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 layers 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 transferring the packet to other node. In this poster, 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 the packets in a 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]. It compromised node has notable consequences. Based on researchers, limited power and low memory are obstacles that make conventional security measures inappropriate for WSNs [2]. A compromised node selectively drops packets. Malicious nodes work in the same manner such as other nodes in the network field. However, these malicious nodes attempt to find sensitive messages and drop them before sending the entire packets to the next nodes. The attackers make sensor network rely on the redundancy forwarding by using broadcast for data to spread in network. They compromise internal sensor nodes then launch attacks, which it is hard to detect. Also, attackers can refuse to forward the messages to other nodes or drop sensitive information. The majority of WSN protocols do not have the security to prevent simple attacks on the nodes [3].

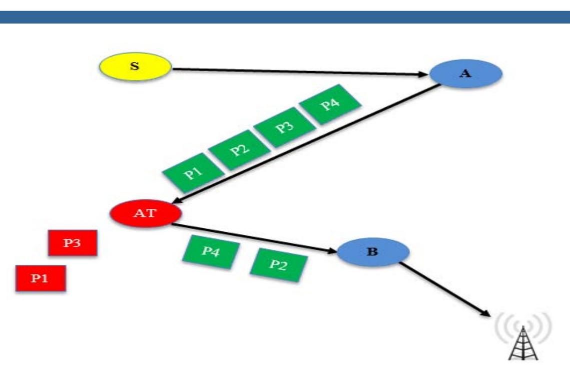

Figure 1. Selective forwarding attack

Sensor node has limited communication and computational resources. It has short radio range and it is simply compromised by an attackers. As a result, in Figure 1, node A sent some packages (P1, P2, P3, and P4) to node B using the route that is between the two nodes. The attacker breaks the link between nodes and steals two packets (P1 and P3), keep the other packets (P2 and P4) transferred to the base station.

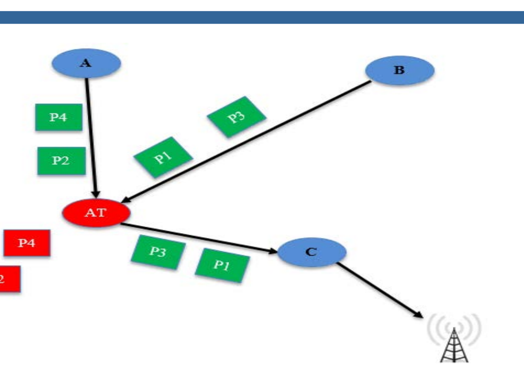

Figure 2. Selective forwarding attack

In Figure 2, there are two sensor nodes A and B transfer some packets to node C. node A send (P2 and P4) and node B send (P1 and P3). The attacker who breaks the link between nodes drop the two packets that sent from node A so the entire packet is not transferred to the base station. However, the other two packets that sent from node B were transferred to node C.

Proposed System

We designed three layers including MAC pool IDs 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 creating a military base scenario. There are some assumptions to detect the selective forwarding attack within certain applications. We assume that all nodes are the same specification. All nodes in the network are having the same energy at starting point and having maximum energy. All nodes can send data to Base station.

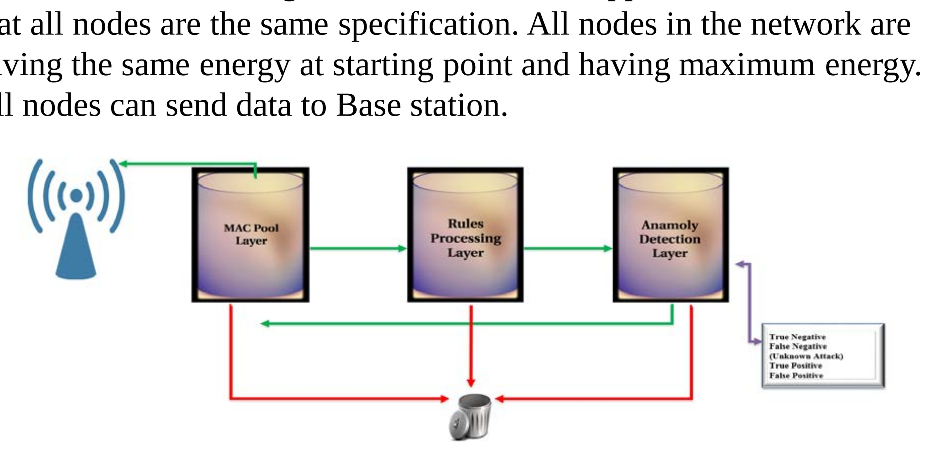

Figure 3. Selective Forwarding Detection-Multi-Layers

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 send it 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 of IDs Layer

```
Input = (MP: Mac Pool)
Network parameter = (SN: sensor node, RT: route, TSN: Total sensor node)
For (SN = 0; SN <= TSN; SN++)
      Set SN = SN + 1
   If SN ∈ MP then
      Set SN = 0 // the node is declared as malicious node not allowed for communication.
         Rejected
         Dropped
   Else if SN = 1 // Node is declared as a legitimate node and allowed for communication
         Accept
         Store
      Set SN = RT
         SN → RP
   End if
   End else
End for
```

Rule Processing Layer

The second layer involves rule-based processing. It is the middle layer. It detects known attacks using rules. These are techniques used to define and describe the normal operations for detecting selective forwarding attacks. 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 send it 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. 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
         Rejected
         Dropped
Else if (SFAT ⊄ RP) then
      Set SN = RT
         SN → AD
   End if
   End else
End for
```

MAC Pool ID 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, which is a false negative, it sends an alert that is a malicious node thus it dropped. Otherwise, the traffic is returned to the pool of MAC IDs by confirming the legitimacy of the node as shown in Algorithm 3.

Algorithm 3. Anomaly Detection Layer Based on IDS

```
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
         FN = 1/N ∑ FN
            M = 1
      Set Alert
         Rejected
         Dropped
   Else if RL2 ∉ AD then
      No Attack
      Set SN = RT
         Return
         SN → MP
         Declared
   End if
   End else
End for
```

System Model

The goal of this model is to extend the network life time 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.

Reliability

$$\prod_{i=0}^{\forall K} RP_{ij}$$

$$RP : RP_{min} \sum_{(i,j\in RP)}^{N} -log \frac{1}{RP_{ij}} - RP_{min} \sum_{(i,j\in RP)}^{N} -log^2$$

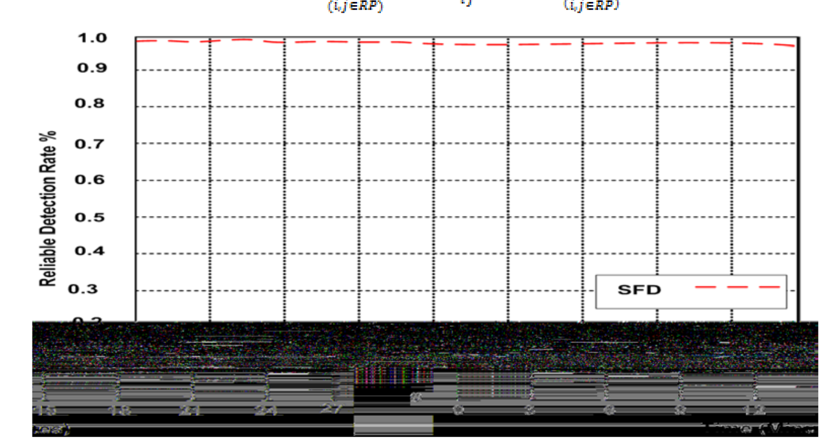

Figure 4. Reliable Detection Rate of SFD Approach

Energy efficiency

$$\Delta E_a = \sum_{k=0}^{n} k(\Delta E_m)$$

$$\Delta E_m = \Delta\beta_t \prod_{u\in S(k)}^{n} Y_{uk} + \Delta\gamma_r \prod_{v\in S(k)}^{n} Z_{vk}$$

$$\Delta E_a = \sum_{k=0}^{n} k \left(\Delta\beta_t \prod_{u\in S(k)}^{n} Y_{uk} + \Delta\gamma_r \prod_{v\in S(k)}^{n} Z_{vk} \right)$$

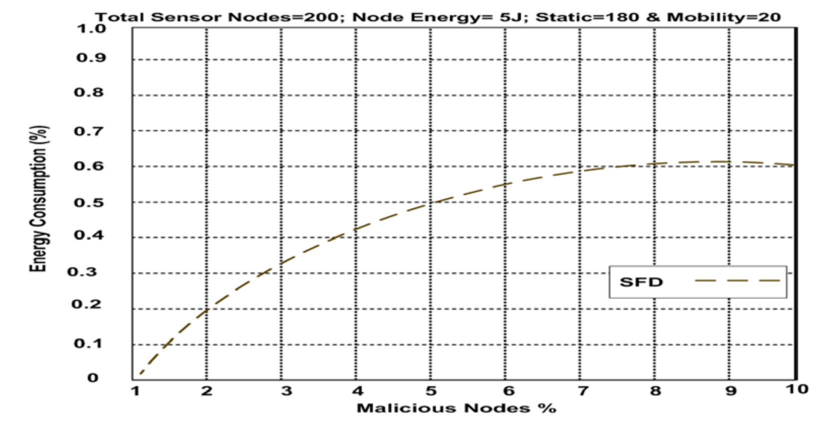

Figure 5. Energy Efficiency of SFD Approach

Scalability

$$S_p^{+} = \sum_{k=0}^{\infty} (k_t) + k_j \times \iint_{i=0\,\&\,j=0}^{N+} (\Delta p)^n + (\nabla p)$$

$$S_p^{-} = \sum_{k=0}^{\infty} (k_t) - k_j \times \iint_{i=0\,\&\,j=0}^{N+} (\Delta p)^n - (\nabla p)$$

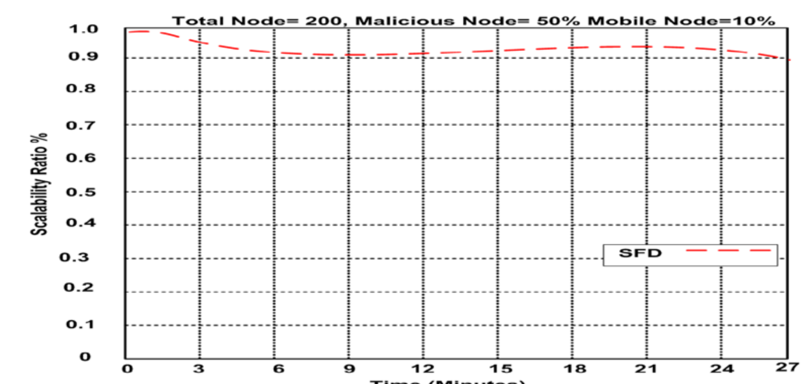

Figure 6. Scalability Ratio of SFD Approach

Results and Discussion

SFD approach is estimated through the simulation. We have pointed on reliable detection rate, energy consumption, and scalability ratio. In the simulation, 200 sensor nodes are deployed in an area network size 800 * 800 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.

Figures 4, 5, and 6 describe the reliable detection rate, energy consumption, and scalability ratio of our approach. We proved our approach with 50% malicious nodes and static nodes. It clearly shows that SFD is stable at almost the same level when the time increased from 0 min to 27 min. Therefore, the new approach is successfully detect the malicious node.

Conclusion

Selective forwarding detection and monitoring objectives are to detect malicious nodes, extend the network's life time, maintaining the Quality of Service (QoS) based on the three factors which are reliability, energy efficiency, and scalability. The new approach contains of three layers including MAC pool IDs layer, rule-based processing layer, and anomaly detection layer. Selective forwarding detection maintains the safety of data transmission between the source and base station. Also, it improves the performance of attack detection such as in a military application. In addition, the approach is demonstrated using Network Simulation (NS2). The network's lifetime is most significant metrics of wireless sensor networks. So, we improved reliability detection, reduced the energy consumptions and developed scalability ratio.

References

1. Halawani, S., Khan, A., Sensors Lifetime Enhancement Techniques in Wireless Sensor Networks - A Survey. Journal of Computing, vol. 2, issue 5, May 2010.
2. Koubaa, A., Alves, M., Tovar , E., Lower Protocol Layers for Wireless Sensor Networks: A Survey. IPP- HURRAY Technical Report, HURRAY-TR-051101. 2012.
3. S. H. Lee, S. Lee, H. Song, and H. S. Lee, "Wireless sensor network design for tactical military applications: remote large-scale environments," in Military Communications Conference, 2009. MILCOM 2009. IEEE, 2009.