A Multipath Immunity-based Statistical En-route Filtering in Wireless Sensor Networks

Yuji Watanabe and Tomotsugu Tamura

Nagoya City University, Nagoya 467-8501, Japan
(Tel: 81-52-872-5037, Fax: 81-52-872-5037)

yuji@nsc.nagoya-cu.ac.jp

Abstract: In our previous studies, we have proposed an immunity-based statistical en-route filtering (ImSEF) to not only eliminate false data injection attack in wireless sensor networks but also identify compromised nodes which are injecting false data. Some simulation results showed that ImSEF outperformed the original SEF. However, ImSEF does not deal with false negative attack where a compromised node can block legitimate reports from forwarding through it. In addition, ImSEF mistakenly filter out legitimate reports en-route with low probability (mistaken filter). In this paper, we propose a multipath immunity-based statistical en-route filtering (ImMEF) to combat both the false negative attack and the mistaken filter. Like a multipath en-route filtering method (MEF) proposed by Kim and Cho, ImMEF exploits a multipath routing technique and a random key pre-distribution scheme for key assignment. We carry out some simulations to evaluate the performance of ImMEF.

Keywords: Wireless sensor networks, Statistical en-route filtering, Immunity-based approach, Multipath routing

1 INTRODUCTION

Wireless sensor networks consisting of many small and cheap sensor nodes may be deployed in a potentially adverse environment where an attacker can launch various kinds of threats. *False data injection attack*, which is also called *false positive attack*, is that sensor nodes compromised by an attacker can inject false reports of non-existing or bogus events. The attack may cause not only false alarms but also the waste of the limited energy of the nodes forwarding these reports. A *statistical en-route filtering* (SEF) [1] and several revised schemes [2-4] have been proposed to combat the attack.

In our previous studies [5-7], we also have proposed an *immunity-based statistical en-route filtering* (ImSEF) to identify compromised nodes and achieve earlier detection of false reports. In ImSEF, each node assigns *credibility* to its neighboring nodes and updates the credibility based on the success or failure of filtering and transmission. And then each node uses the updated credibility as the probability of the next communication. Both simulation results and mathematical analyses [6,7] showed that ImSEF outperformed the original SEF. However, SEF and ImSEF do not deal with *false negative attack* where a compromised node can block legitimate reports from forwarding through it. As a result, users cannot receive the legitimate reports and cannot take appropriate countermeasures. In addition, ImSEF mistakenly filters out legitimate reports en-route with low probability (*mistaken filter*) in the environment where both legitimate and fake reports exist.

In this paper, we propose a *multipath immunity-based statistical en-route filtering* (ImMEF) to deal with not only false negative attack but also mistaken filter. Like a *multipath en-route filtering method* (MEF) proposed by Kim and Cho [3], ImMEF also exploits a multipath routing technique and a random key pre-distribution scheme for key assignment. We carry out some preliminary simulations to evaluate the performance of ImMEF.

2 SENSOR NETWORK MODEL

Following the previous studies on SEF, we consider a large-sized sensor network composed of a lot of sensor nodes and a base station (BS) which is a data collection center. We further assume that the nodes are deployed at a high density, so that an event (sensing target) can be detected by multiple surrounding nodes. It is unnecessary for each of the detecting nodes to send the event report (e.g., the location, the time, and the type of event) to the BS, so that one of them is elected as cluster head (CH). The CH collects all the event reports from all the detecting nodes and forwards a synthesized report to the BS. The report potentially traverses a large number of hops.

We assume that an attacker can compromise some nodes to obtain the security information installed in the nodes. Once compromised, the nodes can be used to inject false data reports of bogus events. Such an attack is called a *false data injection attack* (*false positive attack*). This paper also focuses on *false negative attacks* where a compromised node can block legitimate reports from forwarding through it. However, we consider that the attacker cannot defeat the BS because the BS has powerful security.

3 IMMUNITY-BASED STATISTICAL EN-ROUTE FILTERING (ImSEF) [5-7]

SEF and ImSEF can probabilistically filter out false reports en-route. They exploit collective decision-making by multiple detecting nodes and collective false detection by multiple forwarding nodes. They consist of three major components: (1) key assignment and report generation, (2) en-route filtering, and (3) base station verification. In addition, ImSEF has the credibility update and the communication based on the updated credibility.

3.1 Key Assignment and Report Generation

The process of key assignment and report generation in ImSEF is as follows.

1) The BS maintains a global key pool of N secret keys $\{K_i, 0 \leq i \leq N-1\}$, divided into n non-overlapping partitions $\{P_j, 0 \leq j \leq n-1\}$. Each partition has m keys (i.e., $N = m\ n$). A simple way to partition the key pool is $P_j = \{K_i | jm \leq i \leq (j+1)m - 1\}$.
2) Before each sensor node is deployed, it stores randomly chosen k ($k < m$) keys from a randomly selected partition in the key pool.
3) After all the nodes are deployed, they broadcast their indexes to their neighboring nodes within one-hop distance. Every node receives the message from each of its neighbors, establishes a list of neighboring nodes, and then assigns a state variable $R(t) \in [0,1]$ indicating the *credibility of neighbor* to each neighboring node. The initial value of credibility $R(0)$ is set to 1.
4) When an event appears, multiple surrounding nodes can detect the event. A CH is elected from the detecting nodes for creating the synthesized event report.
5) Each of the nodes that detected the event generates a keyed message authentication code (MAC) M_i using the event report E and a randomly selected K_i, one of its k stored keys. Each detecting node then sends the key index and the MAC, $\{i, M_i\}$, to the CH. K_i is secret while M_i is public.
6) The CH collects all the $\{i, M_i\}$s from the detecting nodes and randomly chooses T MACs from distinct partitions. This set of multiple MACs acts as the proof that the report is legitimate. Then the CH sends the final report with T attached key indices and T MACs, e.g. $\{E, i_1, M_{i1}, i_2, M_{i2}, \ldots, i_T, M_{iT}\}$, toward the BS.

Fig. 1 depicts an example of the key assignment and report generation in ImSEF. In this figure, the BS has a global key pool of N = 12 keys divided into n = 4 partitions, each of which has m = 3 keys. Each node randomly picks k = 2 secret keys from one partition of the key pool. After each detecting node endorses the event report by producing a keyed MAC using one of its 2 stored keys, the CH collects all the MACs from the detecting nodes and attaches randomly selected T = 3 MACs, that is, M_2, M_9, and M_{10}, to the event report E.

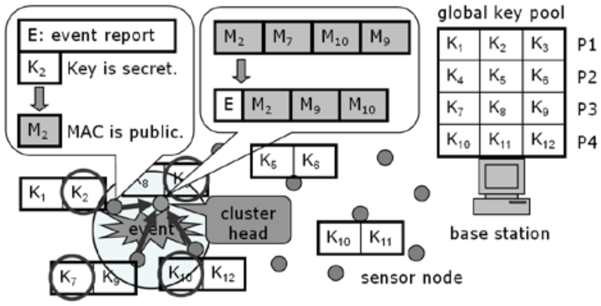

Fig. 1. An example of the key assignment and report generation in ImSEF [5].

3.2 En-Route Filtering and Credibility Update

In the en-route filtering component of SEF and ImSEF, intermediate forwarding nodes verify the correctness of the MACs probabilistically, and drop a report with forged MACs en-route. ImSEF also performs the credibility update and the communication based on the updated credibility. The process of en-route filtering in ImSEF is as follows.

1) Forwarding node j receives a report from the previous neighboring node i in proportion to the credibility $R_{ji}(t)$ of node i. In other words, node j drops a report from node i with the probability (1 - $R_{ji}(t)$) unconditionally and finishes the filtering process.
2) Since a legitimate report carries exactly T MACs produced by T keys of distinct partitions, a report with fewer than T MACs or more than one MAC in the same partition is dropped. Node j decreases the credibility $R_{ji}(t)$ of the previous node i and finishes the filtering process.
3) For the randomized key assignment, node j has a certain probability of possessing one of the keys that are used to produce the T MACs. If node j finds out that it has one of the T keys in the report, then it reproduces the MAC using its stored key and compares the result with the corresponding MAC attached to the report. If the reproduced MAC is different from the attached one, then the report is

dropped, the credibility $R_{ji}(t)$ of the previous node i decreases, and the filtering process is finished.

4) If node j verifies the reproduced MAC is the same as the attached one or if node j does not have any of the T keys, then it forwards the report to the next neighboring node k and replies an acceptance message to the previous node i to inform that the validation of the report is successful. Note that node j does not reply to node i if it discards the report.

5) Node j waits a reply from the next node k for a certain time. If node j can receive the reply from the next node k, it increases the credibility $R_{ji}(t)$ of the previous node i. Otherwise it decreases $R_{ji}(t)$.

To sum up the credibility update, node j updates the credibility $R_{ji}(t)$ of the previous node i based on its filtering result or the reply from the next node k as follows:

$$R_{ji}(t+1) = \begin{cases} R_{ji}(t) + \Delta_s & \text{if node } j \text{ receives the reply from next node } k \\ R_{ji}(t) - \Delta_f & \text{if node } j \text{ does not receives the reply from next node } k \\ R_{ji}(t) - \Delta_d & \text{if node } j \text{ drops the report} \end{cases}$$

For example, in Fig. 2, node i increases the credibility R_{ih} of the previous node h because the reply from the next node j can be received. However, node j decreases the credibility R_{ji} of the previous node i because the next node k drops the report and does not reply to node j. Since node k discards the report by itself, the credibility R_{kj} of the previous node j also decreases. To achieve the identification of compromised nodes, ImSEF not only updates the credibility but also uses the updated credibility as the receiving probability as mentioned in process 1) of the en-route filtering. In the same example, assuming that node h is compromised. Node i has an adversely higher probability of receiving the report from compromised node h because of the increase in the credibility R_{ih}. However, since node j has a lower probability of receiving a report from node i, node i may fail to send a next report to node j, and then the credibility R_{ih} of the previous node h in the neighborhood list of node i decreases. Although the credibility R_{kj} of the previous node j in the neighborhood list of node k decreases at first, if node j sends legitimate reports received from other previous nodes to node k, the credibility R_{kj} can be recovered. By iterating the credibility update and the communication based on the updated credibility, ImSEF is expected to inhibit neighboring nodes of compromised nodes from forwarding false reports.

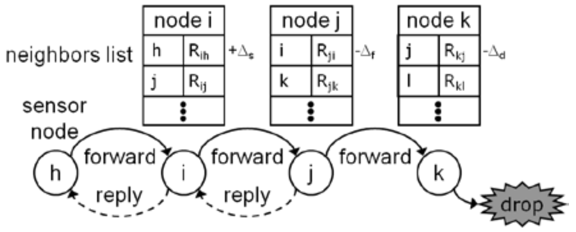

Fig. 2. An example of the credibility update in the en-route filtering process of ImSEF [5].

3.3 Base Station Verification

Owing to the statistical nature of the detection mechanism, a few bogus reports with invalid MACs may escape en-route filtering and reach the BS. In the base station verification process, the BS further verifies the correctness of all MACs and eliminates false reports that elude en-route filtering.

4 PROPOSED MULTIPATH ImSEF (ImMEF)

SEF and ImSEF do not address *false negative attacks* such as blocking legitimate reports or selective forwarding attacks by a compromised intermediate node. Furthermore, ImSEF may mistakenly drop legitimate reports in process 1) of the en-route filtering with low probability (*mistaken filter*). Kim and Cho [3] have proposed a *multipath en-route filtering method* (MEF) to tackle false negative attacks, and shown that MEF is more resilient to the attacks up to a certain number of compromised nodes than SEF.

In this paper, we propose a *multipath immunity-based statistical en-route filtering* (ImMEF) to deal with not only false negative attack but also mistaken filter. Like MEF, ImMEF exploits a multipath routing technique and a random key pre-distribution scheme for key assignment. Specifically speaking, the process 6) of report generation is changed as follows:

6') The CH collects all the $\{i, M_i\}$s from the detecting nodes and classifies the MACs into P separate groups, hashed as a function of key partition number, j of P_j. The CH allocates each of P different hash groups onto each path toward the BS. From each hash group, the CH randomly chooses S MACs and attaches them to the event report on the path. The CH sends P event reports of different hash group to the BS via multiple disjoint paths. The number of transmitted MACs per path is S ($S \leq T$) because the CH aggregates as least T MACs. The BS previously sets values for T and S.

The en-route filtering component in ImMEF is also slightly changed from T MACs to S MACs. In addition, a forwarding node verifies the group of received reports in process 2) of the en-route filtering. If a key index does not belong to the key group in the report, the report is dropped.

Fig. 3 shows an example of event reports of different hash group on multiple disjoint paths where P = 2 and S = 2. There are 2 event reports which have 2 MACs, M_6 and M_{10} and M_2 and M_9, of the hash group for “group 0 mod 2” and for “group 1 mod 2”, respectively. Even if a compromised node can stall forwarding a legitimate report on a path as shown in Fig. 3, or a normal forwarding node mistakenly drops a report, the BS can receive the other reports.

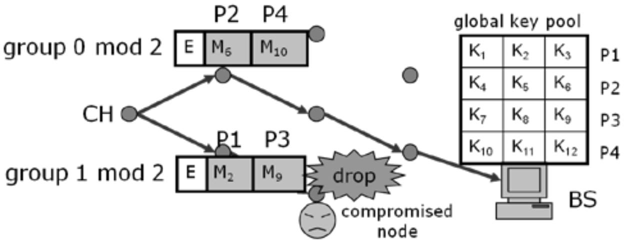

Fig. 3. An example of event reports of different hash group on multiple disjoint paths where P = 2 and S = 2.

5 SIMULATION

We perform some preliminary simulations to evaluate the performance of ImMEF on the following conditions: 9×100 sensor nodes are located in a two-dimensional lattice field. 9 source nodes sit at the left side of the field, and a base station is at opposite ends, with 100 hops between the sources and the base station. One of the source nodes is compromised and sends 1000 bogus reports, while the remaining sources transmit 1000 legitimate reports. A global key pool consists of N = 1000 keys, divided into n = 10 partitions, each of which has m = 100 keys. Each node has k = 50 keys. When T = 5, the number of transmitted MACs S per path and the number of disjoint paths P are varied as satisfying the inequality $P \cdot S \leq T$. All the values of the parameters Δ_s, Δ_f, and Δ_d are set to 0.02.

Fig. 4 illustrates the percentage of mistakenly dropped legitimate reports as a function of the number of paths P for ImMEF. ImSEF corresponds to ImMEF where P = 0. The result shows that as the number of paths increases, the percentage of mistakenly dropped legitimate reports decreases. By using multiple disjoint paths, ImMEF has been shown to deal with mistaken filter. We are now carrying out additional simulations for false negative attacks comparing with MEF, so that we will show the results at conference site.

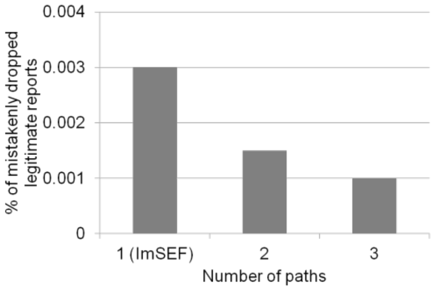

Fig. 4. Percentage of mistakenly dropped legitimate reports as a function of the number of paths P for ImMEF.

6 CONCLUSION

In this paper, we proposed a multipath immunity-based statistical en-route filtering (ImMEF) to deal with not only false negative attack but also mistaken filter. We performed some preliminary simulation to evaluate the performance of ImMEF. In future, the proposed scheme will be combined with the other revised SEFs for a higher security level.

ACKNOWLEDGEMENTS

This work was partly supported by a Grant-in-Aid for Scientific Research (C) (22500063) from the Japan Society for the Promotion of Science.

REFERENCES

[1] Ye F, Luo H, Lu S, Zhang L (2005), Statistical En-Route Filtering of Injected False Data in Sensor Networks. IEEE Journal on Selected Areas in Communications 23(4):839-850

[2] Yu Z, Guan Y (2006), A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks. Proceedings of the 25th IEEE Conference on Computer Communications, 1-12

[3] Kim MS, Cho TH (2007), A Multipath En-Route Filtering Method for Dropping Reports in Sensor Networks. IEICE Transactions on Information and Systems E90-D(12):2108-2109

[4] Krauß C, Schneider M, Bayarou K, Eckert C (2007), STEF: A Secure Ticket-Based En-route Filtering Scheme for Wireless Sensor Networks. 2nd IEEE International Conference on Availability, Reliability and Security, 310-317

[5] Watanabe Y (2010), An Immunity-based Scheme for Statistical En-route Filtering in Wireless Sensor Networks. LNCS 6278, 660-665

[6] Watanabe Y (2011), Performance Evaluation of Immunity-based Statistical En-route Filtering in Wireless Sensor Networks. Artificial Life and Robotics, 16(3):422-425

[7] Watanabe Y (2011), An Analysis of Immunity-based Statistical En-route Filtering in Wireless Sensor Networks. 3rd International Conference on Management of Emergent Digital EcoSystems, 250-256