Wireless Sensor Network, 2013, 5, 33-40
http://dx.doi.org/10.4236/wsn.2013.53005 Published Online March 2013 (http://www.scirp.org/journal/wsn)

A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks*

Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho
College of Information and Communication Engineering, Sungkyunkwan University, Suwon, South Korea
Email: hmchoi@ece.skku.ac.kr, smnam@ece.skku.ac.kr, taecho@ece.skku.ac.kr

Received May 16, 2012; revised June 14, 2012; accepted June 25, 2012

ABSTRACT

Wireless sensor networks (WSNs) consist of a large number of sensor nodes that monitor the environment and a few base stations that collect the sensor readings. Individual sensor nodes are subject to compromised security because they may be deployed in hostile environments and each sensor node communicates wirelessly. An adversary can inject false reports into the networks via compromised nodes. Furthermore, an adversary can create a wormhole by directly linking two compromised nodes or using out-of-band channels. If these two kinds of attacks occur simultaneously in a network, existing methods cannot defend against them adequately. We thus propose a secure routing method for detecting false report injections and wormhole attacks in wireless sensor networks. The proposed method uses ACK messages for detecting wormholes and is based on a statistical en-route filtering (SEF) scheme for detecting false reports. Simulation results show that the proposed method reduces energy consumption by up to 20% and provide greater network security.

Keywords: Wireless Sensor Network; Security; Statistical En-Route; Wormhole; Secure Routing

1. Introduction

Recent advances in micro electro mechanical systems and digital electronic and wireless communication technologies have enabled the development of low-cost, multi-functional sensor nodes [1]. Wireless sensor networks (WSNs) have long been used in many types of computing systems. A WSN consists of a large number of sensor nodes that monitor the environment and one or more base stations that collect the sensor readings [2]. In many applications such as military surveillance, sensor nodes are deployed in open, large-scale, and even hostile environments and potential issues range from accidental node failure to intentional tampering. Due to their relatively small sizes and unattended operations, sensor nodes are at high risk of being physically captured and having their security compromised [3]. Additionally, the power of the sensor nodes is limited and non-replaceable [4-6]. The security and energy efficiency of sensor nodes are thus extremely important in WSNs.

If sensor nodes are physically captured and compromised, security information such as network keys can be revealed to the adversary. The adversaries can then inject false reports into sensor network via the compromised nodes. These injected false reports can not only result in false alarms but also in quick usage of the limited amount of energy in the sensor nodes [7]. Several researchers have proposed mechanisms to combat attack by injection of false reports [7-14]. The statistical enrouting filtering scheme (SEF) was proposed by Fan Ye *et al.* [7] to detect and drop injected false reports during the forwarding process.

Another type of wireless sensor network attack is a wormhole attack, which is made up of two adversaries and a wormhole tunnel. The two adversaries communicate with each other through the wormhole tunnel, which is a direct and dedicated channel using a wired link or additional RF transceivers on an out-of-bound channel available only to the attacker. A wormhole attack can alter or drop messages as well as eavesdrop. To combat this type of attack, a few different countermeasures have been proposed [2,4-6,9-13,15-18]; a simple lightweight protocol called LITEWORP is one of these. LITEWORP uses a secure two-hop neighbor discovery and local monitoring of control traffic to detect nodes involved in a wormhole attack [17].

In this paper, we propose a secure routing method for detecting multiple attacks in wireless sensor networks, particularly false report injections and wormholes. Previous research has focused on single attacks (e.g., either false report injections or wormholes); there are currently no reports of research in cases in which the two types of attacks occur in a network at the same time. To defend

*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. 2012-0002475).

against multiple attacks, it is possible to simply implement two countermeasures (*i.e.*, SEF and LITEWORP) together; however, because each individual countermeasure does not consider the use of the other, this approach can result in wasteful energy consumption. In the proposed method, we consider both false report injections and wormhole attacks, leading to prevention of additional energy consumption. Simulation results show that the proposed method can save up to 20% of total energy consumption compared to the simple combination of the SEF and LITEWORP, while simultaneously providing greater security.

The remainder of this paper is organized as follows: Section 2 briefly describes false report injections and wormhole attacks. Section 3 presents the problem statement, followed by a detailed description of the proposed method in Section 4. In Section 5, the performance of the proposed method is shown via simulation and discussed. Finally, Section 6 presents the conclusions of our study.

2. Background

2.1. Attack Models and Related Works

Figure 1 shows a schematic of a false report injection attack. A compromised node can inject false reports into the network, which both wastes the limited energy of the many nodes that deliver them to the base station (BS) and lead to false alarms. Several reports in the literature have proposed methods to combat false report injection attacks [7-14], including one by Fan Ye *et al.* [7], which used statistical en-route filtering (SEF) as a means to detect and drop injected false reports during the forwarding process. SEF carefully limits the amount of security information assigned to each node to prevent any single compromised node from disrupting the entire system. It relies on the collective decisions of multiple sensors for false report detection.

Figure 2 shows a schematic of a wormhole attack. The nodes X and Y are compromised and form a wormhole tunnel connected via wired link or a powerful out-of-bound RF channel. If node S wants to send a message to the BS, the routing path that includes the wormhole link has an advantage because its hop count is lower than that of the normal routing path. Messages routed via a wormhole node can also be dropped or altered; it is thus important that messages are not routed through wormhole nodes. To combat these wormhole attacks, Hu *et al.* [15] proposed geographical and temporal packet leashes as techniques for detecting wormholes. For the geographical leash, the sender appends its location and the sending time to the packet. Based on this information, the receiving node computes an upper bound on the distance to the sender. In the temporal leash, the sender appends the sending time to the packet and the receiving node computes a traveling distance for that packet using the difference between the packet sending and receiving times, assuming propagation at the speed of light. To implement these two schemes, the geographical leashes require that all nodes have a localization system such as GPS, and the temporal leashes require accurate local clocks and global time synchronization of all nodes in the network. For instance, Lingxuan *et al.* [16] proposed use of a directional antenna and ultrasonic signals to address both of these issues. However, the schemes mentioned above require that each sensor node be equipped with special devices. In LITEWORP [17], the neighboring nodes common between two nodes are chosen as guard nodes. The guard node monitors all traffic from both nodes and verifies that both nodes are free of malicious behavior; via this kind of monitoring, guard nodes can detect selective forwarding by a wormhole attack. Addi-

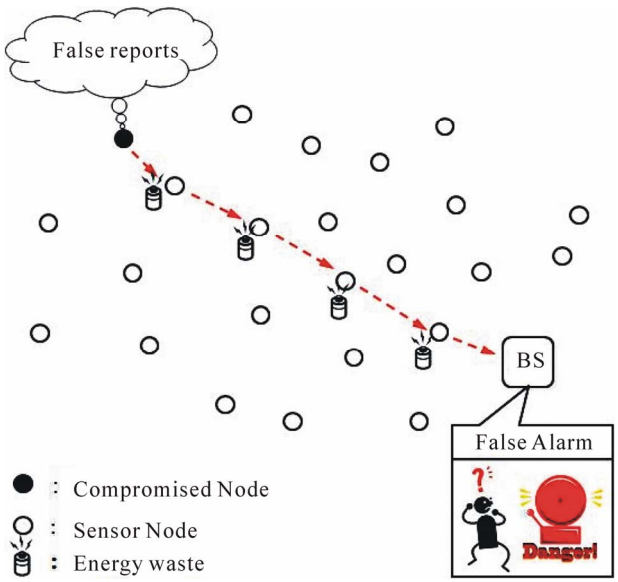


Figure 1. False reports injection attack model.

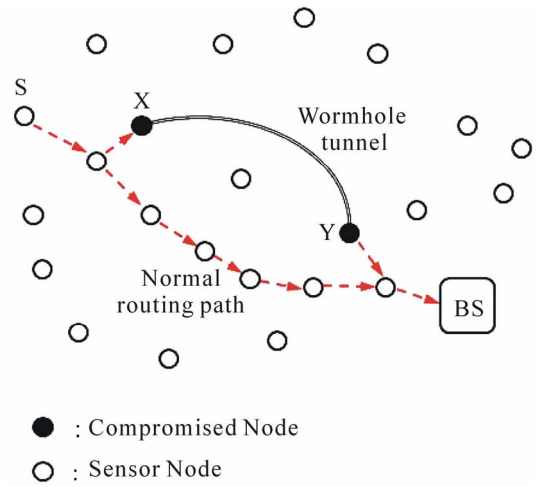


Figure 2. Wormhole attack model.

tionally, LITEWORP can operate without any special devices such as GPS. However, the guard nodes must monitor all traffic between the two nodes, resulting in increased processing overheads; as the guard nodes are not special nodes, such overhead invariably shortens their lifetime.

2.2. Statistical En-Route Filtering (SEF)

In this section, the main characteristics of the SEF scheme are described. Similar to the general en-route scheme, the SEF also involves two primary phases.

2.2.1. Key Assignment and Report Generation

The BS maintains a global key pool and divides it into n partitions. Each partition has m keys, and each key has a unique key index. Before the nodes are deployed, the user randomly selects k keys from one partition. The selected keys and the associated key indices are stored in the node before being deployed to the sensing field.

When an event occurs in the sensing field, all surrounding nodes detect the event and one of these nodes is elected as the CoS (Center of Stimulus) node. All detecting nodes generate a message authentication code (MAC) via one of their keys and send it to the CoS node along with the key index. The CoS node collects and classifies MACs based on the key partitions. Then the CoS node generates a report consisting of the event information, the MACs chosen from the distinct partitions and the key indices used to generate the MACs. The number of MACs included in each report is exactly same for all reports.

2.2.2. En-Route Filtering and BS Verification

As reports are forwarded via multiple hops, each intermediate forwarding node is able to verify them via the following operations:

1) Check the number of MACs in the reports. If the report has a different number of MACs, the node drops the report.

2) Check that the key indices in the attached report belong to distinct partitions. If the report has more than one key index from the same partition, the node drops the report.

3) If the node has a key that matches that of the report, the node generates a MAC with that key. If generated MAC and the corresponding MAC are different, the node drops the report.

4) If the report passes operations 1-3, the node sends it to the next hop.

The SEF can detect false reports en-route, but even if false reports arrive at the BS, the BS is able to verify every MAC because it has all the keys. If there are any mismatches, the BS discards the report.

2.3. Lightweight Countermeasure for Wormhole Attacks (LITEWORP)

LITEWORP [17] is a countermeasure for wormhole attacks that does not require specialized hardware such as GPS. In the LITEWORP scheme, neighboring nodes common between two nodes are chosen as their guard nodes, which monitor the incoming and outgoing traffic of their neighbors. LITEWORP is operated in two phases as follows:

- Wormhole Detection: Guard nodes monitor every incoming and outgoing data packet of its neighbor nodes. When a node sends a data packet to a receiving node, the guard nodes save the packet information in a watch buffer. The information includes the packet's identification and type, source, destination, and immediate sender and receiver. The guard nodes expect that the receiving node will forward the packet toward the base station unless the receiving node is itself the base station. Each entry in the watch buffer has a time threshold; the receiving node must send the packet onwards before the time threshold expires. A malicious activity counter is maintained by each guard node. The malicious activity counter is incremented for each neighbor node malicious event that is detected by the guard node.
- Isolation: When the malicious activity counter of node A crosses a threshold, the guard node revokes node A from its neighbor list, then sends alert messages to each neighbor node of node A indicating that node A is a suspected malicious node. When a neighbor node X of node A receives the alert, it stores the identity of the guard node in an alert buffer associated with A. When the number of alert messages regarding node A is over the threshold for node X, node X removes node A from its neighbor list. After isolation, node X does not receive or send any packet to a revoked node.

3. Problem Statement

Figure 3 shows a schematic of a combined false report injection and wormhole attack in a wireless sensor network. Generally, to combat this multiple attack, the network can use two countermeasures to deal separate with the false report injection attacks (*i.e.*, SEF) and wormhole attacks (*i.e.*, LITEWORP). These two countermeasures are not designed to work together, so a few problems occur as follows:

- Energy consumption: The two countermeasures, SEF and LITEWORP, may contain some duplication because they are not designed to work together. For example, for sensor networks using both countermeasures, the SEF attaches message authentication codes (MACs) to reports for detection of false reports, in-

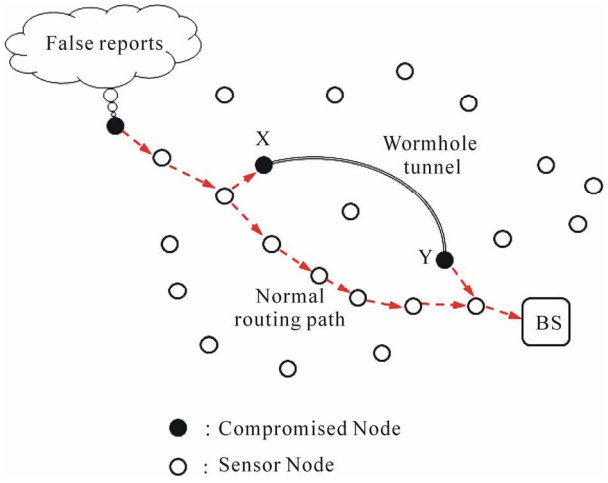


Figure 3. Schematic of two attacks occurring simultaneously in a sensor network.

creasing the size of each report. LITEWORP monitors all traffic in the network for wormhole attack detection, but the large reports generate high overhead and wasteful energy consumption.

– Security Level: The best way to combat false data injection attacks is to detect false reports at an early stage and drop it immediately. On the other hand, the key countermeasure to combat wormhole attacks is to find abnormal behavior in the network and drop nodes with these abnormal behaviors. One behavior considered abnormal is selective forwarding, the refusal of malicious nodes to forward certain reports, resulting in dropped messages not delivered to the base station. Because these two countermeasures do not communicate with each other, nodes enacting the false report injection countermeasure that drops false reports are considered by the wormhole countermeasure to be part of a wormhole.

To address these problems, we introduce improvements as follows:

– The false report detection method is based on SEF, but SEF drops false reports without any other operations such as a message to other nodes notifying the dropping of a false report. The proposed method sends the key index to the base station when false reports are dropped; this key index message can be used to notify the base station and other nodes of a dropped false report.
– All nodes that send reports must receive an ACK message from the node two hops down the line. The ACK messages are transmitted in a different way from the reports and include the node IDs on the routing path. A detailed description of these ACK messages is presented in the following section.

The analysis and simulation results described in Section 5 show the effectiveness of these improvements.

4. Proposed Method

4.1. System Model and Assumptions

We consider a large scale sensor network composed of a large number of small sensor nodes and a BS. We also assume that the reports are forwarded via multiple hops toward the BS. The sensor nodes are not moved after deployment. We also assume that the energy at the BS is unlimited. The sensor nodes are small and operated individually, so attacker can compromise a sensor node and inject false reports into the network with it. Moreover, the attacker can make a wormhole using a laptop or another similar device. We also assume that false report injection attacks occur with wormhole attacks in the network.

4.2. Overview

In this paper, we propose a secure routing method for detection of false report injection and wormhole attacks in wireless sensor networks. The proposed method is more efficient than one that uses two different methods simultaneously because the two different defense methods are not designed to work with each other. Additionally, it solves the problems that occur in previous solutions and provides efficient energy consumption. The proposed method is divided into three phases: Initialization, en-route filtering, and wormhole detection.

– Initialization: This phase is operating before node deployment and immediately after node deployment. Before node deployment, the global key pool is divided into n partitions in the BS. Each node stores k keys from one of these partitions. Then the nodes are deployed in the sensing field. After nodes are deployed, each node sends hello messages to recognize their neighbor nodes. The BS sends routing messages or operates other routing method to establish routing paths.
– En-route filtering: When an event occurs in the sensing field, the surrounding sensing nodes compete with each other to generate reports. The CoS node collects MACs from collaborating sensing nodes, attaches them to the report and forwards it towards the BS. Each intermediate forwarding node can verify the reports and drop false reports. When a false report is dropped, the intermediate node sends a drop message to the next node. If the intermediate node does not send a drop message, the previous node cannot receive an ACK message, causing the previous node to regard the intermediate node as a wormhole link. To prevent this problem, the intermediate nodes send drop messages to the next node when dropping false reports.
– Wormhole detection: All nodes sending reports wait for an ACK message. If nodes do not receive the

ACK messages, the next node is wormhole link. The ACK messages must be transmitted between nodes separated by two hops, but cannot be transmitted via the path that the original report is sent on. Since the ACK messages must be sent via other path, the time to live (TTL) is important. The TTL is the maximum number of hops used to transmit the ACK messages. If the ACK messages cannot be delivered to the previous node within the TTL hop limit, a wormhole is detected.

Overall, the focus of this method is on solving the conflict between the false report and wormhole detection mechanisms.

4.3. Initialization

Before any nodes are deployed, key assignment is based on the SEF scheme. The global key pool is divided into n non-overlapping partitions. Each partition has m keys, and each key has a corresponding key index. The user randomly selects one of the n partitions, and randomly chooses k keys from it. The chosen key and key indices are stored in the node. After all nodes store keys and key indices, the nodes are deployed into the sensing field. After deployment, all nodes immediately send hello messages to their neighbor nodes. All neighbor nodes replying to the hello message with their partition information. This partition information is used to determine alternative routing paths.

4.4. False Report Detection

When an event occurs in the sensing field, all surrounding nodes detect the event and one of these nodes is elected as the center of stimulus node. The CoS node cooperates with the surrounding nodes to generate a report. As a report is forwarded multiple hops, each intermediate forwarding node can verify it via the SEF scheme. If a node drops a false report, it sends a drop message to the next node. **Figure 4** shows that a compromised node sends a false report, but node B detects this false report and drops it. If node B does not notify the next node C of the false report drop event, node C never sends an ACK message to node A, leading node A to regard node B as a wormhole link. To prevent this problem, the proposed method sends a drop message after nodes drop false reports.

4.5. Wormhole Detection

Nodes that transmit reports wait for ACK messages after sending reports, but if the ACK messages do not arrive until after time t, the next node is regarded as a wormhole. Therefore the sending node eliminates the next node in the routing path, and then retransmits the reports to another node. **Figure 5** shows the report transmission process. The CoS node sends a report to the BS, and each intermediate node sends an ACK message to detect wormholes.

All nodes that transmit reports must wait for ACK messages. It means all nodes that receive reports have to reply with ACK messages. The ACK messages are used to detect wormhole links. **Figure 6** shows an example of replying with ACK messages. When node A sends a report to node B and node B sends it on to node C, node C replies with an ACK message to a neighbor node common to nodes B and C. Furthermore, nodes receiving ACK messages (node X) also send ACK messages to neighbor nodes common to node B and itself. This operation is

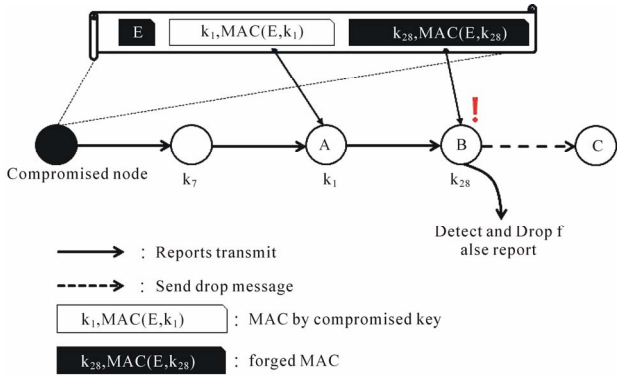


Figure 4. False report detection process.

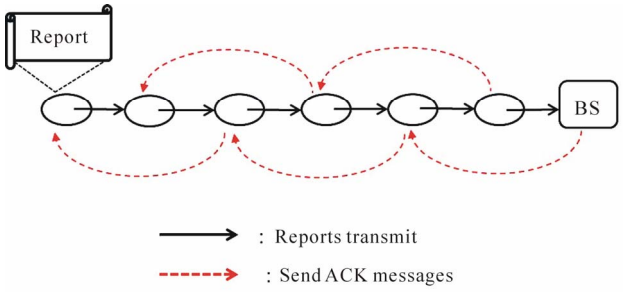


Figure 5. Overview of the message transmission process.

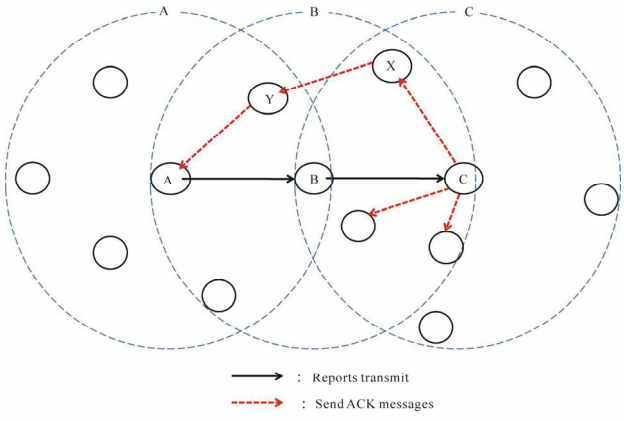


Figure 6. ACK message transmission.

repeated until the ACK message is delivered to node A.

Figure 7 shows a report transmitted to node B from a node A via a wormhole tunnel. Since node A sends the reports, it waits for an ACK message, which it cannot receive. The node B sends an ACK message to node A, but the ACK message has a maximum hop limit called Time-to-Live (TTL). If no limit was set, the ACK messages would float throughout the network, wasting limited node energy. **Figure 7** shows that node B sends an ACK message to node A with a limited TTL value, but the ACK message cannot be delivered to node A. If the TTL value is too large, it may be delivered to node A even when reports are transmitted via a wormhole. If the TTL value is too small, it may not be delivered to node A even when reports are not transmitted via wormhole. Therefore the TTL value must be carefully determined based on network statements.

5. Simulation Results

To show the effectiveness of the proposed method, we compare the proposed method with the combined LITEWORP and SEF schemes via simulation. Each node consumes 16.25 μJ and 12.5 μJ to transmit and receive a byte, respectively. The size of an original report and a MAC is 24 byte and 1 byte, respectively. Each message includes 5 MACs for the SEF. There is a global key pool of 1000 keys, the number of partitions is 25 and each node possesses 30 keys.

A probability comparison for wormhole detection between the LITEWORP+SEF method and the proposed method is presented in **Figure 8(a)** and the probability of false alarms (assuming no false reports in the network) are presented in **Figure 8(b)** herein, we calculate the probability of wormhole detection based on the percentage of isolated wormhole nodes and the probability of false alarms based on isolated normal nodes. The proposed method shows a higher wormhole detection performance than the LITEWORP+SEF method when the number of neighbor nodes is less than 7 or greater than 21; however, the proposed method shows a lower false alarm performance (higher probability) than the LITE WORP+SEF method. Because the proposed method uses ACK messages for wormhole detection, the ACK messages cannot be delivered to the previous node if the number of neighbor nodes is low.

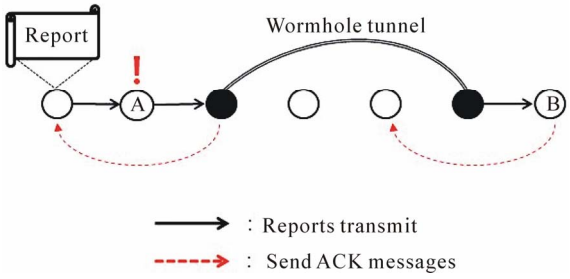
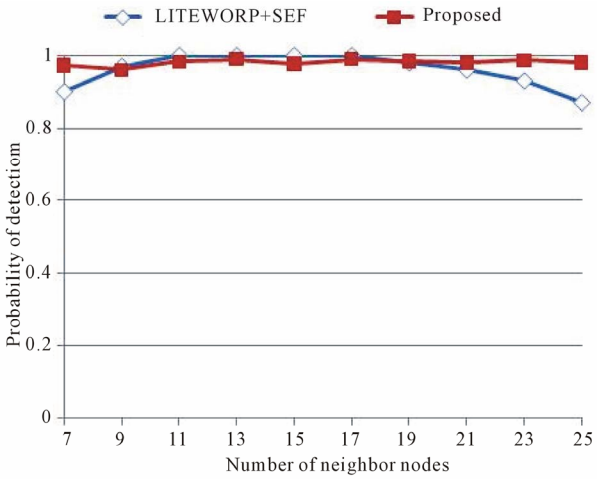
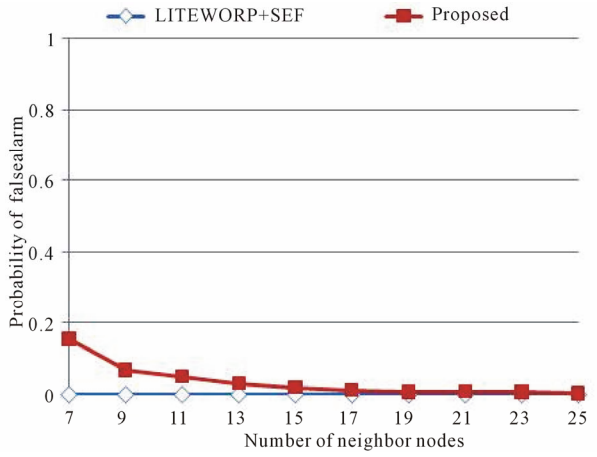


Figure 7. Wormhole detection.

Figure 9 shows the probability of false alarms versus



(a) Probability of wormhole detection



(b) Probability of false alarm

Figure 8. Probability of detecting wormholes and false alarms.

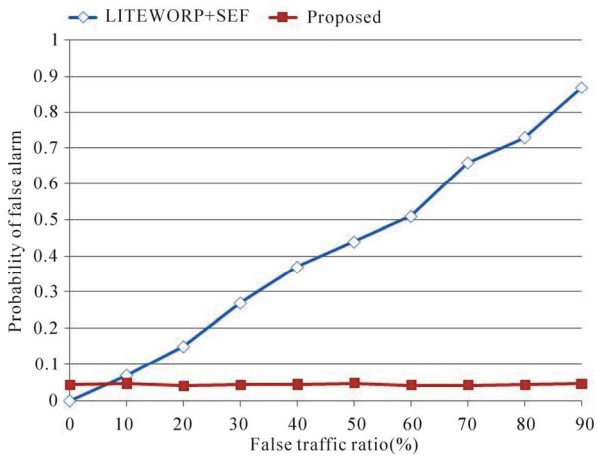


Figure 9. Probability of false alarm.

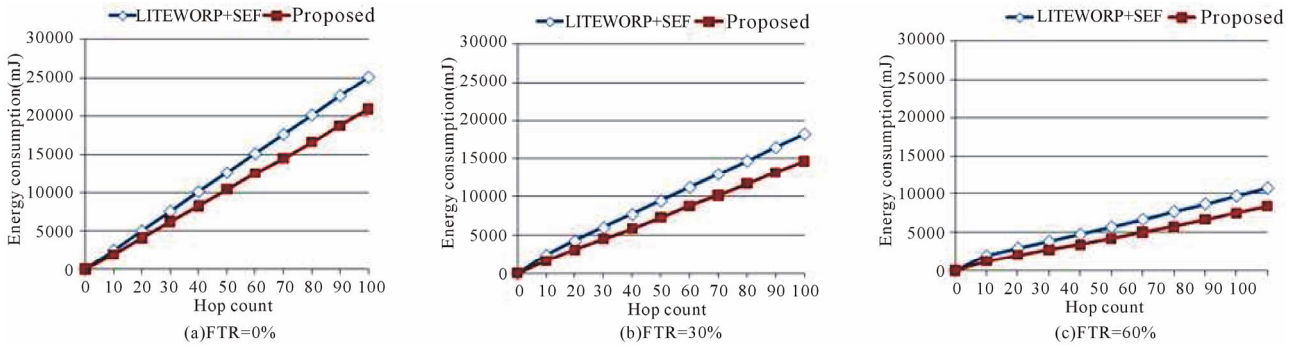


Figure 10. Energy consumption for different false traffic ratios (FTR).

the ratio of false reports when TTL = 3 and the number of neighbor nodes is 9. The proposed method has the same probability of false alarms regardless of the false traffic ratio. The LITEWORP+SEF method has a high probability of false alarms when the false traffic ratio is high because SEF detects false reports and drops them without notifying neighbor nodes. LITEWORP monitors this drop event and regards it as malicious behavior, hereby increasing the probability of a false alarm.

Figure 10 shows the energy consumption of the proposed method and the LITEWORP+SEF method. The simulation results show that the proposed method consumes less energy than the LITEWORP+SEF method for every false traffic ratio (FTR) shown. The proposed method consumes less energy than the LITEWORP+SEF method when the FTR is increased because false reports are detected and dropped in the early routing stages. The LITEWORP+SEF method consumes more energy than the proposed method because LITEWORP monitors all traffic in the network and SEF attaches message authentication codes to all reports. The proposed method uses ACK messages instead of monitoring traffic. The resulting large report size of the LITEWORP+SEF method is overhead, but the proposed method is unaffected by the report size.

6. Conclusion

In this paper, we proposed a secure routing method for detecting false reports and wormhole attacks in wireless sensor networks. The LITEWORP and SEF methods have two problems because they are designed without consideration of each other. The first problem is false alarms that isolate normal nodes. The SEF method detects false reports and drops them but LITEWORP regards this dropping as malicious behavior and isolates the node. The second problem is energy consumption; the report size increases because SEF attaches MACs to reports, and LITEWORP monitors all of this increased traffic in the network. The LITEWORP+SEF method thus consumes a lot of energy. The proposed method solves these problems using ACK messages. The simulation results show that the proposed method decreases both the probability of false alarms and energy consumption.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A Survey on Sensor Networks," *IEEE Communications Magazine*, Vol. 40, No. 8, 2002, pp. 102-114. doi:10.1109/MCOM.2002.1024422

[2] L. Buttyan, *et al*., "Statistical Wormhole Detection in Sensor Networks," *Lecture Notes in Computer Science*, Vol. 3813, 2005, pp. 128-141. doi:10.1007/11601494_11

[3] B. Przydatek, D. Song and A. Perrig, "SIA: Secure Information Aggregation in Sensor Networks," *Proceedings of the First International Conference on Embedded Networked Sensor Systems*, Vol. 15, No. 1, 2003, pp. 255-265. doi:10.1145/958491.958521

[4] A. C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H. C. Wong and A. A. Loureiro, "On the Security of Cluster-Cased Communication Protocols for Wireless Sensor Networks," *Lecture Note in Computer Science*, Vol. 3420, 2005, pp. 449-458. doi:10.1007/978-3-540-31956-6_53

[5] S. Park, A. Savvides and M. B. Srivastava, "SensorSim: A Simulation Framework for Sensor Networks," *Proceedings of International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2000, pp. 104-111.

[6] M. Tubaishat and S. Madria, "Sensor Networks: An Overview," *IEEE Potentials*, Vol. 22, No. 2, 2003, pp. 20-23. doi:10.1109/MP.2003.1197877

[7] 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, 2005, pp. 839-850. doi:10.1109/JSAC.2005.843561

[8] H. Yang ans S. Lu, "Commutative Cipher Based En-Route Filtering in Wireless Sensor Networks," *Proceedings of the 60th IEEE Vehicular Technology Conference*, Vol. 2, 2004, pp. 1223-1227.

[9] J. N. Al-Karaki and A. E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Communications*, Vol. 11, No. 6, 2004, pp. 6-28. doi:10.1109/MWC.2004.1368893

[10] Z. Yu and Y. Guan, "A Dynamic En-Route Scheme for

Filtering False Data Injection in Wireless Sensor Networks," *Proceedings of the 25th IEEE International Conference on Computer Communications*, 2006, pp. 1-12.

[11] 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," *Proceedings of IEEE Symposium on Security and Privacy*, 2004, pp. 259-271.

[12] F. Li and J. Wu, "A Probabilistic Voting-Based Filtering Scheme in Wireless Sensor Networks," *Proceedings of the 2006 International Conference on Wireless Communications and Mobile Computing*, 2006, pp. 27-32. doi:10.1109/ICWMC.2006.5

[13] H. Y. Lee and T. H. Cho, "Fuzzy Adaptive Selection of Filtering Schemes for Energy Saving in Sensor Networks," *IEICE Transactions on Communications*, Vol. E90-B, No. 12, 2007, pp. 3346-3353.

[14] H. Y. Lee and T. H. Cho, "Key Inheritance-Based False Data Filtering Scheme in Wireless Sensor Networks," *Lecture Notes in Computer Science*, Vol. 4317, 2006, pp. 116-127. doi:10.1007/11951957_11

[15] Y. C. Hu, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks," *IEEE Infocom*, 2003, Vol. 3, 2003, pp. 1976-1986.

[16] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," *Proceedings of the 11th Annual Network and Distributed System Security Symposium*, 2004, pp. 1-11.

[17] I. Khalil, "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," *Proceedings of International Conference on Dependable Systems and Networks*, 2005, pp. 612-621.

[18] S. Capkun, L. Buttyán and J.-P. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks," *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2003, pp. 21-32. doi:10.1145/986858.986862

