Secure Acknowledgement based Misbehavior Detection in WSN (S-ACK)

A. Senthil Kumar* and E. Logashanmugam

1Department of Electronics and Communication Engineering, St. Peter’s University, Chennai - 600054, Tamil Nadu, India; senthilkumarstpeters@gmail.com
2Department of Electronics and Communication Engineering, Sathyabama University, Chennai - 600119, Tamil Nadu, India

Abstract

Security is a most significant challenge for generating a vigorous and consistent sensor networks, such as routing attacks have the capability to separate or isolate a sensor network from its Base Station (BS). Routing misbehavior in the network is that some malicious nodes will play in the route discovery and maintenance process but refuses to forward the data packets. In this paper, we propose Secure Acknowledgement (S-ACK) based Routing Misbehavior Detection in Wireless Sensor Networks (WSN). Objective: The objective of this scheme is to identify the node misbehavior and reduce the overhead in WSN. Methods/Statistical Analysis: This scheme consists of 3 phase such as Acknowledgement (ACK) phase, Secure Acknowledgement (S-ACK) phase and (Misbehavior Verification) MV phase. If the source does not get the acknowledgement from the destination during ACK phase, the source sent the S-ACK packet to the S-ACK phase. S-ACK phase generates the misbehavior report. The Misbehavior Verification phase verifies the misbehavior report is authenticated or not. Finding: The proposed misbehavior detection scheme is capable to attain high detection accuracy for routing attacks. Application/Improvements: The simulation result implies that the SACK provides better Packet Delivery Rate and reduces end-to-end delay.

1. Introduction

Wireless Sensor Network (WSN) is a network comprising of huge number of resource constrained sensor nodes. WSN have become increasingly one of the most promising and interesting areas in recent years. This network is a large system consists of small sized, low power, low-cost sensor devices that gather general or specified information about the physical surroundings.

The interest in WSNs by both the commercial and military continues to develop at a staggering rate. WSNs are susceptible to many types of security attacks owing to multi hop decentralized transmission; open wireless medium and placing in hostile and physically non-protected areas. One of the key features of multi hop distributed operations is that it adds more complication in terms of security attack identification and prevention. Numerous techniques for security attack detection and prevention were implemented for WSNs; though most of the existing solutions are able to manage few safety or security attacks. For example, most secure routing protocols are designed to counter few security attacks. Encryption mechanisms are providing protection only to passive attacks. Thus, it is needed to design a new mechanism to detect and preventing security attacks in WSNs.

A decentralized rule based Intrusion Detection System (IDS) detects many routing attacks includes wormhole, black hole, selective-forwarding and delay attacks. This mechanism has three main phases, namely, data acquisition, rule application and intrusion detection. Applying IDS to static sensor networks establishes a technique to observe over the communications of the sensors’
neighborhood optimally. This technique consists of local agents and global agents. Local agents should examine the local activities and these agents are carried out only when the sensor is active thus, the overheads imposed on the sensor node are low. Global agents should examine the communications of their neighbors. However, not all nodes present in the network may perform this process at the same time, since this process would need sensors to examine the contents of all packets in their radio range.

Intrusion Detection based on Emotional Ants for Sensors (IDEAS) introduced an ant colony mechanism that track of the trespasser trials. This scheme works in conventional machine learning based intrusion detection and provides security in sensor networks. Anomaly Intrusion Detection System (HIDS) detects black hole and selective forwarding attack. In this scheme, the network activities are monitored by using heuristic approach and it classifies them as either normal or malicious. It identifies intrusions based on threshold values. If the node activity is below the threshold value, then it is normal and if it is above the threshold value, the node is an intruder one. Even though in some occasion the well-known security attacks were not detected by this scheme. Intrusion Detection for Routing Attacks focuses on anomaly detection, rather than signature detection. It extensively minimizes the power consumption in power constrained sensor nodes; achieve high detection accuracy with a low false positive rate for each variety of attack. Hybrid IDS (HIDS) was designed to detect intruders in the WSN. The energy consumption gets decreased and efficiently reduces the amount of information in the entire network. Nevertheless, the lifetime of the network can be prolonged by the proposed HIDS. Cross Layer Intrusion Detection System exploits interaction of three layers i.e. Network layer, MAC layer and Physical layer. This IDS scheme identifies the intruders while attempting communication with the network nodes.

Watchdog scheme had proposed for the identification of malevolent node misbehaviors present in the network and it improves the throughput of the network. This method consists of two parts such as Watchdog and Pathrater. If the node present next to the Watchdog node fails to forward the packet within a certain period, then the Watchdog node increases its failure counter. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports it as misbehaving. The Pathrater collaborates with the routing protocols to avoid the reported nodes in future transmission. However, this Watchdog scheme fails to detect malicious misbehaviors during receiver collisions, false misbehavior report, uncertain collisions, inadequate transmission power and partial dropping. Acknowledgement Aware Evidence Theory (AAET) modifies the collected evidence process accurately to assess the BS (Base Station) anonymity in WSNs. This scheme includes the conditions such as probability of ACK correlation and weighting factor.

Trust based Adaptive Acknowledgment (TRAACK) IDS was proposed based on number of active successful deliveries and Kalman filter to guess node. In TRAACK, the path selection was done based on trust strength for multi-hop sensor networks and is lapsed to nodes acting as security agent. Acknowledgement is initiated on selected packets to decrease control overhead. Authenticated Anonymous Secure Routing (AASR) adopts key encrypted onion routing to document a discovered route and encrypted secret message to validate the Route Request Route Reply (RREQ-RREP). In order to prevent intermediate nodes from modifying the routing packet, the RREQ packet per hop was authenticated by using Group signature. The key encrypted onion routing with a route secret verification message is used to prevent intermediate hops from inferring a real destination.

Encryption Key Management to provide security in WSNs is depended on structure and properties of each node. Secured Anonymous Routing with Digital Signature (SARDS) performs routing information verification that exchanged among the sensors in WSN. Elliptical curve cryptography technique had used in SARDS for authentication of all the communicating nodes present in the network. This technique ensures to provide energy-efficient routing in WSNs.

This paper is structured as follows. The proposed idea is discussed in Section 2. The simulation scenario for TRACK and S-ACK is discussed in Section 3. In Section 4 presents conclusion.

### 2. Proposed Method

This section presents the design of S-ACK protocol. We describe our proposed objective to detect the node misbehavior and reduce the overhead of the network. S-ACK consists of 3 phases, namely Acknowledgement phase, Secure Acknowledgment phase and Misbehavior Verification phase.
2.1 Acknowledgement Phase

In this phase, the data packet was sent to the destination from the source through the intermediate nodes. If the destination receives the data packets successfully, it sends back an acknowledgement via same routes but in reverse order. The source gets the acknowledgement within a predefined period of time, the source accepts the acknowledgement, otherwise the source switch to S-ACK phase to generate the misbehavior report in the routing path by sending out an S-ACK packet. Figure 1 shows the example scenario of data transmission path in WSN. Source S transmit the data to destination through the intermediate hops A, B, C. The destination D reaches the data and sends ACK back to the source node.

![Figure 1. Example scenario.](image1)

2.2 Secure Acknowledgement Phase

S-ACK scheme detects misbehaving nodes for every node in the routing path. The principle of S-ACK phase is to detect misbehaving nodes in the routing path that there are three consecutive nodes work together in a group. In this phase, among the three consecutive nodes in the routing path, the third node is necessary to send S-ACK acknowledgment packet to the first node. For example, the data is sent form source to destination; three nodes A, B, C are in intermediate nodes. At First, the node A sends out S-ACK data packet to node B. Then the node B forwards the packet to node C. The node C receives the data packet and then it sends S-ACK to the node B. Then the node B forwards the S-ACK to the node A. If the node A does not receive the S-ACK from the node B within a predefined period, then the node A reports that the node B and C are malevolent. Moreover, a misbehavior report will be generated by node A and is sent to the source node. The source obtains the misbehavior report and it immediately sends to the MV phase for confirming about this misbehavior report.

2.3 Misbehavior Verification Phase

The Misbehavior Verification (MV) is intended to verify the misbehavior report as authenticated or not because the malicious node can generate the false misbehavior report. The MV confirms the S-ACK phase has generated the misbehavior report which is authenticated or not. This MV phase checks for the reception of reported missing packet by the destination node via a different route. To initiate the MV phase, the source node first searches an alternative route to the destination node. If the alternative route is not available, the source node finds a new route. This alternative route is used to avoid the misbehavior reporter node. When the MV packet has received by the destination node, then it searches for the packet was already received. If it is received by the destination already, the misbehavior report is false and then the source decides the misbehaving reporter node as a malicious node. Otherwise, the details given by the misbehavior report is trusted and accepted.

![Figure 2. Flowchart of S-ACK.](image2)
The Figure 2 demonstrates the flowchart of the S-ACK. Initially, the source transmits the data to the destination. The process will be finished when the source receives the ACK from the destination. Otherwise, S-ACK phase sends S-ACK packet for detecting the misbehaving nodes in the routing path and it generates the misbehavior report according to obtain the Secure ACK packet. This misbehavior report is send to the Misbehavior Verification phase for the report is authenticated or not. If the report is authenticated, isolate the misbehaving node otherwise, the reporter is a malicious.

3. Performance Evaluation

A simulation scenario with 30 nodes is deployed and configured as the subterranean wireless network in order to validate the method proposed and their specifications is mentioned in the Table 1. Programming in C++ and Object-oriented Tool Command Language (OTCL) is done to determine the locations of various targeted nodes. The performance of the existing system TRACK is compared with the proposed S-ACK system, which is presented in this paper using simulation results. In order to analyze the performances, the packet delivery rate, Packet Loss Rate, delay rate and throughput are compared through simulations.

Table 1. Simulation parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>60 s</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>30</td>
</tr>
<tr>
<td>Routing Protocol</td>
<td>TRACK and SACK</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>800 x 800</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>250</td>
</tr>
<tr>
<td>Antenna Type</td>
<td>Omni Antenna</td>
</tr>
<tr>
<td>Network Interface Type</td>
<td>Wireless PHY</td>
</tr>
<tr>
<td>Channel Type</td>
<td>Wireless Channel</td>
</tr>
</tbody>
</table>

3.1 Packet Delivery Rate

The Packet Delivery Rate (PDR) can be defined as the ratio between the total packets delivered by the senders and the corresponding receivers in the network. It is given by the Equation 1; where n represents the number of nodes in the network.

\[
PDR = \frac{\sum_{0}^{n} \text{PktReceived}}{\text{time}}
\]  

3.2 Packet Loss Rate

PLR (Packet Loss Rate) is defined as the ratio of the packets lost while senders send their packets to their corresponding receivers. It is given by the Equation 2; where n represents the number of nodes in the network.

\[
PLR = \frac{\sum_{0}^{n} \text{PktLost}}{\text{time}}
\]

3.3 Delay

Average Delay refers to the time difference between packets sent and packets received. It is given by the Equation 3; where n represent the number of nodes in the network.
\[ \text{Delay} = \sum_{n}^{\infty} (\text{PktRecvTime} - \text{PktSentTime}) \]  

The average delay is plotted in Figure 5, which shows that the delay value is lower for the proposed scheme S-ACK than the TRACK. The minimum value of delay means that higher value of the throughput of the network.

![Figure 5. Average delay.](image)

### 3.4 Throughput

Throughput is the total number of packets received by the receivers successfully. The average throughput value is calculated using equation 4, where \( n \) is the representation of the number of nodes present in the network.

\[ \text{Throughput} = \frac{\sum_{n}^{\infty} \text{Pkts Received} (n) \times \text{Pkt Size}}{1000} \]  

Figure 6 show that TRACK has higher average throughput when compared to the S-ACK mechanism. The security activity has improved the network performance greatly.

![Figure 6. Throughput.](image)

### 4. Conclusion

The open medium of WSN makes it vulnerable to various attacks. Various methods are included to diminish the malicious nodes from disrupting working of the network. Acknowledgement based protocol is an effective mechanism used for improving the security of wireless networks also it avoid receiver collision, ambiguous collision. Secure Acknowledgement (S-ACK) based Misbehavior Detection in WSNs proposed here shows improved Packet Delivery Rate and decreased end-to-end delay when compared to TRACK routing. Also, the proposed technique shows more efficiency than the TRACK method as the maliciousness in the network increases.

### 5. References