A New Approach for Detecting and Monitoring of Selective Forwarding Attack in Wireless Sensor Networks

Naser Alajmi and Khaled Elleithy
Computer Science and Engineering Department
University of Bridgeport, Bridgeport, CT

Abstract
Wireless sensor networks (WSNs) are prone to most security attacks. These attacks are such as wormhole attack, sinkhole attack, selective forwarding attack, and Sybil attack. So, each layer in WSNs has some security attacks. Sensor nodes are easily susceptible to security attacks since deployed these nodes are unattended and unprotected. Also, 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. Selective forwarding attack is one of an attack that is not easily detected in the networks layer. In selective forwarding attack, malicious nodes function in the same way as other nodes in the networks. However, it attempts to delete or modify the sensitive information prior to transmitting the packet to the other node. In this paper, we proposed an approach for monitoring this type attack in wireless sensor networks.

Introduction
Sensor nodes use communication to transfer packets from the source to base station by using multi-hop. In selective forwarding attack, malicious nodes have attempted to stop a packet in the network by rejecting message forwarding. It is not easy to detect this type of attack due to unreliable communications. Selective forwarding attacks can be impacted to some routing protocols [1]. This compromised node has a longer radio range and it is simply compromised by an attacker. As a result, sensor nodes have limited communication and computational resources. It has short radio range and it is simply compromised by an attacker. It is compromised node having the same energy at starting point and having maximum energy. Creating a military base scenario. There are some assumptions to detect selective forwarding attacks. Furthermore, we demonstrate the performance of the protocol by showing the reliability and scalability ratio of our approach. We proved our approach with 10 malicious nodes and static nodes. It clearly shows that SFD is able to achieve the same level when the time increased from 0 min to 27 min. Therefore, the new approach is successfully detect the malicious node.

MAC Pool ID 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 and sent to the second layer, which is rule processing layer. 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 as shown in Algorithm 1

Algorithm 1. MAC Pool ID Detection Layer

Rule Processing Layer
The second layer involves rule-based processing. It is the middle layer. Rules are used to define and describe the normal operations for detecting selective forwarding attack. 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 as shown in Algorithm 2. Therefore, the traffic will be accepted and sent to the third layer, which is anomaly detection layer. If the traffic does not satisfy 90% of the rules, the node is considered doubtful and is rejected.

Algorithm 2. Rule Processing Layer

Proposed System
We designed three layers including MAC pool ID layer, rule-based processing layer, and anomaly detection layer as shown in Figure 3. They maintain the safety of data transmission between a source node and base station while detecting selective forwarding attacks. Furthermore, we demonstrate the performance of the protocol by showing the reliability and scalability ratio of our approach. We proved our approach with 10 malicious nodes and static nodes. It clearly shows that SFD is able to achieve the same level when the time increased from 0 min to 27 min. Therefore, the new approach is successfully detect the malicious node.

System Model
The goal of this model is to extend the network lifetime while maintaining the Quality of Service (QoS). The network lifetime is very important metrics of wireless sensor networks. The model also aims to make a balance for the energy utilization therefore, provide longer secure surveillance for the military application.

References