Selective Forwarding Attacks Detection in WSNs

Naser M. Alajmi and Khaled M. Elleithy
Computer Science and Engineering Department, University of Bridgeport, Bridgeport, CT, USA
nalajmi@my.bridgeport.edu, elleithy@bridgeport.edu

Abstract

Wireless sensor networks (WSNs) are susceptible to the most security attacks. Limited capacity of sensor nodes accounts for the security attacks on WSNs. Applications such as military surveillance, traffic surveillance, healthcare, and environmental monitoring are impacted by security attacks. Hence, researchers have created various types of detection approaches against such attacks. There are also some limitations such as reliability, energy efficiency, and scalability, which affect sensor nodes. These limitations mostly affect the security of WSNs. Selective forwarding attack is an example of an attack that is not easily detected particularly in the networks layer. In this type of attack, malicious nodes function in the same way as other nodes in the networks. However, it tries to drops the sensitive packets prior to transferring the packet to other sensor node. In this paper, we propose an approach that protects data from selective forwarding attacks. The approach keeps the data transmission moving safely between sensor nodes and at the same time detects malicious nodes.

Keywords

Wireless Sensor Networks (WSNs) and Selective Forwarding Attacks.

Introduction

Wireless sensor networks contain numerous sensors. These sensors communicate with huge numbers of small nodes by using radio links. Sensor networks consist of the source and base station. A sensor is composed of four basic units, which are sensing unit, processing, transceiver, and power[1]. The task of sensor nodes is collecting the information that is needed by smart environments. These environments are for instance: home, transportation system, military, healthcare, buildings etc. The study of the Wireless Sensor Network is crucial in computer science and engineering and has an impact on the community, in economic, and industrialization. Nowadays, many distributed sensor networks can be deployed and have a self-organizing ability. Computational ability needs the sensor nodes, which are not overloaded with too many complicated functions.

WSNs work in open networks with the limited resources of nodes and obstacles. Thus, they are prone to many types of attacks. The security of WSNs has been studied over the past few years. The most traditional threats include eavesdropping, nodes being compromised, interruptions, modified or injected malicious packets, compromised privacy and the denial of service attacks[2]. Networks have different applications that comprise of several levels of monitoring, tracking, and controlling. Therefore, applications are employed for specific purposes. In military applications, sensor nodes include monitoring, battlefield surveillance, and object tracking. The battlefield monitors utilized in military operations have prompted the development of WSNs. In medical applications, sensors assist in patient diagnosis and monitoring. Applications are deployed to monitor an area and then react when a sensitive factor is recorded[3]. There are also some potential applications such as environmental monitoring, factory instrumentation and inventory tracking.

Selective Forwarding Attack

There are several types of attacks that exist in WSNs. Most security attacks are located in the network layer. Furthermore, a sensor node may derive benefits from multi-hop by simply refusing to route packets. It can be performed frequently with the net result. Malicious nodes will not be incapable to change or modify the message if the neighboring node marks a route[4]. The Network layer receives varieties of attacks. For example, injecting the path between sensor nodes.

Selective forwarding attack is one of the insider attacks. A more subtle form of this attack is when an adversary selectively forwards packets. The adversaries are able to create routing loops that attract or repel network traffic. They also can be extend or shorten source routers, generate false messages, and attempt to drop the sensitive information. The selective forwarding attack is not easy to detect particularly when compromised nodes drop packets selectively. The dropped packets come from one node or a set of nodes. A malicious node can refuse to forward the messages or drop packets randomly. For this reason, the base station may not receive the entire message[5, 6].

Related Works

Yu and Xiao[6] proposed an approach based on lightweight security to detect a selective forwarding attack in the environment of sensor networks. The approach utilized a multi-hop acknowledgment to launch alarms by obtaining responses from the nodes that are located in the middle of paths. Authors assumed the approach could identify malicious sensor nodes. The aim of the detection attack is to send an alarm when a malicious node is discovered, which indicates a selective forwarding attack. The authors noted that the detection accuracy of their approach exceeds 95% with an error rate of 15%. Yu and Xiao employed two detection processes in the scheme: a downstream process (the direction on the way to the base station) and an upstream process (the direction on the way to the source node). In the upstream process, a report packet is created and sent to the base station hop by hop when nodes detect a malicious node. Therefore, the base station would receive the alarm packet and forward multiple hops that are produced by the node. An acknowledgement packet and an alert packet will drain the energy during detection.

The identification of suspect nodes is reported via an intermediate node. First, Xiao, Yu, and Gao[7] proposed a checkpoint-based method. In this approach, a node is randomly selected as the checkpoint to send an acknowledgement message for detecting the adversary. It is a mechanism used to identify suspect nodes in a selective forwarding attack. They have attempted to improve the technique by detecting an abnormal packet in sensor networks. They assumed that any compromised nodes could not create alert packets with the aim of maliciously prosecuting other nodes. After collecting evidence to determine whether the node is a malicious node, the source nodes determine the position of the suspect node according to the location. However, it is no guarantee for reliable transmission of messages even though the adversary is positioned by acknowledgement.

Tran Hoang and Eui-Nam[8] proposed an approach against selective forwarding attacks that consists of a lightweight detection mechanism. The detection is a centralized cluster, which utilized the two-hop neighborhood node information and overhearing technique. It is dependent on the broadcast nature of sensor communication and the high density of sensors. Each sensor node is provided with a detection module that is constructed on an application layer. Sensor node sets routing rules and two-hop neighbor knowledge to generate an alert packet. Hoang and Nam suggested that the two routing rules make the monitoring system more suitable. Thus, the first rule is to determine if the destination node forwards the packet along the path to the sink. It generates an alert packet with the malicious factor α to the sender/source node. The second rule governs that the monitor node waits and detects the packet that was already forwarded along the path to the sink. It verifies the two-hop neighbor knowledge to assess whether the destination node is on the right path to the sink. If not, it generates an alert packet with the malicious factor β to the sender/source node.

Proposed System

In wireless sensor networks, several nodes transfer sensor readings to the base station in order to process data. Military bases are important in using sensor networks to explore enemy forces. Sensor nodes have limited sensing and computation. There is also communication ability. Sensors gather data when they detect abnormal movement of enemy forces such as warplanes, war tanks movement in battlefields etc. Data transmission is sent to the base station using routers. So, the attacker compromises nodes to attack the networks (Figure 1). Malicious nodes reject to send the entire message. Thus, it drops the important information and keeps the remaining message to forward to the next node. Because the military applications have sensitive information, selective forwarding attacks damage the transmission message between the source and base station as well as between sensor nodes.

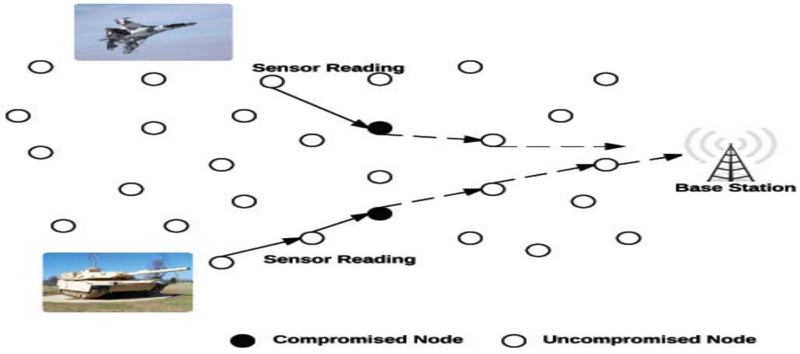


Figure 1. Sensor nodes during selective forwarding attacks

In networks, the malicious node tries to create obstacles during the transfer of packets in the networks. These obstacles include forwarding certain messages to different paths, generating an inaccurate route in the network and also, attempting to delay the transfer of packets between nodes. Therefore, selective forwarding detection approach locates a secure route during data transmission. In this section, we introduce our assumptions and detection approach. Sensor networks are susceptible to several types of attacks.

WSNs is composed of base station and sensor nodes. Sensor nodes are grouped into clusters. Each cluster has several nodes as shown in Figure 2. A packet is transferred via a source node to the base station using a route. During the transmission any malicious node drop a packet, the neighbor nodes work as monitoring and detect the packet that drop by the adversary. In our approach, any node located in an intermediate is responsible to detect the malicious nodes.

The selective forwarding attack in example of Figure 3 may happen between sensor nodes. Thus, node “A” transfers the packets to node “B” and then node “B” stops forwarding the packets to node “C”. As a result, node “B” may forward packets to malicious node. Therefore, packets will not arrive to the base station.

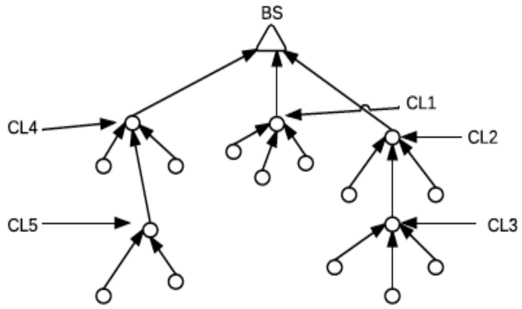


Figure 2. Nodes are arranged in Clusters

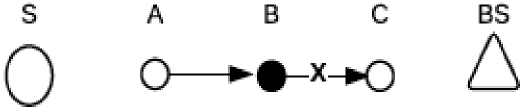


Figure 3. Example of Selective Forwarding Attack

A. Assumptions

The network layer in WSNs is threatened by some attacks such as wormhole, sinkhole, and many types of attacks. Wireless sensor networks are very difficult for the transmission. In order to construct a simple solution to detect the selective forwarding attack, we make assumptions for our approach detection that are suitable in the sensor networks. These assumptions are as follow:

- Secure communication should be part of the networks.
- Malicious nodes should not drop any packet prior to launch the selective forwarding attack.
- The adversary cannot compromise a sensor node during the deployment.
- The authentication broadcast protocols implemented for each sensor node.

B. Analysis

Though the network layer in WSNs is threatened by many security attacks, this paper only focuses on the selective forwarding attack. There are some disadvantages of selective forwarding attacks for instance, malicious nodes may refuse to forward certain messages or sensitive information and drop them, and the adversary overhearing movement between nodes might be capable to simulate selective forwarding by jamming. Consequently, we design a multi layers approach, which includes three security layers. The first layer is data receiving. In this layer, the important information is filtered and stored. The information includes message fields that are beneficial on the rules processing. The second layer is rules processing. In this section, rules must be applied to the stored data before the sensor nodes deployed. The message can be rejected or refused. In addition, no rules will be applied to the message since it fails. The third layer is detection. The selective forwarding detection approach involves identifying the malicious nodes and chooses a secure route to transfer data between the source and base station. Furthermore, the multi layer approach considers reliability, energy efficiency, and scalability. It assumes that detection accuracy is high even when the radio condition is poor.

C. Simulation

In this section, we used NS2 simulation to estimate the performance of the multi-layer detection approach. We have focused our simulation on malicious detection rate and packet delivery ratio. In our simulation, 200 sensor nodes are deployed in an area network size 500 * 500 square meters. Hence, each node has a 35 meters transmission range and sensing range of node is 30 meters. Consequently, the communication overheads are decreased.

Figure 4 shows the performance of our approach for the packet delivery ratio. Thus, the malicious nodes are appearing. During the increasing malicious nodes drop packet, our approach can achieve packet delivery ratio under the overflow of attack. Therefore, it can be accomplished up to 40% malicious nodes. The packet delivery ratio is decreased rapidly while the malicious nodes increase. The effect of the malicious increase of packet delivery ratio, it takes time to defeat and take them away.

The approach in Figure 5 is a perfect detection rate. It is more than 98% as long as the noise error is 2-4%, and the malicious nodes are under 12%. In fact, the noise error rate increases while the detection of malicious nodes failed. Losing packet happened when the collision ratio and malicious nodes increased. Sometime the radio condition is poor because the communication in WSNs. As a result, the detection rate of the malicious nodes will be impacted. We observe that our approach is more efficient when the number of detection nodes increased. The probability of missed detection occurs when collision is available in the network at the time by monitoring the node attempting to send an alert packet.

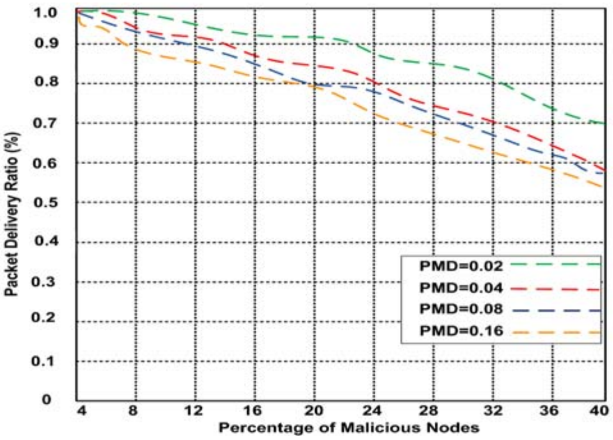


Figure 4. Packet delivery ratio under malicious attacks in WSN

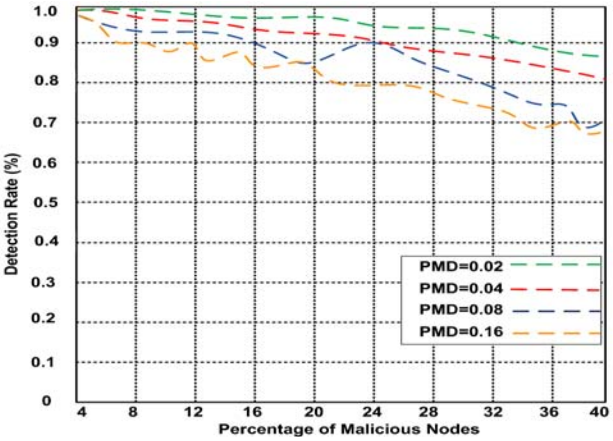


Figure 5. Detection of malicious nodes in the WSN

Conclusion

The security of WSNs has become increasingly concerning. The use of wireless sensor networks is progressively employed in environmental, commercial, health and military applications. The security of packets and the transmission period is fundamentally necessary in WSNs. The selective forwarding attack poses severe threats to wireless networks. In this paper, we propose an approach in detecting this type of attack in WSNs. Monitor sensor nodes detect selective forwarding attacks using neighbor nodes. Our approach is an efficient way of detecting the attacks. We also take into consideration reliability, energy efficiency, and scalability. Analysis and simulation show that our approach is more effective when the numbers of detection nodes increased.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wirelss sensor networks: A survey," Computer Networks, 38(4):393-422, 2002.

[2] A. Perrig, J. Stankovic, and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, 47(6):53– 57, June 2004.

[3] David Martins, and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", 2010 IEEE.

[4] J. P. Walters, et al., "Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, p. 367, 2007.

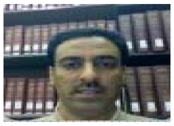
[5] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003.

[6] Bo Yu and Bin Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks", In Parallel and Distributed Processing Symposiun, 2007. ISSNIP 2006, 20th International, page 8 pp., 2006.

[7] Bin Xiao, Bo Yu, and Chuanshan Gao, "CHEMAS: Identify Suspect Nodes in Selective Forwarding Attacks", In Parallel and Distributed Processing Symposiun, 2007.

[8] Tran Hoang Hai and Eui-Nam Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge" Seventh IEEE Internation Symposium on Network Computing and Applications, 2008, pp.325-331.

[9] A. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized intrusion detection in wireless sensor networks", international workshop on Quality of service & security in wireless and mobile networks, 2005.



Mr. Naser Alajmi is pursuing towards his Ph.D., Department of Computer Science and engineering at the University of Bridgeport, Bridgeport, CT. Naser's interests are in Wireless Sensor Network (WSN), Wireless Sensor Network Security, and Network Security

Dr. Khaled Elleithy is the Associate Vice President of Graduate Studies and Research at the University of Bridgeport. He is a professor of Computer Science and Engineering. He has research interests are in the areas of wireless sensor networks, mobile communications, network security, quantum computing, and formal approaches for design and verification. He has published more than three hundred research papers in international journals and conferences in his areas of expertise.

!

Dr. Elleithy has more than 25 years of teaching experience. His teaching evaluations are distinguished in all the universities he joined. He supervised hundreds of senior projects, MS theses and Ph.D. dissertations. He supervised several Ph.D. students. He developed and introduced many new undergraduate/graduate courses. He also developed new teaching / research laboratories in his area of expertise.

Dr. Elleithy is the editor or co-editor for 12 books by Springer. He is a member of technical program committees of many international conferences as recognition of his research qualifications. He served as a guest editor for several International Journals. He was the chairman for the International Conference on Industrial Electronics, Technology & Automation, IETA 2001, 19-21 December 2001, Cairo – Egypt. Also, he is the General Chair of the 2005-2014 International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering virtual conferences.