Kalpa Publications in Computing
Volume 2, 2017, Pages 151–157
ICRISET2017. International Conference on Research and Innovations in Science, Engineering &Technology. Selected Papers in Computing

A Compromised Cluster Detection Method in Dynamic En-route Filtering Utilizing False Reports of Wireless Sensor Networks

Jung Sub Ahn[1*], Dong Jin Park[2] and Tae Ho Cho[2†]
[1] College of Information and Communication Engineering, Sungkyunkwan University, Suwon, Republic of Korea
[2] College of Software, Sungkyunkwan University, Suwon, Republic of Korea
sc4217@skku.edu, jin1307e@skku.edu, thcho@skku.edu

Abstract

Sensor nodes of wireless sensor networks are deployed in open environments. Hence, an attacker can easily compromise the node. An attacker can compromise a node to generate false reports and inject them into the network. This causes unnecessary energy consumption associated with the process of transmitting false alarm messages and false data reports to the system. If the attacker keeps repeatedly attacking, the attacks will cause problems such as a reduction in the entire network life or disabling of the networks. Yu and Guan proposed a dynamic en-route filtering scheme to detect and drop these false reports before they reach the base station. In dynamic en-route filtering, the energy waste of the intermediate nodes occurs until it is detected early. In this paper, we propose a method to save the energy of the intermediate nodes by searching for the compromised node and blocking the reports generated at that node. When verifying a false report at the verification node, it can know its report information. The base station is able to find the cluster of compromised nodes using that information. In particular, by knowing the location of the node that has been compromised, we can block false alarms and energy losses by blocking reports generated in that cluster.

1 Introduction

A wireless sensor network (WSN) is composed of many sensor nodes for detecting events and a base station (BS) for collecting event data, and is used hospitals, military bases, and industrial buildings (F. AkyildizW., 2002) (J. YickB., 2008) (H. ParkT.H., 2012). When the sensor node detects an event, it sends an event message to the cluster head (CH), and the CH node generates a report

[*] First author
[†] Corresponding author

based on the event message and transmits to the BS using multihop (MansouriDjamel,, 2013) (ZhuSencun,, 2004). Sensor nodes deployed in the target field have limited processing ability and battery power. They are vulnerable to various security attacks such as false report injection attacks because they are deployed in open environments. Therefore, research on security schemes associated with limited node environments is currently very important (F. YeH., 2005) (LuRongxing,, 2012) (LiFeng,, 2006). An attacker can compromise a sensor node, use the confidential information contained in the node to generate event data in the form of a report and inject it into the network to perform a false report injection attack. False report injection attacks cause false alarms in the system and unnecessary energy consumption in the intermediate nodes. To solve this problem, Yu and Guan proposed dynamic en-route filtering (DEF) (YuZhen,, 2010). DEF is composed of three phases: a key pre-deployment phase, a key post-deployment phase and a report filtering phase. DEF detects false reports using two keys. DEF has a high filtering rate, but nodes will continue to consume excess energy until false reports are verified to be false.

In this paper, we propose a compromised cluster detection method in dynamic en-route filtering utilizing false reports to find the location of corrupted nodes in the BS and to block reports generated from the nodes. The proposed method sends a new verification result report to the BS using the report information at the node that verified the false report. The BS uses the verification result report in order to know the generated location of the false report and the compromised keys, including the authentication key and secret key. When the same verification result report is received more times than a predetermined threshold, the BS transmits a message blocking the report. If the CH node receives that message, it can't generate a report. As a result, the CH node prevents unnecessary energy consumption by the nodes. We use modeling and simulation of a WSN to demonstrate the proposed scheme. Experimental results show that the proposed scheme saves energy by at least 6% and up to 65%

The remainder of the paper is organized as follows: Section 2 describes false report injection attacks and DEF. Section 3 introduces detailed procedure for the proposed method. Section 4 reviews the analysis of the experiment results. Finally, Section 5 includes the conclusion and future work.

2 Related Works

2.1 False Report Injection Attack

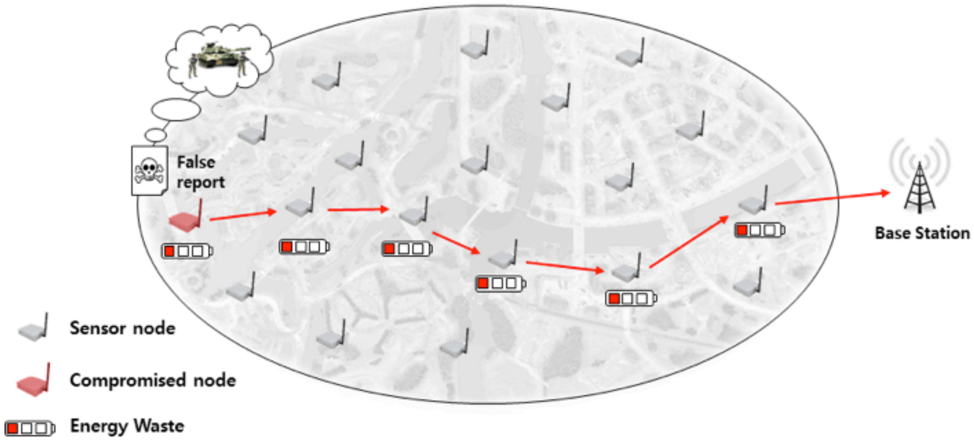

Figure 1: Overview of false report injection attack

Figure 1 shows an attacker compromising the node and obtaining secret information from the node in order to generate a false report and inject it into the network. False Report Injection attacks can drain the power from all nodes through repetitive attacks (YangHao,, 2004). This problem reduces the network lifetime or disables the network. In addition, the BS informs the user of the wrong information and causes confusion and time loss because false reports are a result of false event information. Other security attacks include sinkhole attacks and selective forwarding attacks. Sinkhole attacks occur in a range type, and selective forwarding attacks only compromise some nodes in the path (WangYong,, 2006). BS neighbor nodes are most affected by false report injection attacks because of all the nodes on the routing path to the BS through the BS neighbor nodes. If BS neighbor nodes are depleted of energy, the network is disabled.

2.2 Dynamic En-route Filtering Scheme

A dynamic en-route filtering scheme prevents false report injection attacks, which are one type of application layer attack that may occur in WSN. This scheme distributes the authentication and secret keys to each node before the nodes are deployed, and the member nodes in each cluster encrypt the authentication key and send it to the CH. The CH generates a message using the authentication key and forwards the message to the next node according to the routing path. After receiving the message, the nodes verify the message and load the authentication key or message into memory. The stored authentication key is used to verify the event report.

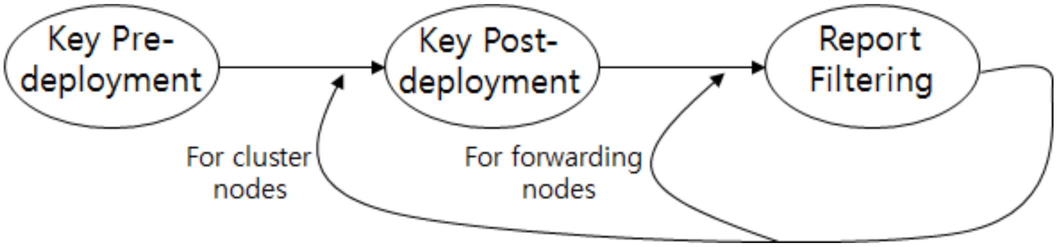

Figure 2: 3-phase procedure for DEF

Figure 2 shows the 3 phases of the DEF procedure. The key pre-deployment phase is executed only once at the BS before the sensor nodes are deployed to the target field. In this phase, a distinct seed key is preloaded on each node, and then authentication keys are generated using a hash chain. The authentication key is calculated as follows:

$$k^{vi}{}_{m\text{-}1} = h(k^{vi}{}_{m})$$
$$k^{vi}{}_{m\text{-}2} = h(k^{vi}{}_{m\text{-}1}) = h^{2}(k^{vi}{}_{m})$$
$$\dots$$
$$k^{vi}{}_{1} = h^{m\text{-}1}(k^{vi}{}_{m}).$$

Here, v_i refers to the index of the node, and $k^{vi}{}_{l}$ is the first key used. Each node has l + 1 secret keys. l is randomly selected in the y-key pool of v size and the remaining key is randomly selected in the z-key pool of w size. There is a node with at least one other z key in the cluster. The key post-deployment phase is performed for verification of generated false reports from the compromised node. In this phase, each node generates an encrypted authentication message and sends it to the CH node. The authentication message is as follows:

$$Auth(v_i) = \{v_i, j_i, id(y_1{}^{vi}), \{id(y_1{}^{vi}), k_j{}^{vi}\},$$
$$\dots, id(y_l{}^{vi}), \{id(y_l{}^{vi}), k_{ji}{}^{v1}\}y_l{}^{vi},$$

$$id(z^{vi}), (id(z^{vi}), k_{ji}^{vi})z^{vi}\},$$

j_i is the index of the current authentication key. $id(y_1^{vi})$ is the index of y_1^{vi} in the global key pool. $\{.\}\ y_l^{vi}$ refers to the encryption operation using y_l^{vi}. CH collects the authentication message from the nodes belonging to the cluster and generates K(n).

$$\mathrm{K(n)} = \{\mathrm{Auth}(v_1),\ldots,\mathrm{Auth}(v_n)\}$$

CH selects $q(q> 1)$ of the transfer threshold value from neighbor nodes and transfers K(n). By transmitting to q forwarding nodes, the report can be switched to another node when the neighboring node is compromised. When the forwarding node receives K(n), it performs as follows:

1) It verifies that K(n) has at least t distinct z-keyed indexes. If not, K(n) is judged to have been falsified and discarded.
2) If it determines that the index of the secret key in K(n) is the same, the corresponding message is decrypted and the authentication key is stored in the memory. If there is no index, K(n) is discarded.
3) K(n) is transmitted to q neighbor nodes. If the time to live (TTL) of K(n) is zero, K(n) is discarded. Otherwise, K (n) is transmitted to the next nodes belonging to the cluster.

The above operation is repeated until K(n) reaches the BS or TTL becomes zero. The y-key and z-key are used to decrypt K(n) at the forwarding node, but for different purposes. In the report filtering phase, the event reporting nodes generate a message authentication code (MAC) and send it to the CH. After receiving the MAC, the CH generates a report including the MACs by a preset threshold value k and sends it to the BS. The intermediate node can detect a false report by verifying the MAC using the authentication key when the report including the same MAC received. This process is repeated until the report arrives at the BS or is discarded.

3 Proposed Scheme

3.1 Assumptions

It is assumed that the network is divided into clusters and each cluster consists of nine member nodes and a cluster head. The BS stores cluster ID and location information. The report does not disappear in the middle. The BS has a y-key pool and z-key pool that are a set of keys distributed to each node. Any report can be verified by the BS. It is assumed that the forwarding nodes can verify the report. The forwarding node can generate a verification report through false reports. The verification report is sent to the BS by the forwarding node. The attacker repeatedly performs a false report injection attack on the same node. A false report injection attack occurs at least two hops from the BS and occurs randomly. The CH nodes are not compromised.

3.2 Detailed Procedure

Figure 3 shows an overview of the proposed scheme. After the key distribution phase, a false event occurs and the CH generates a false report. False reports continue to be forwarded until a forwarding node with the same authentication key is found. If the forwarding node verifies a false report, it drops the report and generates the following verification report:

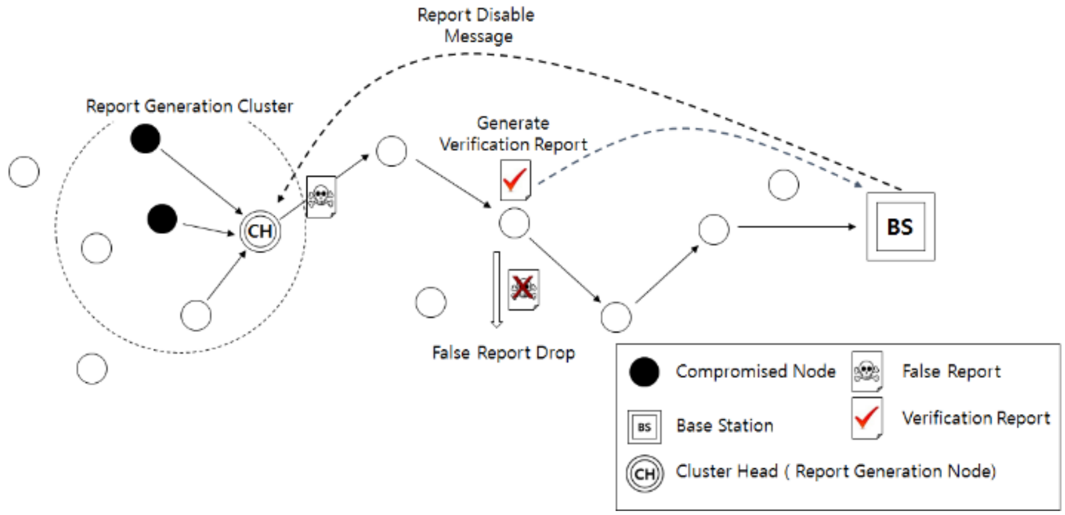

Figure 3: Overview of the proposed scheme

$$VR = \{ Source_{ID} \,||\, id(y_l^{vi}) \,||\, id(Auth_N) \}y_l^{vi}.$$

$Source_{ID}$ is the ID of the CH where the report was generated. The forwarding node generates encrypted VR with the secret key and transmits it to the BS. Encryption prevents capture of the intermediate report. The BS can decrypt the VR using the y_l^{vi} secret key and identify the location of the compromised node using $Source_{ID}$ and $id(y_l^{vi})$. The secret key used above is never redistributed after the initial deployment. If redistribution is completed, the BS also updates the redistributed secret key. The BS stores $id(Auth_N)$. If the BS receives the same messages, it determines that the corresponding authentication key is exposed and performs the key redistribution of the node having the corresponding authentication key. The content of key redistribution is not covered in this paper. The BS uses $Source_{ID}$ and $id(y_l^{vi})$ to encrypt the report-generation-disable message with the secret key. When the CH receives the report-generation-disable message, it does not generate a report even if an event occurs.

4 Performance Analysis

4.1 Experimental Environments

The experimental environment was composed as follows. The total number of nodes arranged in the sensor field is 1,000; 100 CH nodes and 900 member nodes. Each node is placed directly on the field by the user. The size of the sensor field is 1,000 x 1,000 m^2. The nodes consume 16.25 µJ per byte, 12.5 µJ per byte when transmitting and receiving data respectively, 15µJ for MAC generating and 75µJ for report intermediate verification [5]. The size of the report generated by the CH is assumed to be 30 bytes and one MAC is assumed to be 1 byte in size.

4.2 Experimental Results

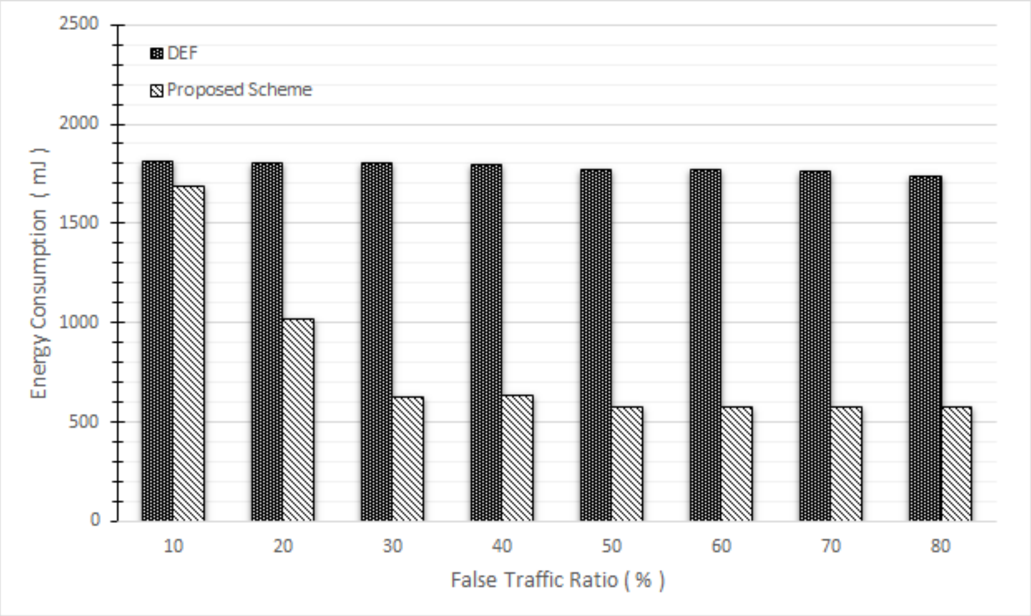

Figure 4: Energy consumption versus FTR

The energy consumption rate was compared with DEF and the proposed scheme. Figure 4 shows the energy consumption of the proposed scheme versus FTR. When the attack ratio is low, there is little difference in the performance compared with the existing method. However, the higher the attack ratio, the more energy that is saved. The reason is that the proposed scheme prevents the load on the same node from getting larger as the attack ratio increases. Also, the amount of false traffic reports and the amount of drop are proportional. This indicates an energy efficiency of 6% on 10% FTR, 43% on 20 FTR and 65% above 40% FTR. The large difference between 10% and 30% is due to the threshold value. If WSN has a low attack ratio, the report generation disable message is not sent to the CH because the attack count is lower than the threshold value.

5 Conclusion and Future Work

False report attacks in a WSN cause false alarms and unnecessary energy consumption. To prevent these problems, Yu and Guan proposed a dynamic filter scheme. However, in that scheme, when an attacker continues to execute a false report injection attack, the energy of the nodes is consumed. In order to solve this problem, we propose a compromised cluster detection method with dynamic en-route filtering that utilizes false reports of wireless sensor networks. The BS can know the location where the false report injection attack occurred through a verification report. Furthermore, searching can identify the CH that generated the false report and blocked report generation. Searching prevents unnecessary energy consumption by forwarding nodes. The experimental results confirm that our method consumes less energy than the DEF. Uncompromised nodes in the cluster may become unusable. In future work, we will study a scheme to block only the compromised node through collaborative verification of neighbor nodes in the cluster.

Acknowledgment

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. NRF-2015R1D1A1A01059484)

References

F. Akyildiz, W. S. (2002). A survey on sensor networks. *Communications Magazine vol. 40*, 102-114. Retrieved from Templates for proceedings: https://easychair.org/proceedings/template.cgi?a=12732737

F. Ye, H. L. (2005). Statistical en-route filtering of injected false data in sensor networks. *Selected Areas in Communications*, 839-850.

H. Park, T. C. (2012). Partial path selection method in each subregion for routing path optimization in SEF based sensor networks. *Journal of Korean Institute of Intelligent Systems 22(1)*, 108-113.

J. Yick, B. M. (2008). Wireless sensor network survey. *Computer Networks, vol. 52*, 2292-2330.

Li, F. a. (2006). A probabilistic voting-based filtering scheme in wireless sensor networks. *Proceedings of the 2006 international conference on Wireless communications and mobile computing. ACM*.

Lu, R. e. (2012). BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks. *IEEE transactions on parallel and distributed systems*.

Mansouri, D. e. (2013). Detecting DoS attacks in WSN based on clustering technique. *IEEE Wireless Communications and Networking Conference.*

Wang, Y. G. (2006). A survey of security issues in wireless sensor networks.

Yang, H. a. (2004). Commutative cipher based en-route filtering in wireless sensor networks. *Vehicular Technology Conference*.

Yu, Z. a. (2010). A dynamic en-route filtering scheme for data reporting in wireless sensor networks. *EEE/ACM Transactions on Networking*.

Zhu, S. e. (2004). An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks. *Security and privacy IEEE symposium*.