Asian Journal of Scientific Research

ISSN 1992-1454

science alert
http://www.scialert.net

ANSInet
an open access publisher
http://ansinet.com

OPEN ACCESS Asian Journal of Scientific Research

ISSN 1992-1454
DOI: 10.3923/ajsr.2016.242.247

Research Article
A Multi-layer Framework for Detection Selective Forwarding Attacks in WSNs

Naser M. Alajmi and Khaled M. Elleithy

Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT 06604, United State of America

Abstract
Security is a major threat in Wireless Sensor Networks (WSNs). These networks are increasingly used due to their broad range of important applications in both military and civilian domains. The WSNs are prone to several types of security attacks. Limited power and low memory are obstacles that make conventional security measures inappropriate for WSNs. Sensor nodes have limited capacities and are deployed in dangerous locations, therefore, they are vulnerable to different types of attacks, including wormhole, sinkhole and selective forwarding attacks. Security attacks are classified as data traffic and routing attacks. These security attacks could affect the most significant applications of WSNs, namely, military surveillance, traffic monitoring and healthcare. Therefore, there are different approaches to detecting security attacks on the network layer in WSNs. Reliability, energy efficiency and scalability are strong constraints on sensor nodes that affect the security of WSNs. Because sensor nodes have limited capabilities in most of these areas, selective forwarding attacks cannot be easily detected in networks. A compromised node selectively drops packets. A malicious node works in the same manner as any other node in the network. However, it tries to find sensitive messages and drop them before transferring packets to other nodes. In this study, we propose an approach to Selective Forwarding Detection (SFD). The approach has three layers: MAC pool IDs, rule-based processing and anomaly detection. It maintains the safety of data transmission between a source node and base station while detecting selective forwarding attacks. Furthermore, the approach is reliable, energy efficient and scalable.

Key words: Wireless sensor network , sensor node, data traffic, security attacks, SFD

Received: May 16, 2016 **Accepted:** August 29, 2016 **Published:** November 15, 2016

Citation: Naser M. Alajmi and Khaled M. Elleithy, 2016. A multi-layer framework for detection selective forwarding attacks in WSNs. Asian J. Sci. Res., 9: 242-247.

Corresponding Author: Naser M. Alajmi, Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT 06604, United State of America

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

A sensor node is a small, light-weight sensing device. It is composed of a constrained processing unit and small amount of memory for its small operating system. Additionally, a sensor node includes a limited-range transceiver and a battery unit a mobile node also includes a mobility subsystem. Wireless Sensor Networks (WSNs) manage thousands of sensor nodes. In fact, these sensor nodes communicate with a vast number of small nodes via radio links. Sensor nodes in a network gather data that are necessary to include in a smart network environment. These environments include homes, transportation systems, military installations, healthcare systems and buildings. The WSNs make it technologically possible to reorganize information and communication technology. The study of WSNs is a significant topic in computer science and engineering. It has an economic impact and affects industry[1].

In WSNs, sensor nodes transfer packets from the source to the base station. Because a sensor node is a limited-transmission device, it uses a multi-hop method to transfer packets to the base station. Eavesdropping, compromising nodes, interrupting or modifying packets and injecting malicious packets compromise privacy and denial of service attacks are threats to the security of WSNs[2]. Attackers compromise the internal sensor nodes from which they launch attacks, which are difficult to detect. A selective forwarding attack is the one of these attacks.

PROBLEM IDENTIFICATION

A selective forwarding attack is difficult to detect in a network. The adversary installs a malicious node, which drops packets in the network. Once the malicious node is present in the network, it organizes routing loops that attract or repel network traffic. Additionally, it can extend or shorten source routers, generate false messages and attempt to drop significant messages. Packets that are dropped selectively come from one node or a group of nodes. A malicious node refuses to forward the packets. Therefore, the base station does not receive the entire message. There is a need for a new paradigm for detecting selective forwarding attacks that increases the detection rate while consuming less energy.

Xiao *et al.*[3] proposed a LWSS-based approach that uses lightweight security to detect a selective forwarding attack in a sensor network environment. The approach uses a multi-hop acknowledgment to launch alarms by obtaining responses from the nodes that are located in the middle of a path. The aim of attack detection is to send an alarm that indicates a selective forwarding attack when a malicious node is discovered. Yu and Xiao[4] employed two detection processes in the scheme: A downstream process and an upstream process. Sending an acknowledgment packet and alert packet would drain energy during the detection process. In this approach, a node is randomly selected as the checkpoint that sends a message acknowledging the detection of an adversary.

Hai and Huh[5] proposed an LWD-based approach to detecting selective forwarding attacks that consist of a lightweight mechanism. Each sensor node is provided with a detection module that is constructed on top of an application layer. A sensor node sets its routing rules and uses information on its two-hop neighborhood to generate an alert packet. Hai and Huh[5] suggested 2 routing rules to improve the monitoring system. The 1st rule is to determine whether the destination node forwards the packet along the path to the sink. The 2nd rule is that the monitoring node waits and detects a packet that had been forwarded along the path to the sink.

Deng *et al.*[6] proposed an SDT-based scheme for secure data transmission and for detecting a selective forwarding attack. They used watermark technology to detect malicious nodes. Prior to employing a watermark-based technique, they used a trust value to find a source path for message forwarding. When the network is initialized, all of the nodes are assigned the same trust value. Deng *et al.*[6] used a watermark-based technique to calculate the amount of packet loss. The base station compares the extracted watermark to the original watermark to detect a selective forwarding attack.

Tumrongwittayapak and Varakulsiripunth[7] proposed an RSSI-EM-based lightweight scheme. They used Extra Monitoring (EM) to eavesdrop and monitor all of the traffic when data were transferred between nodes. The value of an RSSI is that four EM nodes can be arranged to establish the positions of all of the sensor nodes, with the base station located at (0, 0). They assumed that the attackers could capture and damage the nodes. Therefore, all of the sensor nodes must protect themselves or be made from tamper-resistant hardware.

MATERIALS AND METHODS

In a sensor network, data are sent to the base station through routers. An attacker compromises the nodes by attacking the network resources. Selective forwarding attacks destroy the packets transmitted between the source and base station. As a result, a malicious node refuses to transfer a complete packet. It attempts to drop the important data.

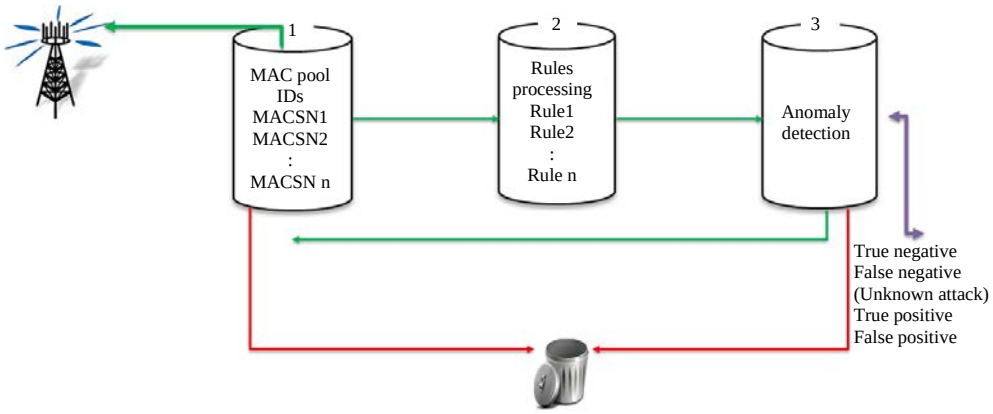

Fig. 1: Multi layers in rules based IDS

Therefore, the entire packet is not transferred to the base station. Furthermore, physical attacks frequently occur in WSNs because they are easy for adversaries to execute.

Sensor networks are vulnerable to many types of security attack. A malicious node tries to create blocks that occur while messages are being transferred between sensor nodes in the network by, for instance, forwarding a message along another path, generating an inaccurate network route and delaying the transfer of packets between nodes. Selective Forwarding Detection (SFD) discovers a secure route for data to be sent from one node to other nodes. In this study, we introduce the assumptions and a multi-layer approach to detection.

Assumptions: To create a simple solution to detecting selective forwarding attacks, we make some assumptions for detection within certain applications that are vulnerable in networks. Specifically, we assume that secure communication is the focus of sensor networks, malicious nodes should not drop any packets before launching a selective forwarding attack and an adversary cannot attack nodes during their deployment.

Selective Forwarding Detection (SFD) using multi-layer: Rule-based IDS is also known as signature-based IDS, which is one of the mechanisms for protecting a network from security threats. The network layer in WSNs is threatened with many types of attacks, including wormhole and sinkhole attacks. Our proposal focuses on the selective forwarding attack. We design a multi-layer approach to detection that includes the three security layers shown in Fig. 1. The first layer is a pool of MAC IDs. In this layer, the important information is filtered and stored. The information includes message fields (e.g., packet, destination and source IDs) that are useful for rule-based processing. The 2nd layer is the rule-based processing layer. In this layer, there are some rules that must be applied to the stored data. Incoming traffic is either accepted or rejected. In addition, no rules are applied to a message that fails. The 3rd layer is the anomaly detection layer, which detects the false negative anomalies that comprise unknown attacks. The 2nd layer (rule-based processing) and the third layer (anomaly detection-based IDS) can identify and control selective forwarding attacks in all phases. The three layers are supported with three algorithms. These algorithms are to used resolve the attack on the network. The detection approach saves energy by using little time and memory. It chooses a secure route along which to transfer data between the source and base station. Furthermore, the approach to SFD using multiple layers is reliable, energy efficient and scalable. All of these factors are important for networks of sensor nodes. Additionally, this approach to SFD is highly accurate.

Selective Forwarding Detection (SFD) algorithms:

Algorithm1: MAC pool IDs layer

```
Input = (MP: Mac Pool)
Output = (DT: Selective Forwarding Detector)
Network parameter = (SN: Sensor node, RT: Route, TSN: Total sensor node)
Attacking parameter = (SFAT: attacker)
For (SN = 0; SN<= TSN; SN++)
Set SN = SN+1
If SN MP then
Set SN = 0 //Node is declared as malicious node not allowed for communication
Drop
Else if SN = 1 //Node is declared as a legitimate node and allowed for communication
Accept
End if
End else
End for
```

MAC pool IDs layer: The first layer consists of a pool of MAC IDs that filter and match the traffic. Each traffic packet is monitored. The packet is matched to identify malicious activity using message fields (e.g., the packet, destination and source IDs). It checks whether a node is legitimate or malicious. Therefore, if a node is assigned a value of zero, it drops a packet and is considered malicious. Otherwise, it is accepted as a legitimate node. In our study, we analyze the malicious nodes that are detected in the first step using an algorithm based on the pool of MAC IDs.

Algorithm2: Rules processing layer

```
Input = (RP: Rules process)
Output = (DT: Selective forwarding detector, RU: Rules)
Network parameter = (SN: Sensor node, RT: Route)
Attacking parameter = (SFAT: Attacker)
RL1 = Rules based in IDS (RL1IDS)
RP⊂RL1IDS
Set RL1 >= RU//90% from the rules
For (SFAT = RL1, SFAT <= RP, SFAT ++)
If SFAT RP then
DT→SFAT
Attack alert
Reject Packets
Else if (SFAT⊄RP) then
Set SN = RT
Return
SN→MP
Release Packets
End if
End else
End for
```

Rules processing layer: The second layer involves rule-based processing. It is the middle layer. It detects known attacks using rules. These rules must be applied before nodes are deployed in a network area.

The rule-based processing layer checks the traffic by comparing it to a list of rules. If the traffic satisfies at least 90% of the rules, the node is confirmed to be legitimate. Therefore, the traffic will be returned to the pool of MAC IDs for release. If the traffic does not satisfy 90% of the rules, the node is considered doubtful and is rejected.

Algorithm3: Anomaly detection layer

```
Input = (AD: Anomaly detection)
Output = (DT: Selective forwarding detector)
Network parameter = (SN: Sensor node, RT: Route)
Attacking parameter = (SFAT: Attacker)
RL2 = Anomaly detection based in IDS (RL2IDS)
AD⊂RL2IDS
For (RL2 = 0, RL2 <= AD, RL2++)
RL2 = RL2+1
If RL2∈AD then
Compute FN
Set Alert
Reject Packets
Else if RL2⊄AD then
No Attack
Set SN = RT
Return
SN→MP
Release Packets
End if
End else
End for
```

Anomaly detection layer: The third layer involves anomaly detection, which is the recognition of unknown attacks. This layer checks the traffic that comes from the rule-based processing layer. Therefore, it works to analyze the traffic. The possible results of anomaly detection are false negative, false positive, true negative and true positive. If the algorithm determines that an unknown attack is a false negative, it sends an alert and rejects the relevant packet. Otherwise, the traffic is returned to the pool of MAC IDs by confirming the legitimacy of the node.

RESULTS AND DISCUSSION

The approach to detecting selective forwarding attacks is tested using a simulation. In the simulation, 200 sensor nodes are deployed in a network with an area of 800×800 m^2 using NS2. Therefore, each node had a transmission range of 35 m and a sensing range of 30 m. The energetic cost of a node is 5 J and there are 180 static and 20 mobile nodes. We calculated the amount of energy consumed. Figure 2 showed the energy consumption of our approach to SFD when 10% of the nodes were malicious and 10% were mobile. The network consumed less energy when it included mobile nodes; therefore, it was 60.4% at the highest point and the energy cost was low. Therefore, if there are malicious nodes along the routes, this approach to SFD costed less in terms of communication overhead. Figure 3 showed all of the approaches, including SFD and the RSSI-EM, SDT, LWSS and LWD approaches for the same percentages of malicious and mobile nodes. Therefore, the number of malicious nodes and the energy consumption are comparable in all of the approaches. However, the other approaches consumed more energy when the network includes mobile nodes. Their energy costed are 68.5, 69.1, 75.1 and 81.8%, respectively. Thus, the proposed approach to SFD was more energy efficient. Figure 4 illustrates the rate of reliably detecting selective

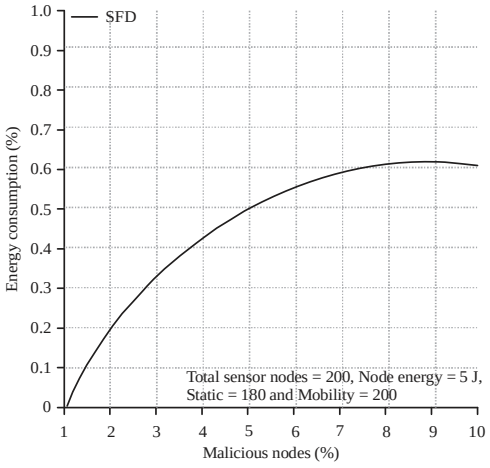

Fig. 2: Energy consumption of SFD approach under malicious node

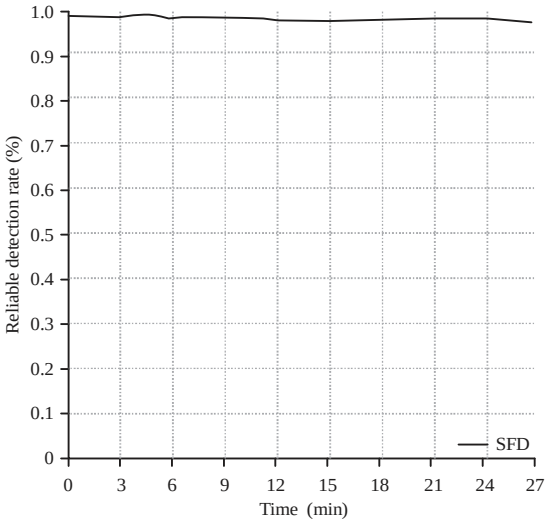

Fig. 4: Reliable detection rate of SFD approach

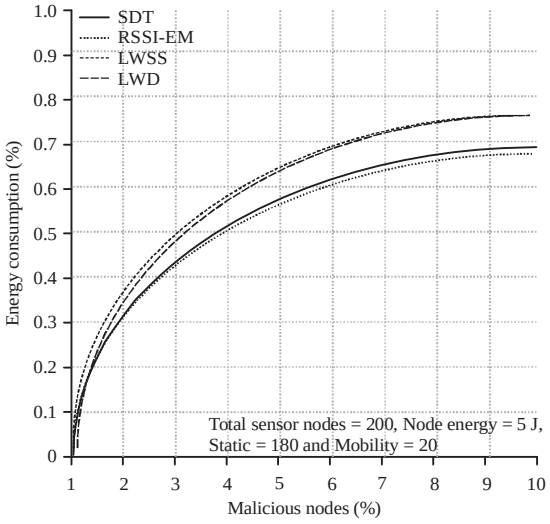

Fig. 3: Comparison of approaches in energy consumption

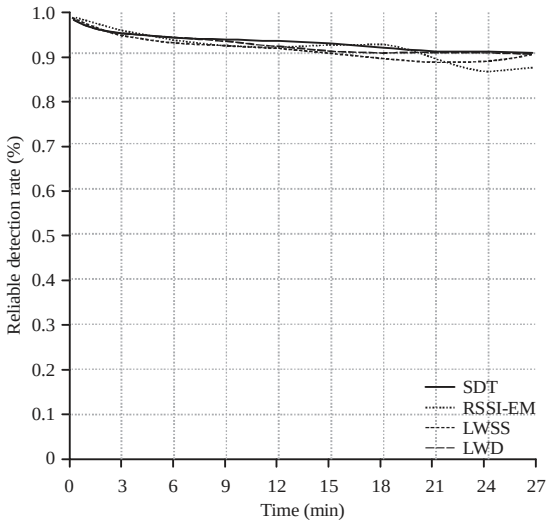

Fig. 5: Comparison of approaches in reliable detection rate

forwarding attacks. The proposed approach to SFD has a perfect detection rate. This rate is greater than 98%; therefore, it is easier to detect malicious nodes when they dropped packets. During the lifetime of a network, the SFD algorithm accurately detects the malicious nodes. We compared our approach with the RSSI-EM-, LWSS-, SDT- and LWD-based approaches (Fig. 5). Their rates of reliably detecting selective forwarding attacks are 86.3, 88.2, 89.6 and 90.6%, respectively. The graphs showed detection rates of all of the approaches. Therefore, this approach to SFD is more reliable than other approaches.

CONCLUSION

A multi-layer detection framework is introduced to handle one type of severe attack (the selective forwarding attack). We proposed an approach to detect selective forwarding attacks to address this issue. The multi-layer detection framework consists of 3 layers, each of which is supported by a different algorithm. In the first layer, we used an algorithm based on a pool of MAC IDs that authenticates incoming traffic to determine whether a node is legitimate or malicious. In the second layer, we used a rule-based processing algorithm, which checks the traffic by comparing it to a list of rules. In the

third layer, we used an anomaly detection algorithm to identify unknown attacks, which appear as false negatives, send an alert and reject the traffic. In addition, the framework was validated using NS2. Based on the simulation results, we demonstrated that this approach's detection rate and energy consumption are higher than those of other approaches. Therefore, the proposed approach to SFD is more effective than other approaches.

REFERENCES

1. Karlof, C. and D. Wagner, 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad Hoc Networks, 1: 293-315.
2. Perrig, A., J. Stankovic and D. Wagner, 2004. Security in wireless sensor networks. Commun. ACM, 47: 53-57.
3. Xiao, B., B. Yu and C. Gao, 2007. CHEMAS: Identify suspect nodes in selective forwarding attacks. J. Parallel Distrib. Comput., 67: 1218-1230.
4. Yu, B. and B. Xiao, 2006. Detecting selective forwarding attacks in wireless sensor networks. Proceedings of the 20th International Parallel and Distributed Processing Symposium, April 25-29, 2006, Rhodes, Greece.
5. Hai, T.H. and E.N. Huh, 2008. Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge. Proceedings of the 7th IEEE International Symposium on Network Computing and Applications, July 10-12, 2008, Cambridge, MA., pp: 325-331.
6. Deng, H., X. Sun, B. Wang and Y. Cao, 2009. Selective forwarding attack detection using watermark in WSNs. Proceedings of the International Colloquium on Computing, Communications Control and Management, Volume 3, August 8-9, 2009, Sanya, pp: 109-113.
7. Tumrongwittayapak, C. and R. Varakulsiripunth, 2009. Detecting sinkhole attack and selective forwarding attack in wireless sensor networks. Proceedings of the 7th International Conference on Information, Communications and Signal Processing, December 8-10, 2009, Macau, China, pp: 1-5.