the scheme. Hence, sensor nodes' energy consumption for forwarding false reports decreases.

Keywords— wireless sensor network, statistical en route filtering, false report injection, path selection, security

I. INTRODUCTION

Advancements in processors and wireless communication technologies enabled the development of low power, wireless sensor nodes [1]-[3]. WSNs are composed of small, lightweight sensor nodes, which are capable of sensing, computing, and communicating with each other, and one or more sink nodes which collect event information from sensor nodes and report it to users. WSNs can be applied to areas including environment monitoring, social networking, and health care [1].

In many applications, sensor nodes suffer from the limitation of resources such as battery power, computation capacity, and memory [4], [5]. Additionally, sensor nodes communicate with each other using wireless links. Due to the features, there are many security threats in WSNs. Among these, in false report attacks, an attacker captures several sensor nodes in the field and reprograms them so that they report non-existent events to users. False reports injected by such compromised nodes result in depletion of forwarding nodes' energy and confuse a user. Fig. 1 depicts the false report attacks.

To detect and remove the false reports early, Fan Ye et al. proposed the statistical en route filtering (SEF) scheme [6]. In SEF, selection of routing path for event reports influence filtering rate of false reports. In this paper, we propose a hop by hop on demand path selection method to enhance filtering

capability. In the proposed method, each sensor node maintains the list of candidate parent nodes which can be selected as a forwarding node. When a sensor node sends an event report, it considers message authentication codes in the report and security key information of candidate parent nodes. Then it selects one node which is with high probability able to verify the report. Proposed method increases the false report filtering rate of SEF, and result in decrease of energy consumption for forwarding the false reports.

The remaining sections are as follows. In section 2, we review the SEF. In section 3, we present the path selection method and explain its operational phases. In section 4, we compare filtering rate of SEF and the proposed method based on simulation results. In section 5, some existing path selection methods are described. Finally, we conclude the paper in section 6.

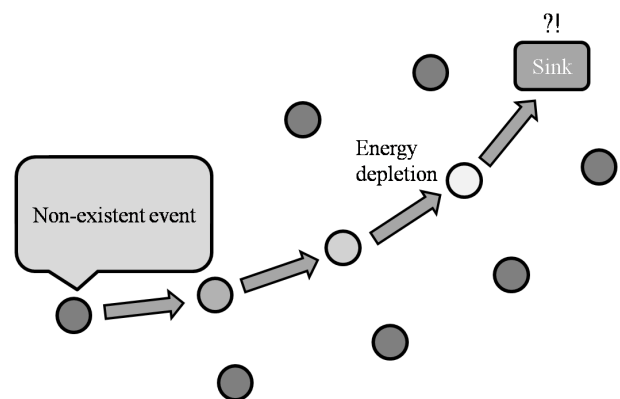


Figure 1. False Report Attacks in WSN

II. BACKGROUND

A. Statistical En route Filtering

Statistical en route filtering (SEF) scheme [6] was proposed by Fan Ye et al. and it aims to detect and drop false reports in early phase. In SEF, event sensing nodes collaborate to authenticate event information. If an attacker compromises sensor nodes less than certain threshold value, false reports

generated by the compromised nodes are detected and dropped en-route.

In SEF, sensor nodes are assigned with authentication keys which are part of global key pool managed by a sink node. The global key pool is divided into key partitions and a node is loaded with a portion of a key partition. After the sensor nodes are deployed in the target area, they continuously monitor the area until interesting events occur.

When an interesting event occurs, the sensing nodes elect a center of stimulus (CoS) node. CoS node collects message authentication codes (MACs) from other sensing nodes to guarantee the authenticity of event information. CoS node generates an event report containing event information, the MACs and corresponding key indices. Then CoS node forwards the event report to the next node in the path between itself and the sink node. Intermediate nodes verify the MACs in the report by using their own authentication keys and drop if the verification fails.

The SEF is able to detect and drop false reports independently of routing paths. However, the selection of routing paths affects the filtering rate of SEF because each node possesses only a small portion of the global key pool. Figure 2 illustrates the filtering operation of SEF.

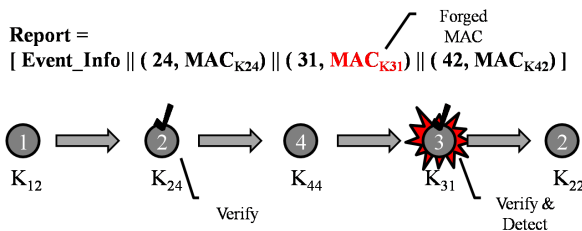


Figure 2. Filtering operation in SEF

In figure 2, the false report contains three MACs, which was generated by using the authentication of partition 2, 3, and 4 each. In this case, one MAC corresponding to key K_{31} was forged. As the false report proceeds, forwarding nodes verify the MACs in the report if they possess one of keys corresponding to a MAC in the report. The node with the key K_{24} verifies the corresponding MAC in the report. However, since the MAC is valid, the false report is not detected. When the node with the key K_{31} receives the report, it verifies the $MAC_{K_{31}}$. Since the MAC is forged MAC, the false report is detected and dropped by the node.

III. PATH SELECTION METHOD

A. Motivation

In SEF, each sensor node possesses authentication keys those are part of the global key pool. Hence a sensor node is able to verify only MACs generated by using one of its authentication keys. As a result, the filtering rate of the scheme is affected by routing paths for event reports. To increase the filtering rate, it is needed to consider key information of MACs in the received report and neighbor nodes. Then a node can forward the report to the node which

is with high probability capable of verifying a MAC in the report. If one neighbor node possesses authentication keys from the same key partition to which a MAC in the report belongs, then the neighbor node is considered the node which is with high probability capable of verifying the MACs in the report.

B. Assumptions

The assumptions in the proposed method are as follows. Each node knows its location information. Sensor nodes use bi-directional wireless links to communicate with each other. The sink node initializes a routing message and propagates it to the entire sensor network to set routing paths. A sensor network is secure until neighbor nodes discover each other.

C. Overview

There are six phases in the proposed method. In the pre-deployment phase, sensor nodes are assigned with their IDs and authentication keys from global key pool. In the neighbor discovery phase, sensor nodes placed within radio communication range communicate with and discover each other using simple hello and response messages. Every node broadcasts the hello message to all the nodes in its transmission range. Each node that received the hello message replies with a response message. A hello message contains the ID of the sender, and a response message includes the IDs of the sender and receiver of the message. When a node receives a hello message or a response message, it adds the sender's ID to its neighbors list. In the route discovery phase, the sink node creates a routing message and propagates it to the entire network using flooding. The routing message includes the sender's ID, the distance to the sink node and key partition of the sender. When a sensor node receives the routing message, it checks whether the sender's ID is in its neighbours list. Then it compares the distance from itself and the sender to the sink node. If the sender is closer to the sink node than itself, it stores the information of the sender to its list of candidate parent nodes and forwards the message to its neighbor nodes. Table 1 shows the candidate parent nodes list of each node.

TABLE 1. CANDIDATE PARENT NODES LIST

ID	Distance to the sink	Key partition
N1	DN1	PN1
N2	DN2	PN2
...	...	...

In the event report generation phase, event sensing nodes collaboratively elect a center of stimulus (CoS) node which is responsible for generating an event report. The CoS node collects MACs generated by other sensing nodes exploiting their authentication keys to guarantee the authenticity of event information. Then it organizes the event report containing the event information, MACs and the corresponding key indices. In the en route filtering phase, sensor nodes receive the event report and verify MACs in it if they have corresponding keys. If the verification fails the report is dropped. When a sensor node forwards the report to the next node, it chooses one of candidate parent nodes as the next node. It considers distance to

the sink node and key partition information of each candidate parent node.

D. Selection of a next node

In the proposed method, a routing path of each event report is selected hop by hop and on demand fashion. Each forwarding node independently chooses the next node by an evaluation function. The evaluation function outputs the fitness value of each candidate parent node as a next node. The function can be represented as the equation below.

$$Q(n) = \alpha \cdot D(n) + \beta \cdot VP(n) \quad (1)$$

In the above equation, n is a candidate parent node, $D(n)$ is the distance from the node to the sink node, and $VP(n)$ is the verification probability of the node for the event report to be sent. The two constants, α and β are weights for each factor, respectively. Each node selects the candidate parent node with the largest fitness value as the next node and forwards the event report to it. Figure 3 describes the selection of a next node.

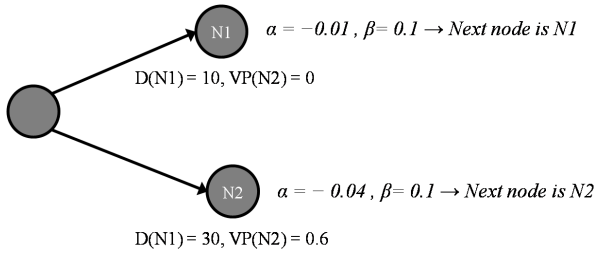


Figure 3. Selection of a next node

In the figure 3, the node on the left selects a forwarding node from the two candidate parent nodes, N1 and N2. $D(Ni)$ and $VP(Ni)$ ($i=1, 2$) means the distance from the node to the sink node and its verification probability for an event report to be forwarded. By adjusting α or β (or both), we can choose energy efficient path or secure path hop by hop and on demand fashion.

IV. RELATED WORK

Other than the SEF, many filtering schemes have been proposed. The dynamic en-route filtering [7] scheme was proposed by Yu and Guan. In [7], sensor nodes are grouped into clusters and each cluster header node disseminates the authentication keys of the sensor nodes in its cluster. Sensor nodes can detect and drop false reports in a sensor network with dynamic topology. The probabilistic voting-based filtering scheme [8] was proposed by Li and Wu. In [8], sensor nodes can defend both false MAC attacks and false report attacks by adopting a voting scheme when filtering event reports. Zhu proposed the interleaved hop-by-hop authentication [9] scheme. In [9], a false report is detected and dropped within t hops if no more than t nodes are

compromised and every node is aware of the IDs of its associated nodes [10].

A few path selection methods to enhance false report filtering rate in sensor networks were proposed recently. Sun et al. proposed path selection method [11] for SEF. In [11], a control message initiated by the sink node is propagated to set routing paths. Each control message contains the sender ID, the hop count and detecting power of the path through the sender. Every node chooses one path from it to the sink node based on the information. The method can increase the en route filtering probability of SEF. However, in [11] it is hard to detect and drop false reports early since each sensor node forwards event reports through the same, fixed path regardless of the MACs in the reports.

In [12], Lee and Cho proposed fuzzy-based path selection method to improve the filtering capability of dynamic en route filtering scheme [7]. In the method, each cluster chooses a forwarding path to the sink node based on fuzzy logic in consideration of detection power, distance, and the energy level of a path. As same as in [11], it is hard to detect and drop false reports early and adapt to node failure since each cluster forwards event reports through the same fixed path.

V. SIMULATION RESULT

We simulated the filtering rates and energy consumption of the SEF and the proposed method. In the simulation, 600 sensor nodes are deployed in the sensor field of $500 \times 500 \text{ m}^2$ size. Energy consumption for transmitting/receiving a byte is $16.25/12.5 \mu\text{J}$, and $15 \mu\text{J}$ for generating a MAC [13], [14]. The size of an event report is 36 bytes. Figure 4 compares the filtering rates of the SEF and the proposed scheme.

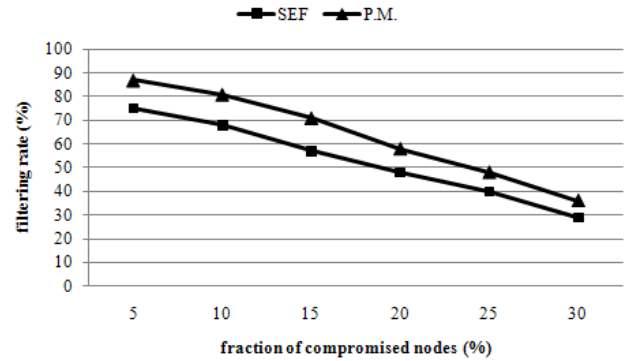


Figure 4. Comparison of Filtering Rates

As shown in Figure 4, the proposed method achieves higher filtering rate than that of the SEF as the fraction of compromised nodes varies. Since in the proposed method each node considers key information of MACs in the received report and neighbor nodes, false reports are detected and dropped earlier and with higher probability than in the SEF. Figure 5 represents the amount of energy consumption in the SEF and in the proposed method.

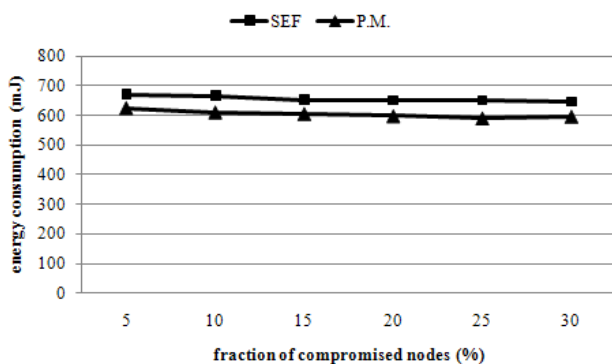


Figure 5. Comparison of energy consumption

Figure 5 shows that the proposed method consumes less energy than the SEF as the fraction of compromised nodes increases. Since false reports are detected and dropped earlier and with higher probability in the proposed method than in the SEF, energy consumption of intermediate nodes for forwarding false reports decreases.

VI. CONCLUSION

In this paper we proposed the hop by hop on demand path selection method to enhance the filtering rate of SEF. In SEF, selection of routing paths for event reports affect the filtering rates of false reports since each node can verify only the MACs generated by exploiting one of its authentication keys. In the proposed method, the selection of routing paths is performed hop by hop, on demand manner. Each node manages the information of candidate parent nodes and chooses the next node based on the distance to the sink, and the verification probability. The proposed method enhances the filtering rate of the SEF and hence reduces the energy consumption of intermediate nodes for forwarding false reports. Our future work is to investigate other factors that can be exploited to improve the proposed method in terms of security and energy conservation.

ACKNOWLEDGMENT

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

REFERENCES

- [1] J. A. Stankovic, "When Sensor and Actuator Networks Cover the World," *ETRI Journal*, vol. 30, no. 5, 2008.
- [2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-116, 2002.
- [3] K. Akkaya, Mohamed Younis, "A survey on routing protocols for wireless sensor networks," *Ad Hoc Networks*, vol. 3, pp. 325-349, 2005.
- [4] C. Karlof, and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Elsevier, Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Protocols and Applications*, vol. 1, no. 2-3, pp. 293-315, 2003.
- [5] D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile Ad-Hoc and Sensor Networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, pp. 2-28, 2005.
- [6] F. Ye, H. Luo, and S. Lu, "Statistical en-route filtering of injected false data in sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 4, pp. 839-850, 2005.
- [7] Z. Yu, and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," *Proc. of INFOCOM*, pp. 1-12, 2006.
- [8] F. Li, and J. Wu, "A Probabilistic voting-based filtering scheme in wireless sensor networks," *IWCMC '06*, pp. 27-32, 2006.
- [9] S. Zhu, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 3, no. 3, pp. 1-33, 2007.
- [10] P. T. Nghiem and T. H. Cho, "A fuzzy-based interleaved multi-hop authentication scheme in wireless sensor networks," *Journal of Parallel and Distributed Computing*, vol. 69, no. 5, pp. 441-450, 2009.
- [11] C. I. Sun, H.Y. Lee and T.H. Cho, "A Path Selection Method for Improving the Detection Power of the Statistical Filtering in Sensor Networks," *Journal of Information Science and Engineering*, vol. 25, no. 4, pp. 1163-1175, 2009.
- [12] H. Y. Lee, T. H. Cho, "Fuzzy-based Path Selection Method for Improving the Detection of False Reports in Sensor Networks," *IEICE Transactions on Information and Systems*, vol. E92-D, no. 8, pp. 2009.
- [13] Xbow sensor networks, <http://www.xbow.com>
- [14] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System Architecture Directions for Networked Sensors," in *Proc. ASPLOS*, pp. 93-104, 2000.