PREVENTION METHOD OF FALSE REPORT GENERATION IN CLUSTER HEADS FOR DYNAMIC EN-ROUTE FILTERING OF WIRELESS SENSOR NETWORKS

Jung-Sub Ahn[1] and Tae-Ho Cho[2]

[1]College of Information and Communication Engineering, Sungkyunkwan University, Suwon 16419, Republic of Korea
[2]College of Software Platform, Sungkyunkwan University, Suwon 16419, Republic of Korea

ABSTRACT

Wireless sensor networks collect data through collaborative communication between sensor nodes. 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 into the network. This causes unnecessary energy consumption in the process of transmitting false alarm messages and false data reports to the system. If the attacker keeps repeatedly attacking thereby causing problems such as reduction in the entire network life or disabling the networks. Yu and Guan proposed a dynamic en-route filtering scheme to detect and drop these false reports before reaching to the Base station. In the 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 report information. The base station is able to find the cluster of compromised nodes using that information. In particular, the base station can know the location of the node that has been compromised, we can block false alarms and energy losses by blocking reports generated in that cluster.

KEYWORDS

Network Simulation, Wireless Sensor Network, Dynamic en-route filtering, False Report Injection Attack.

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 applied to various fields such as hospitals, military, and industrial [1-3]. When the sensor node detects an event, it sends an event message to the cluster head (CH), and the CH node generates a report based on the event message and transmits to BS using multihop [4-5]. Sensor nodes deployed in the target field have limited processing ability and battery power. It is vulnerable to various security attacks such as false report injection attacks because it is deployed in open environments. Therefore, research on security scheme considering limited node environment is actively studied today [6-8]. The attacker can compromise the sensor node and 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 false report injection attack. False report injection attacks cause false alarms in the system and unnecessary energy consumption of intermediate nodes. To solve this problem, Yu and Guan proposed Dynamic en-route filtering (DEF) [9]. DEF is composed of three phases as key pre-

DOI:10.5121/ijcsit.2017.9305

deployment phase, key post-deployment phase and report filtering phase. DEF detects false reports using two keys. DEF have high filtering rate, but it continues to consume the energy of the nodes until verification of false reports.

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. BS uses the verification result report to know the generated location of the false report and the compromised keys including authentication key and secret key. When the same verification result report is received more than predetermined threshold, the BS transmits a message blocking the report. If the CH node received that message, it can't generate any report. As a result, it prevents unnecessary energy consumption by the nodes. We have modelling and simulation of WSN to prove the proposed scheme. Experimental results show that the proposed scheme saves energy by at least 6% and up to 29%.

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

2. RELATED WORKS

2.1. FALSE REPORT INJECTION ATTACK

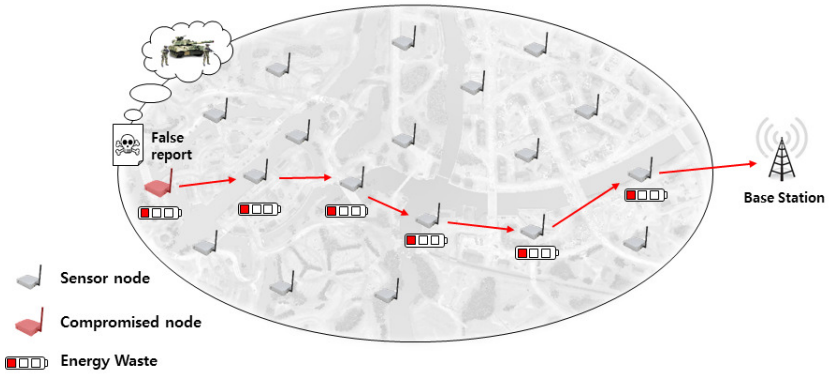

Figure 1.Overview of False report injection attack

Figure 1 shows an attacker compromising the node, and obtaining the secret information of the node, to generate a false report and inject it into the networks. False Report Injection attacks can exhaust all the energy of the all nodes in repetitive attacks. This problem reduces the networks lifetime or disables the networks [10-12]. In addition, The BS informs the user of the wrong information and causes confusion and time loss. Because false report has the 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 [13-16]. BS neighbor nodes are most affected by false report injection attacks because of all 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

Dynamic en-route filtering scheme prevents false report injection attack which is one of application layer attacks 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 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.

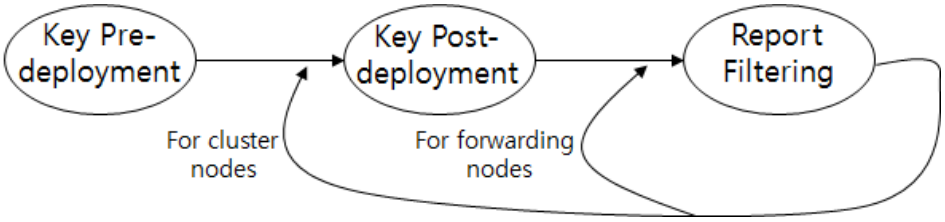

Figure 2.3-phases procedure of DEF

Figure 2 shows the 3-phases procedure of DEF. The key pre-deployment phase is executed only once at the BS when 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:

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

vi means the index of the node, and k^{vi}_{1} is first used key. Each node has l + 1 secret keys. l is randomly to 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 a cluster. The key post-deployment phase is performed for verification of generated false reports from compromised node. In this phase, each node generates an encrypted authentication message and sends to the CH node. The authentication message is as follows:

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

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

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

CH selects q(q> 1) of 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 checks 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, discard K(n).
3) K(n) is transmitted to q neighbor nodes. If 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 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 to the CH. After receiving the MAC, the CH generates a report including the MACs by a preset threshold value k and sends to the BS. The report can detect the false report by verifying the MAC using the authentication key distributed at the post-deployment phase at verification node when report transmission to the BS is performed. This process is repeated until the report arrives at the BS or discarded.

3. PROPOSED SCHEME

3.1. ASSUMPTIONS

It is assumed that network is divides into clusters and each cluster consists of nine member nodes and a cluster head. Since sensor nodes are deployed by the user, BS stores cluster ID and location information. The report does not disappear during transmission. BS has 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. The forwarding node can generate a verification report utilizing false reports. The verification report is sent to the BS by the forwarding node verifying the false report. 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. CH nodes deployed in a specific place are not compromised.

3.2 DETAILED PROCEDURE

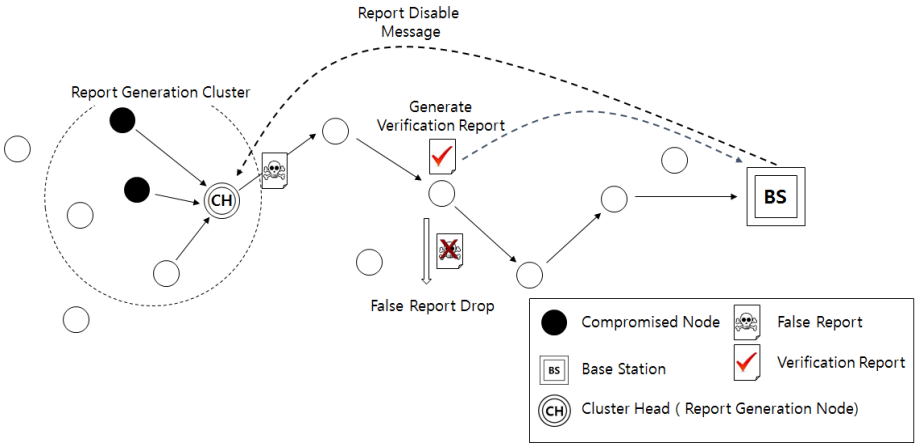

Figure 3. Overview of proposed scheme

Figure 3 shows overall 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:

$$VR = \{ Source_{ID} \| id(y_l^{vi}) \| id(Auth_N) \} y_1^{vi}$$

$Source_{ID}$ is the ID of the CH where the report was generated. The forwarding node generates encrypted VR with the secret key and transmit to the BS. The reason for the encryption is to prevent capturing the report in the intermediate. The BS can decrypt the VR using the y_l^{vi} secret key and identify the location of the compromised node using the $Source_{ID}$ and id(y_l^{vi}). Because the secret key used above was never redistributed after the initial deployment. If redistribution is done, the BS also updates the redistributed secret key. The BS stores the id($Auth_N$). If BS receive 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 the $Source_{ID}$ and the 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 ENVIRONMENT

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 sensor field is 1,000 x 1,000 m2. Each node consists of two y-keys and one z-key key. The nodes consume 16.25μJ/byte, 12.5μJ/byte when transmitting and receiving data respectively, 15μJ for MAC generating, 70 μJ for report generating and 75μJ for report intermediate verification [18]. When generating a VR report that includes the encryption process, it consumes 105μJ of energy. The size of the report generated by the CH is assumed to be 30 bytes and one MAC is assumed to be 1 byte. False Report Injection attacks occur 1000 times in random places.

4.2 EXPERIMENTAL RESULTS

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 performance compared with the existing method. However, the higher the attack ratio, the more energy 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. That shows Energy efficiency of 6% on 10% FTR, 20% on 20 FTR and 29% after 80%. The large difference between 10% and 30% is due to the threshold value. If WSN has low attack ratio, the report generation disable message is not sent to the CH because the attack count is lower than the threshold value. Both DEF and Proposed scheme detect more than 80% false reports. If the attacker continuously attacks through the same node, the proposed scheme will save the maximum energy.

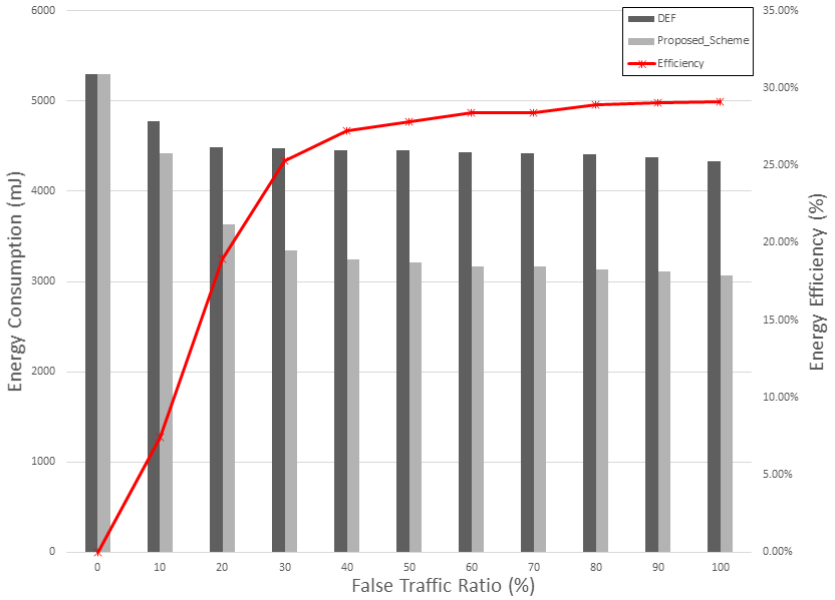

Figure 4. Energy consumption versus FTR

Figure 5 shows the network lifetime according to FTR. It represents the lifetime of the network when the attacker continuously executes the attacks. When the FTR is 100%, the lifetime improvement performance is 22% in the DEF scheme but the lifetime improvement performance is 72% in the proposed scheme.

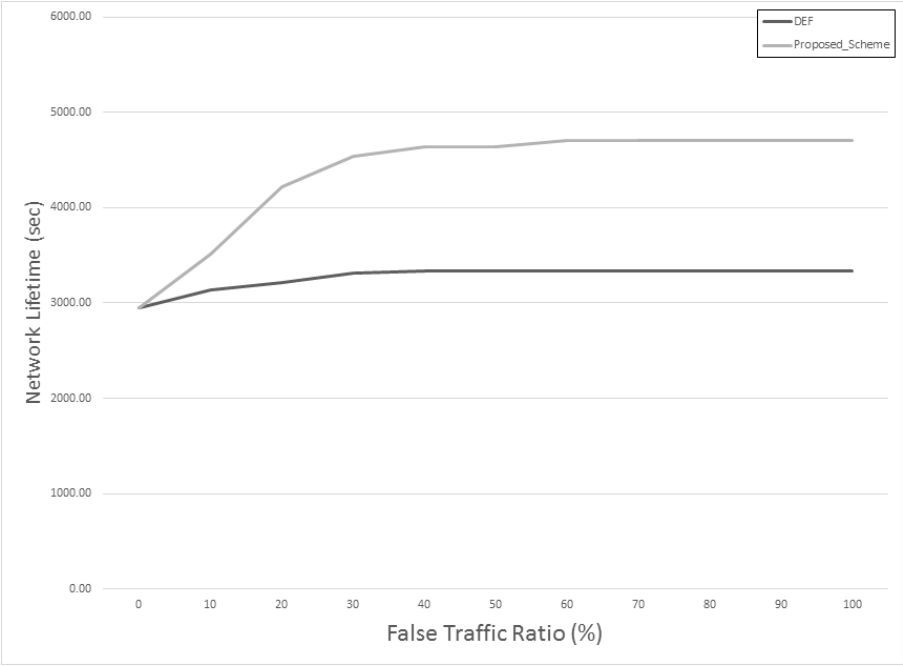

Figure 5 Networks Lifetime versus FTR

5. CONCLUSION AND FUTURE WORK

False report attacks in WSN cause false alarms and unnecessary energy consumption. To prevent this 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 nodes is consumed. In order to solve this problem, we propose a compromised cluster detection method in dynamic en-route filtering utilizing false reports of wireless sensor networks. The BS can know the location where the false report injection attack occurred through the verification report. Furthermore, searching the CH that generated the false report and blocking the report generation. It prevents unnecessary energy consumption of forwarding nodes. The Experimental results confirm that our method saves 29% energy than the DEF. But, uncompromised nodes in the cluster also become unusable. In the future works, we will study a scheme that can block only the compromised node through collaborative verification of neighbor nodes in the cluster.

ACKNOWLEDGEMENTS

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

[1] Reejamol, K. J., and P. Dhanya Raj. "Hole handling techniques in wireless sensor networks: A survey." Computational Intelligence and Computing Research (ICCIC), 2016 IEEE International Conference on. IEEE, (2016)

[2] Nam, Su Man, and Tae Ho Cho. "A fuzzy rule-based path configuration method for LEAP in sensor networks." Ad Hoc Networks 31 (2015)

[3] H. Park and T. H. Cho. 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), pp. 108-113. (2012)

[4] Mansouri, Djamel, et al. "Detecting DoS attacks in WSN based on clustering technique." 2013 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, (2013)

[5] Winkler, Thomas, and Bernhard Rinner. "Security and privacy protection in visual sensor networks: A survey." ACM Computing Surveys (CSUR) 47.1 (2014)

[6] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on, vol. 23, pp. 839-850, (2005)

[7] Lu, Rongxing, et al. "BECAN: a bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks." IEEE transactions on parallel and distributed systems 23.1 (2012)

[8] Li, Feng, and Jie Wu. "A probabilistic voting-based filtering scheme in wireless sensor networks." Proceedings of the 2006 international conference on Wireless communications and mobile computing. ACM, (2006)

[9] Yu, Zhen, and Yong Guan. "A dynamic en-route filtering scheme for data reporting in wireless sensor networks." IEEE/ACM Transactions on Networking (ToN) 18.1 (2010)

[10] Yang, Hao, and Songwu Lu. "Commutative cipher based en-route filtering in wireless sensor networks." Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. Vol. 2. IEEE, (2004)

[11] Gupta, Pallavi, Vinay Prakash, and Preetam Suman. "Noticeable key points and issues of sensor deployment for large area Wireless Sensor Network: A survey." System Modeling & Advancement in Research Trends (SMART), International Conference. IEEE, (2016).

[12] Mohammed, Fihri, et al. "Investigating the impact of black-hole attack on hierarchical protocols and direct transmission in WSN." Proceedings of the International Conference on Internet of things and Cloud Computing. ACM, (2016)

[13] Joshi, Jetendra, et al. "SEED: Secure and energy efficient data transmission in Wireless Sensor Networks." Information and Communication Technology (ICoICT), 2016 4th International Conference on. IEEE, (2016)
[14] Saghar, Kashif, et al. "RAEED: A formally verified solution to resolve sinkhole attack in Wireless Sensor Network." Applied Sciences and Technology (IBCAST), 2016 13th International Bhurban Conference on. IEEE, (2016)
[15] Wang, Ding, and Ping Wang. "Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks." Ad Hoc Networks 20 (2014)
[16] Kumar, Vikash, Anshu Jain, and P. N. Barwal. "Wireless sensor networks: security issues, challenges and solutions." International Journal of Information and Computation Technology (IJICT) 4.8 (2014)
[17] Hwang, Ren Junn, and Yan Zhi Huang. "Secure Data Collection Scheme for Wireless Sensor Networks." Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on. IEEE, (2017)

AUTHORS

Jung Sub Ahn received the B.S. degree in computer engineering from Kyunil Universityt in 2016 and now doing M.S. degree in Department of Electrical and Computer Engineering from Sungkyunkwan University.

Tea Ho Cho received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University, Repulic of Korea, and the University of Alabama, USA, respectively. He is currently a Professor in the College of Information and Communication Engineering, Sungkyunkwan University, Korea.