Node Density Loss Resilient Report Generation Method for the Statistical Filtering Based Sensor Networks

Jin Myoung Kim, Nonmember and Hae Young Lee, Member

SUMMARY In the statistic en-route filtering, each report generation node must collect a certain number of endorsements from its neighboring nodes. However, at some point, a node may fail to collect an insufficient number of endorsements since some of its neighboring nodes may have dead batteries. This letter presents a report generation method that can enhance the generation process of sensing reports under such a situation. Simulation results show the effectiveness of the proposed method.

key words: false positive attacks, node compromise, report generation, report endorsement, wireless sensor networks

1. Introduction

A wireless sensor network (WSN) is usually comprised of a large number of cheap and battery-powered sensor nodes, each of which has limited communication and computation capabilities. These sensor nodes monitor the environment; once some of the nodes have detected an event of interest, such as wildfire, they report the event to the base station (BS). The environment that the node monitors is often harsh, so that the nodes are commonly not attended by the network administrator. Thus, they are subject to potential threats, such as being physically captured by an adversary [1]–[3].

Captured nodes can be used to, with compromised keys in the nodes, launch various types of insider attacks, including a false positive attack (FPA) that injects false data into the network [4]–[7]. To deal with FPAs, researchers have proposed en-route filtering schemes [1], [5], [8], including the statistical en-route filtering scheme (SEF) [4]. In SEF, each sensing report must carry $T$ message authentication codes (MACs). These $T$ MACs must be generated by different nodes, with keys from different partitions in the global key pool. At the initial stage, $T$ is carefully determined with the consideration of the node density of the network. However, the node density would decrease over time, mainly due to dead batteries, so that, at some point, some sensing reports may fail to be generated.

In this letter, we propose a report generation method that is resilient node density loss in SEF-based WSNs. In the proposed method, if a report generation node fails to collect $T$ MACs, the node gathers additional MACs from orphan nodes that are out of communication range, through its 1-hop neighboring nodes. Thus, the proposed method can enhance the rate of successful report generation under node density loss. We show the reliability of the proposed method, compared to the original SEF, through simulation results.

2. Background and Related Work

This section describes FPAs and SEF briefly, and the problem statement.

2.1 Background

Once a node has been compromised physically or through fabricated messages, the adversary can achieve full control over it by reading its memory and influencing the operation of its software [9]. Using the node, the adversary could thus inject false sensing reports that represent non-existent events into the network. As shown in Fig. 1, the adversary’s goal may be not only to confuse the BS with false alarms, but also to drain the energy resources of the network and bandwidth in delivering them to the base station. Such a type of insider attacks is called a FPA in WSNs [4]–[7].

SEF [4] proposed by Ye et al. is the first scheme to address FPAs in the presence of compromised nodes. SEF focuses on the en-route detection of false reports injected through compromised nodes. In SEF, when an event of interest occurs, each of the detecting nodes sets a random timer. Upon the timer expiration, the node broadcasts its draft report to its neighboring nodes. The node whose draft report is accepted by the other detecting nodes becomes the report generation node, called the center-of-stimulus (CoS). The CoS then collects $T$ tuples from its neighboring nodes.
Each tuple is comprised of the index of a key and a MAC generated with that key. Finally, the CoS compiles and forwards its final report that carries the $T$ tuples. While the report being forwarded, the tuples are used by some of the forwarding nodes to verify the legitimacy of the report.

2.2 Problem Statement in SEF

In SEF, every report must carry $T$ tuples: key indices and MACs. Forwarding nodes drop any reports carrying an insufficient number (i.e., $< T$) of tuples immediately. That is, a CoS must collect $T$ tuples from its neighboring nodes. Thus, $T$, a design parameter, should be carefully selected with the consideration of the node density. Since nodes are cheap, battery-powered, and unattended, we should consider sensor failure, dead batteries, and node destruction [9]. This also means that the node density of a WSN would decrease over time. Therefore, at some point, a CoS may fail to collect $T$ tuples from its neighboring nodes (i.e., some of them may have dead batteries), so that the event would not be reported to the BS.

WSN applications require the networks to be tolerant to hardware and software failures, as well as node disconnectivity [15]. This requires that nodes to be able to guarantee fault tolerance; when nodes detect an event, the generation of a report should be guaranteed. Therefore, a failure within the report generation process needs to be handled as a kind of faults in WSNs.

3. Proposed Method

The section describes the proposed method in detail.

3.1 Network Model

The proposed method considers a flat, highly-dense WSN that consists of homogeneous, battery-powered sensor nodes. We assume that SEF is applied to the network as a FPA countermeasure. Initially, $T$ is carefully chosen by the network administrator, with the consideration of the node density of the network and the number of partitions in the global key pool. Once an event occurs, it is detected by multiple nodes. Some of them are then elected as CoSs. We also assume that a CoS may not directly communicate with some of the detecting nodes due to out of communication range. We further assume that the administrator cannot replace or recharge nodes’ batteries, so that the nodes density decreases over time.

3.2 Overview

Figure 2 shows the election of three CoSs. Filled, gray, and empty circles are the CoSs, detecting, and non-detecting nodes, respectively. Some nodes have detected the same event but not involved in the report generation since they are out of communication range (from the CoSs). We call such nodes orphan nodes. In Fig. 2(a), the number of the CoS’s neighboring nodes that have detected the event is 9 and the number of orphan nodes is 4. In Fig. 2(b), each of the CoSs has the 5 neighboring nodes that have detected the event, and 2 orphan nodes. When $T$ is 6, 7, 8, and 9 in Fig. 2(a), the probability† of successful report generation is 74.8%, 34.8%, 6.8%, and 0.3%, respectively. But a report cannot be generated in Fig. 2(b) since the CoS could collect at most 5 ($< T$) tuples.

In the proposed method, if a CoS fails to collect $T$ tuples from its 1-hop neighboring nodes, it gathers additional ones from orphan nodes, through the 1-hop neighbors. By doing so, the CoS may be able to collect $T$ tuples from its 1-hop and 2-hop neighbors. Thus, a report for the event would be successfully generated and then be delivered to the BS. If the CoS also fails to collect $T$ tuples from its 1-hop and 2-hop neighbors, the current CoS is dismissed and never becomes a CoS from now on. A new CoS will be elected through the same procedure.

3.3 Multi-Level CoS

Algorithm 1 is the algorithm of the proposed method, for CoS election and report generation, which is based on that of SEF. Once a node has detected an event, the node sets random timer $r$. (2) Before the expiration of $r$, the node listens message draft_report broadcasted by other node. Upon receiving draft_report that is acceptable, the node considers the broadcaster to be the CoS and cancels its timer. Then, the node generates a MAC over draft_report with one of its keys and sends the index of the key and the MAC (i.e., the tuple) to the CoS. Finally, the node awaits message report_sent broadcasted by the CoS.

(12) If the node has not received an acceptable message before the expiration of $r$, the node becomes the CoS and thus broadcasts its own draft_report. The CoS then collects tuples from the detecting nodes. (15) If the CoS has collected $T$ or more tuples, it compiles and sends message final_report towards the BS. Finally, the CoS broadcasts message report_sent. (20) If the CoS fails to collect $T$ tuples, it collects additional ones from orphan nodes and then attempts to send final_report. (26) If the CoS fails again, to collect $T$ tuples from its 1-hop and 2-hop neighboring nodes, it is dismissed and will be never elected as a CoS from now on.

†These rates can be calculated by Cartesian products.
4. Simulation Results

Simulations have been performed to compare the proposed method with the original SEF. Table 1 shows our simulation parameters. The criterion is the number of reports successfully generated for events. We have modeled a sensor field whose size is 100 × 100 m². Nodes are uniformly deployed on the field as shown in Fig. 3.

Figure 4 shows the number of reports that were successfully generated for 500 events. 500 events were generated, each of which occurred in a random location on the field. Random seeds were 0, 1, ..., 9. A node died if its battery ran out. So, some nodes on the field died (i.e., node density decreased) as time goes by. As shown in the figure, he proposed method (filled circles) could reduce, compared to the original SEF (filled rectangles), failures in the report generation since it allows CoSs to collect tuples from 2-hop neighbors. On average, 93.6% of events were properly reported to the BS in the proposed method, while 69.9% of them were done in the original SEF.

Figure 5 shows a CoS election result for an event at the 18th round. The location of the event is marked with ‘STIMULUS’ in Fig. 3. As shown in the figure, node 405 was elected as a CoS and nodes 37, 45, 49, 86, and 469 participated in the report generation in the original SEF. Although nodes 52, 196, and 287 had detected the same event, they did not participate during the generation due to out of transmission range. In the original SEF, the CoS (node 405) may fail to generate a report for the event if some of the participating nodes were loaded with keys from the same partition. In contrast, the proposed method allows the CoS to collect tuples from nodes 52, 196, and 287 (i.e., orphan nodes), so that it could generate a report successfully.

A report for the event could be generated in the original SEF if node 37 or 469 was elected as a CoS. However, SEF lacks a mechanism for CoS re-election. But in the proposed method, a CoS could be re-elected if the current CoS candidate fails to collect $T$ tuples from its 1- and 2-hop neighboring nodes.

5. Related Work

FPAs (or false data injection attacks) in the presence of compromised nodes were first addressed by Ye et al. [4]. To deal with FPAs, they proposed SEF, the first en-route filtering solution. The advantages of SEF include that it can applied to
flat WSNs and does not require special equipment, so that many en-route filtering solutions [1], [8], [11], [12], [14] have been proposed based on SEF. Most of them have focused on the enhancement of the en-route verification of SEF. For example, Yu and Guan’s dynamic en-route filtering scheme [1] enhanced the early detection capability of SEF, by disseminating keys used for the en-route verification to neighboring nodes at the initial stage. Sun et al. proposed a path selection method [11] for SEF, in which each node chooses the most secure routing path against FPAs at the initial stage. Kim et al. proposed a path renewal method [12] for SEF that provides a mechanism for renewing routing paths during the operational phase, with the consideration of security and balanced energy consumption. The bandwidth-efficient cooperative authentication scheme proposed by Lu et al. [8] achieves energy saving by the early detection capability based on the cooperative bit-compressed authentication technique. The efficient geographical information-based en-route filtering scheme proposed by Yi et al. [14] enhances the security of SEF by employing the en-route verification of geographical locations carried in reports.

However, they, including SEF, do not consider node density loss (mainly due to battery depletion) at the time of the generation of each report, which this letter addresses. A real event on the field will not be reported to the BS if CoS for the event fails to collect a certain number of MACs from its neighboring nodes. Thus, node density loss should be considered.

Other en-route filtering solutions [10], [13] usually require hierarchical WSNs. For example, in the interleaved hop-by-hop authentication scheme proposed by Zhu et al. [10], every report is generated within a cluster. In the group-based filtering scheme proposed by Yu et al. [13], nodes on the field should be divided into some groups at the initial stage, with the consideration of their geographical locations. They also do not consider node density loss, so that some events may not be reported as time goes by. Thus, they also need to consider node density loss. In fact, it could be a more critical problem; in some cases, regrouping needs to be performed on a network-wide scale.

6. Conclusion

In this letter, we propose a node density loss resilient report generation method for SEF-based WSNs. By allowing 1-hop neighbors of each CoS to relay tuples from orphan nodes, the probability of successful report generation could be enhanced by 24%, compared to the original SEF. The effectiveness of the method was shown with the simulation results.

References

[1] Z. Yu and Y. Guan, “A dynamic En-route Filtering Scheme for Data Reporting in Wireless Sensor Networks,” IEEE/ACM Trans. Netw., vol.18, no.1, pp.150–163, Feb. 2010.
[2] S.M. Nam and T.H. Cho, “A Fuzzy Rule-Based Path Configuration Method for LEAP in Sensor Networks,” Ad Hoc Netw., vol.31, no.8, pp.63–79, 2015.
[3] I. Torni and J.A. McCann, “A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols,” IEEE Internet of Things Journal, vol.4, no.6, pp.1910–1923, Dec. 2017.
[4] F. Ye, H. Liao, S. Lu, and L. Zhang, “Statistical En-route Filtering of Injected False Data in Sensor Networks,” IEEE J. Sel. Areas Commun., vol.23, no.4, pp.839–850, April 2005.
[5] X. Yang, J. Lin, P. Moulema, W. Yu, X. Fu, and W. Zhao, “A Novel En-route Filtering Scheme against False Data Injection Attacks in cyber-physical networked systems,” IEEE Trans. Comput., vol.64, no.1, pp.4–18, Jan. 2015.
[6] A. Al-Riyami, N. Zhang, and J. Keane, “An Adaptive early Node Compromise Detection Scheme for Hierarchical WSNs,” IEEE Access, vol.4, pp.4183–4206, Aug. 2016.
[7] W. Dong, J. Yu, J. Wang, X. Zhang, Y. Gao, C. Chen, and J. Bu, “Accurate and Robust Time Reconstruction for Deployed Sensor Networks,” IEEE/ACM Trans. Netw., vol.24, no.4, pp.2372–2385, Aug. 2016.
[8] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen, “BECAN: A Bandwidth-Efficient Cooperative Authentication scheme for Filtering Injected False Data in Wireless Sensor Networks,” IEEE Trans. Parallel Distrib. Syst., vol.23, no.1, pp.32–43, Jan. 2012.
[9] I. Banerjee, P. Chanak, H. Rahmaner, and T. Samanta, “Effective Fault Detection and Routing Scheme for Wireless Sensor Networks,” Comput. & Elect. Eng., vol.40, no.2, pp.291–306, 2014.
[10] 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. IEEE Symp. Security and Privacy, pp.259–271, 2004.
[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,” J. Info. Sci. and Eng., vol.25, no.4, pp.1163–1175, 2009.
[12] J.M. Kim, Y.S. Han, H.Y. Lee, and T.H. Cho, “Path renewal method in filtering based wireless sensor networks,” Sensors, vol.11, no.2, pp.1396–1404, 2011.
[13] L. Yu and J.Z. Li, “Grouping-based resilient statistical en-route filtering for sensor networks,” Proc. IEEE Comp. Commun. Societies, pp.1782–1790, 2009.
[14] C. Yi, G. Yang, H. Dai, L. Liu, and Y. Chen, “Efficient Geographical Information-Based En-route Filtering Scheme in Wireless Sensor Networks,” KSII Trans. Internet Inf. Syst., vol.12, no.9, pp.4183–4204, 2018.
[15] W. Elsayed, M. Elhoseny, S. Sabbeh, and A. Riad, “Self-maintenance model for wireless sensor networks,” Comput. & Elect. Eng., vol.70, pp.799–812, 2018.