Selective Forwarding Detection (SFD) in Wireless Sensor Networks

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

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

Abstract— **Security is the critical subject in wireless sensor networks. Therefore, WSNs are susceptible to several types of security attacks. One reason to attack sensor networks is the limited capacity of sensor nodes. The security attacks could affect the most significant applications in WSNs area such as military surveillance, traffic monitor, and healthcare. Thus, there are different types of detection approaches against security attacks on the network layer in WSNs. Also, there are severe constraints on sensor nodes like reliability, energy efficiency, and scalability, which affect the security in WSNs. Since the sensor nodes have limited capabilities for most of these constraints, a selective forwarding attack is difficult to detect in the networks. Malicious nodes in the selective forwarding attack, work as normal nodes. However, it attempts to find the sensitive messages and drop them before sending the packet to other nodes. In order to keep this type of attacks away from networks, we propose a multi layers approach (SFD) that preserves the safely of data transmission between sensor nodes while detecting the selective forwarding attack. Furthermore, the approach includes reliability, energy efficiency, and scalability.**

Keywords— Wireless Sensor Networks (WSNs) and Selective Forwarding Attacks.

I. Introduction

Sensor networks gather data that is necessary to include in smart networks environments. For example, these environments include home, transportation system, military, healthcare, and buildings. The study of Wireless Sensor Network is an active topic in computer science and engineering. WSNs have an impact on economics, and effect industrial industry. It contains numerous sensors, in fact these sensors communicate with a vast number of small nodes via radio links. Sensor networks have a source and a base station. WSNs manage thousands of sensor nodes. A sensor consists of four basic units, sensing unit: processing, transceiver, and power [1]. Currently many distributed sensor networks can be deployed, and have a self-organizing ability. Within the computation ability technique of WSNs mechanism's development, the technique must insure that sensor nodes are not overloaded with too many complicated functions.

The security of wireless sensor networks has been extensively investigated over the past few years. WSNs are susceptible to many types of attacks because they serve as an open network with the limited resources of nodes. Therefore, the obstacles of securing a wireless sensor network are the main disadvantage for all devices. The most conventional threats to the security of wireless sensor networks include eavesdropping, node compromised, interrupt, modify or inject malicious packets, compromised privacy and denial of service attacks [2]. Networks have different applications. Therefore, applications comprise several levels of monitoring, tracking, and controlling. A group of 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. Here, most applications are deployed to monitor an area and then react when a sensitive factor is recorded [3]. In general, sensor networks have potential applications in various industrial such as environmental monitoring, factory instrumentation and inventory tracking.

II. Selective Forwarding Attacks

A network layer in WSNs is subjected to many types of attacks. Furthermore, a sensor node may acquire advantages of multi-hop by simply refusing to route packets. Therefore, it could be executed all the time with the net result. If a neighboring node marks a route through the malicious node, then it will be unable to modify messages [4]. There are assortments of attacks targeting the network layer. The attacker can attack the routing protocol by injecting the path between the source and the base station.

In WSNs, there are two types of attacks: insider and outsider attacks. One of the insider attacks is referred to as a selective forwarding attack. In selective forwarding attack, the adversaries are able to create routing loops that attract or repeal network traffic. Also, they can extend or shorten source routers, generate false messages, and attempt to drop the significant messages. The selective forwarding attack is hard to detect particularly, when compromised nodes drop packets selectively. The drop packets come from one node or a set of nodes. A malicious node refuses to forward the messages or drop packets randomly. Thus, the base station would not get the entire messages [5,6].

III. 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.

The detection module is responsible for passively detecting a selective forwarding attack in its neighboring sensor node. The malicious counter is defined as the threshold of abnormal activity in a sensor node, which could not skip. When the malicious counter crossed the threshold X, it revoked the malicious node from its neighbor list. The authors have assumed that the neighboring node should be recognized. The neighboring node must be secure and confidential in the deployment time. The network has a static topology and uses key management to prevent any outside attacks. The selection of one type of network topology prevents the scheme from working with other topologies.

Huijuan Deng et al, [9] proposed a scheme for secure data transmission and detecting a selective forwarding attack. They used watermark technology to detect malicious nodes. Prior to employing a watermark technique, they used a trust value to determine a source path for message forwarding. The trust value involves weighting the credit of each sensor node. The author notes an error rate of 10% and detection accuracy greater than 95%. They assumed that the base station is always trustworthy and cannot be comprised by the adversary, which renders the scheme inappropriate for real wireless sensor networks. Every node has a trust value. At the beginning of network initializing, all nodes should have the same trust value. Huijuan Deng et al. utilized the watermark technique to calculate the packet loss. Data transmission begins when an optimal routing path is confirmed. The base station creates a κ bits binary sequence as the original watermark message. Therefore, a watermark message is part of the packets. A base station compares the extract watermark to the original watermark to detect a selective forwarding attack. The simulation results reveal a channel error rate of 10% and detection accuracy greater than 95%.

Chanatip et al. [10] have proposed a lightweight scheme. They referred to it as a traffic monitor-based selective forwarding attack detection scheme. They used Extra Monitor (EM) to eavesdrop and monitor all traffic when transferring data between nodes. They also employed RSSI to detect a sinkhole attack. The value of RSSI is that four EM nodes can be arranged to establish the positions of all sensor nodes, of which the base station position should be (0,0). Chanatip et al. have assumed that the network is static when sensor nodes are deployed; thus, any change in the type of topology will immediately affect their approach. They assumed that the attackers could capture and damage the nodes. Therefore, all sensor nodes must protect or use tamper robust hardware. These assumptions have caused the detection scheme to drain the energy of the sensor nodes and contribute to the high cost.

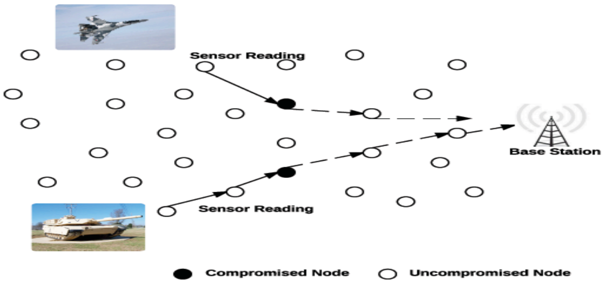

Fig 1. Sensor nodes during selective forwarding attacks

IV. Proposed System

In wireless sensor network, several nodes transfer sensor readings to the base station to process data. Military bases might find the importance of using sensor networks in order to explore enemy forces. Sensor nodes have limited sensing and computation. Also, nodes have communication ability. Sensor readings collect data when it detects unusual activities of enemy forces such as warplanes, and war tanks movement in battlefields. Data will be sent to the base station through routers. As shown in Figure 1, the attacker compromised the nodes by attacking the networks. In military applications, selective forwarding attacks destroy the transmission packets between the source and base station, and sometimes between the sensor nodes. Malicious nodes refuse to transfer an entire packet. It drops the sensitive information and then forwards the remaining packet. Furthermore, physical attacks frequently occur in WSNs because it is easy for adversaries to execute them.

Our approach finds a secure route during the data transmission. In this part, we introduce our assumptions and detection approach. Sensor networks are susceptible to several types of attacks. The malicious node attempts to make some obstacles occur during transferring packets with in the networks. The following obstacles may occur: forward message to another path, generate inaccurate route in the network, and delay transfer of the packets between nodes.

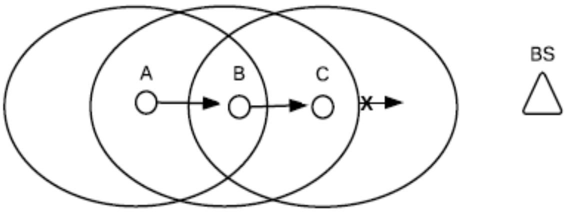

Fig 2. Example of selective forwarding attack

The selective forwarding attack in Figure 2 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 a malicious node. Therefore, packets will not arrive to the base station.

A. Assumptions

Wireless sensor networks are complicated. In order to create a simple solution to detect the selective forwarding attack, we have made some assumptions for the approach detection within significant applications that are susceptible in networks. These assumptions should be acceptable in the sensor networks. First of all, we assume that secured communication should be part of the networks. Second, Malicious nodes should not drop any packets prior to the launching of the selective forwarding attack. Third, we assume that the adversary cannot compromise a sensor node during the deployment. Finally, we assume that authentication broadcast protocols were applied to each sensor node.

B. Selective Forwarding Detection (SFD) Approach

In wireless sensor networks, the rule-based intrusion detection system (IDS) is one of the mechanisms for protection against the security attacks. Rule-based IDS are known as signature-based IDS. The network layer in WSNs is threatened via some attacks such as a wormhole attack, a sinkhole attack and other types of attacks. Our proposal focuses on the selective forwarding attack. We design multi layer approach, which includes three security layers depicted in Figure 3. The first layer is data receiving. In this layer, the important information is filtered and stored. The information includes message fields that are useful to the rule processing. The second layer is rule processing. In this section, rules must be applied to the stored data. 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 detection approach saves energy by using low memory and it takes not much time. It chooses a secure route to transfer data between the source and the base station. Furthermore, SFD approach is reliable, energy efficient, and scalable. All these factors are significant for the sensor nodes. Our approach assumes that the detection accuracy is high, even though the radio condition is poor.

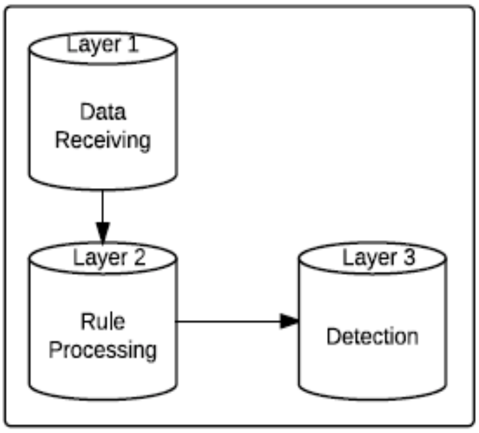

Fig 3. Detection steps in rules based IDS-Redrawn [11]

C. Performance Evaluation

Our approach is estimated through the simulation. We have pointed on malicious detection rate and energy consumption. In the 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.

Energy is an important factor. Figure 4 shows the performance of our approach for the energy consumption. The node cost is about 5J energy with 160 static nodes and 40 mobility nodes. As a result, we used different percentage malicious detection 2%, 4%, 8%, and 16%. Thus, the total of malicious nodes and energy consumption are appearing. During the increasing malicious nodes drop packet, our approach can achieve energy under the overflow of attack. Therefore, it can be accomplished up to 40% malicious nodes.

In Figure 5, the graph shows the energy consumption. The node cost about 5J energy with 200 static nodes and no mobility nodes. It is more than 98% as long as the noise error is 2-4%, and the malicious nodes are under 12%. In fact, we used different percentage malicious detection 2%, 4%, 8%, and 16%. Thus, the total of malicious nodes and energy consumption are appearing. As a result, the detection rate of the malicious nodes will be impacted. We observe that our approach is more efficient when in fact the number of detection nodes increased.

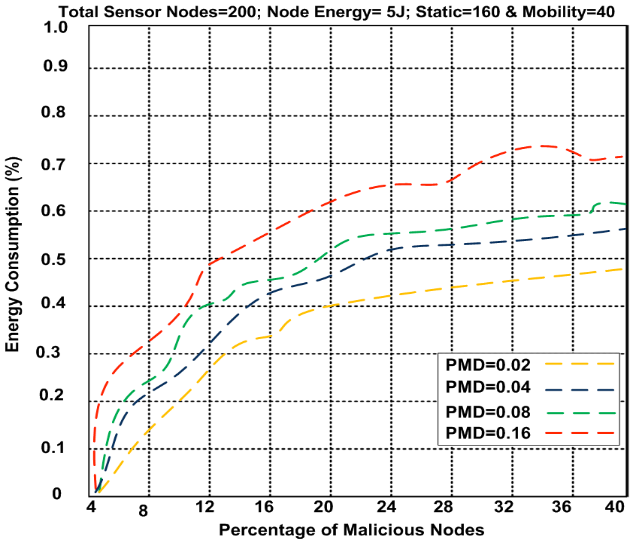

Fig 4. Energy consumption under malicious attacks in WSN

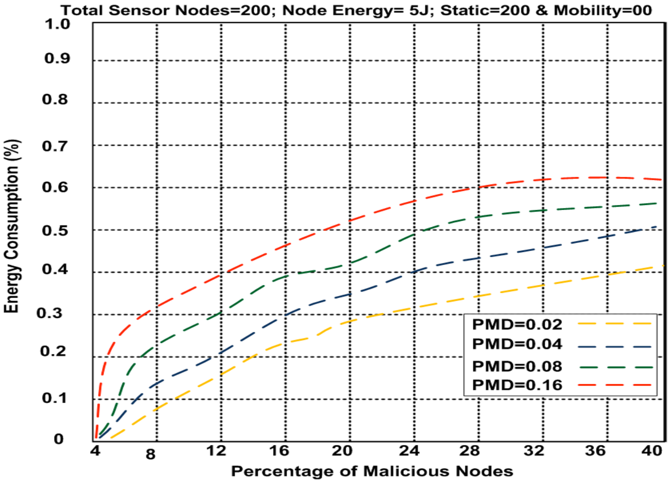

Fig 5. Energy consumption under malicious attacks in WSN

V. Conclusion

Security of WSNs has become increasingly concerning. The use of wireless sensor networks is increasingly employed in environmental, commercial, health and military applications. Secure of packet and the transmission period is the fundamental need in WSNs. Selective forwarding attack might be a sever threats on the wireless networks. In this paper, we present an approach that detection selective forwarding attacks over the WSNs. The monitor sensor nodes detect selective forwarding attacks using detector. Our approach is efficient to detect the attacks. Also, the approach includes reliability, energy efficiency, and scalability. Analysis and simulation show that our approach is more effective when the numbers of detection nodes are 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] Huijuan Deng, Xingming Sun, Baowei Wang, Yuanfu Cao, “Selective Forwarding Attack Detection using Watermark in Wireless Sensor Networks”, International Colloquium on Computing, Communications Control, and Management (2009 ISECS), pp. 109-113.

[10] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth, “Detecting Sinkhole Attack and Selective Forwarding Attack in Wireless Sensor Networks”, ICICS 2009.

[11] 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.

Naser Alajmi

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.

Khaled Elleithy

Dr. 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 2005-2013 International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering virtual conferences.