Results and Discussion

Case Studies

Objectives

- To illustrate a hostile environment case study.
- To illustrate Layerwise Security Framework with SNAuth-SPMAODV for two different scenarios.

Introduction

Mobile ad hoc networks are considered to be the future of wireless networks owing to their specific characteristic features namely practical, simple, self-organization, self-configuration, ease to use and inexpensive when operating in a licence-free frequency band. There are many applications to ad hoc networks, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, having highly dynamic mobility such as:

- In education, ad hoc networks may be deployed for student laptops interacting with the lecturers during classes.
- Health care and telecare systems.
- Inter-Vehicle Communications, ad hoc networks for vehicles, for example, sending instant traffic reports and other information between drivers.
- Electronic email and file transfer.
- Web services that can be used by ad hoc network users in case a node in the network serves as a gateway to the outside world.
- A wide range of military applications, such as a battlefield in an unknown territory where an infrastructure network is not available or impossible to maintain.
- Collaborative work for business environments.
- Emergency search-and-rescue operations, in disaster areas where it is almost impossible to implement an infrastructure network.
- Personal Area Networking (PAN) and Bluetooth.
- Electronic payments from anywhere (i.e. taxi).
- Home Wireless Network and smart homes.

This chapter evaluates Layerwise Security Framework with SNAuth-SPMAODV with concentration to defend against Denial of Service attack in MANET layers. A military case study with two scenarios are introduced: the first scenario study modifies its channel and physical layer settings
for army military devices in an unknown and unstable MANET military environment system with concentration to defend against Denial of Service attack. This scenario combines authentication, authorization, confidentiality and integrity to provide a privacy protection against Denial of Service attack. The second scenario illustrates Layerwise Security Framework with SNAuth-SPMAODV in an unstable and unknown military environment with modified channel and physical layer settings to provide a secure military system to defend against Denial of Service attack.

**Case Study 1: Hostile Environment**

This military case study shows a battlefield in unknown territory, where infrastructure deployment is hard to achieve or maintain; therefore, MANET will be the perfect solution to such a scenario. As already known, the military domain is a very challenging environment described by ambiguity and there is a need to be able to deal with significant and disruptive dynamic changes. The goal of military system is mainly concerned with the ability to satisfy a secure environment for its components, because opponents (enemies) always try their best to break down or destroy the activities. Therefore, the proposed framework concentrates to defend against Denial of Service attack in MANET layers.

This scenario configures a military alliance with three armies (Army1, Army2 and Army3); each one of them has a specific priority upon the other. For instance, the Army1 is categorized as priority one (Highest), while Army2 is categorized as priority three. This categorization is used to provide authorization and authentication to other nodes.

**Simulation setup for Hostile Environment (Scenario One)**

The LaySec framework is simulated using Qualnet5.0 (Bajaj et al., 1999). This simulated environment is defined by the following parameters as shown in Table 10.1 and Table 10.2.

The simulation model consists of two sets of scenario files; topology scenario files and traffic generation pattern files. The topology scenario files define the simulation area and the mobility model of randomly distributed mobile nodes over the simulation time period. On the other hand, the traffic pattern files define the characteristics of data communications, notably, data packet size, packet type, packet transmission rate and the number of traffic flows. In all scenarios, each node is assumed to be equipped with a wireless transceiver operating on 802.11 wireless standards (IEEE 802.11 Standard Committees, 1999). The physical radio frequency characteristics of each wireless transceiver such as the antenna gain, transmit power and signal to noise and interference ratio, are chosen to mimic the commercial Lucent WaveLAN technology with a nominal bit rate of 2Mb/sec and a nominal transmission range of 250 meters with an omni directional antenna. The propagation model used is two-ray propagation model. The reference model used is PRC-999K device (http://www.add.re.kr/), A. D. Tasker, U. S. Military Portable Radios, (http://hereford.ampr.org/history/portable.html).

Each node participating in the network is transmits within the 300m transmission range and each simulation runs for a period of 10000sec. It is worth noting that the above settings could
represent a Hostile Environment MANET scenario. Note that the number of mobile nodes could be larger than the one presented in these scenarios and the operational time could be longer; the values chosen are to keep the simulation running time manageable while still generating enough traces for analysis. Flows of Variable Bit Rate (VBR) unicast data packets, each with size 512 bytes and sending rate of 4 packets/sec have been used as it is important to challenge the proposed method with identical offered loads and environmental conditions in order to enable direct and fair comparison among SNAuth-SPMAODV and AODV.

In this study, mobile nodes move according to the widely used random waypoint mobility model where each node at the beginning of the simulation remains stationary for pause time seconds, then chooses a random destination and starts moving towards it with a speed selected from a uniform distribution $[0, V_{\text{max}}]$. After the node reaches its destination, it again stands still for a pause time interval $t$ sec and picks up a new random destination and speed. This cycle repeats until the simulation terminates. The maximum speed $V_{\text{max}}$ is varied for each simulation scenario from 3m/sec to 18m/sec and pause times of 0 seconds are considered to allow constant mobility. Other simulation parameters used in this research study have been widely adopted in existing performance evaluation studies of MANETs and are summarized below in Table 10.1 and Table 10.2.

Simulation Metrics

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>

TABLE 10.1. SIMULATION METRICS OF LAYSEC FRAMEWORK (Case Study1)
TABLE 10.2: PHYSICAL LAYER MODEL FOR HOSTILE ENVIRONMENTS (Case Study1)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Military devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>30-300 MHz</td>
</tr>
<tr>
<td>Propagation limits</td>
<td>-120 dBm</td>
</tr>
<tr>
<td>Radio propagation model</td>
<td>Free space</td>
</tr>
<tr>
<td>Data rates</td>
<td>200 Kbps</td>
</tr>
<tr>
<td>Transmit power</td>
<td>45 dBm</td>
</tr>
<tr>
<td>Receive sensitivity</td>
<td>-150 dBm</td>
</tr>
<tr>
<td>Reference model</td>
<td>PRC-999K device</td>
</tr>
</tbody>
</table>

Performance Evaluation

The performance analysis of Layerwise security framework with SNAuth-SPMAODV has been conducted using the simulation setup for Hostile Environment as outlined in Table 10.1 and 10.2. The simulation scenarios consist of three different settings, each specifically designed to assess the impact of a particular network operating condition on the performance of the protocols. First, the impact of network density or size is assessed by deploying a different number of mobile nodes over a space of 1500m x 1500m. The second simulation scenario investigates the effects of an offered load on the performance of Layerwise security framework with SNAuth-SPMAODV by varying the number of source destination pairs (flows for short) for each simulation scenario. Lastly, the simulation scenario evaluates the performance impact of node mobility by varying the maximum node speed of a fixed number of mobile nodes in a fixed area of 1500m x 1500m.

Impact of Network Density
This section presents the performance impact of network density on proposed framework is examined. The network density has been varied by deploying 100 and 600 nodes over a fixed area of 1500m x 1500m. Each node in the network moves with a speed randomly chosen between 3 and 25m/sec. 15 identical random source destination connections (i.e. traffic flows), each generating 4 data packets per second, have been used. The packet size is 512 bytes. In the figures presented below, the x-axis represents node density, while the y-axis represents the results of the performance metric of interest.

**Average Packet Delivery Ratio (PDR)**

In Figure 10.1 (a), the Average Packet Delivery Ratio of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV for different network sizes of 100 to 600 nodes are placed in a topology area of 1500m x 1500m. Packet delivery ratio shows how successfully a protocol performs delivering packets from source to destination.

![Figure 10.1(a) Layerwise Security Framework with SNAuth-SPMAODV-Avg. Packet delivery ratio versus number of nodes placed over 1500m x 1500m area](image)

**Average Throughput**

The network throughput is the average rate of successful message delivery over a communication channel.
Figure 10.1(b) shows the throughput of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV. Layerwise Security Framework with SNAuth-SPMAODV show high throughput even for networks with more than 500 nodes compared to AODV. The network throughput of Layerwise Security Framework with SNAuth-SPMAODV could be increased when compared against AODV, SNAuth-SPMAODV in a relatively dense network.

**Average End-to-End Delay**

Figure 10.1(c) shows an average end-to-end delay of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV according to the increase of network density. Layerwise Security Framework with SNAuth-SPMAODV exhibits the lowest end-to-end delay most of the time. AODV has much higher end-to-end delay than proposed method. Layerwise Security Framework with SNAuth-SPMAODV keeps up good performance in delay as the network density becomes high. Layerwise Security Framework with SNAuth-SPMAODV performs poorly in sparse networks. (eg 200 to 300 nodes)
Figure 10.1(c) Layerwise Security Framework with SNAuth-SPMAODV-Avg. End to End Delay versus number of nodes for a network placed in 1500m x 1500m area.

Average Jitter

Figure 10.1(d) depicts the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of Average Jitter over varying network density. Layerwise Security Framework with SNAuth-SPMAODV performs poorly in sparse networks (e.g., 100 to 200 nodes). However, in a relatively dense network, Layerwise Security Framework with SNAuth-SPMAODV outperforms compared to SNAuth-SPMAODV and AODV.
Routing Overhead

Figure 10.1(e) illustrates the routing overhead generated by the proposed framework when the number of nodes is varied. The figure shows that the generated routing overhead in AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased number of nodes. Layerwise Security Framework with SNAuth-SPMAODV performs well compared to AODV and SNAuth-SPMAODV.
4.7.2 Impact of Offered Load

In this section, the effects of offered load on the performance of the proposed framework have been investigated. Simulation runs have been conducted for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV where the offered load is varied by increasing the number of source-destination pairs (flows, for short) from 5 to 30. The topology for each simulation scenario consists of 200 nodes placed randomly on a flat area of 1500m x 1500m, each moving with the random waypoint mobility with speed between 0 and 25m/sec.

Average Packet Delivery Ratio

Figure 10.2 (a) depicts the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of Average Packet Delivery Ratio versus offered loads. The figure shows that the Average Packet Delivery Ratio for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased offered loads. It can also be noticed from the figure that for a given offered load, the generated Average Packet Delivery Ratio of Layerwise Security Framework with SNAuth-SPMAODV is much higher compared with that of AODV, SNAuth-SPMAODV.
Figure 10.2(a) Layerwise Security Framework with SNAuth-SPMAODV-Avg. packet delivery ratio versus offered load for a network of 200 nodes placed in 1500m x 1500m area.

Average Throughput

Figure 10.2(b) reports the results of the network throughput versus offered load for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV. It can be noticed in the figure that the Average throughput achieved by AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV degrade as the offered load increases. (ex 20 and 25 flows); The network throughput in Layerwise Security Framework with SNAuth-SPMAODV is increased when compared with AODV and SNAuth-SPMAODV respectively.
Throughput versus offered load for a network of 150 nodes placed 
in 1500m x 1500m area.

Average End-to-End Delay

Figure 10.2(c) shows the impact of offered load on the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of end-to-end delay. For example, at offered load of 30 flows, the delay incurred by Layerwise Security Framework with SNAuth-SPMAODV is reduced when compared against AODV, SNAuth-SPMAODV respectively.
Average Jitter

Figure 10.2(d) shows Average Jitter plotted against the offered load. Across the offered loads 25 and 30 flows Layerwise Security Framework with SNAuth-SPMAODV achieved higher jitter compared to SNAuth-SPMAODV and AODV. At offered load of 5 to 20 flows, the jitter incurred by Layerwise Security Framework with SNAuth-SPMAODV is reduced when compared against AODV, SNAuth-SPMAODV respectively.

Routing Overhead

Figure 10.2(e) depicts the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of routing overhead versus offered loads. The figure
shows that the generated routing overhead for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased offered loads. It can also be noticed from the figure that for a given offered load, the generated routing overhead of Layerwise Security Framework with SNAuth-SPMAODV is much lower compared with that of AODV, SNAuth-SPMAODV.

4.7.3 Impact of Node Mobility

To evaluate the effects of node mobility on the performance of the proposed framework different maximum node speeds in the network have been considered. The speeds are chosen over a range in order to simulate human slow walk speed and vehicular speed. The speeds ranging from 5m/sec to 10m/sec are assumed to model human movements from a slow walk to a fast run while the speeds ranging from 3m/sec to 18m/sec are assumed to model vehicular motion, from slow movements in urban areas to fast movements on highways. Each simulation run consists of a network of 200 nodes placed over a simulation area of 1500m x 1500m. The offered load has been fixed at 15 flows.

Average Packet Delivery Ratio

Figure 10.3(a) shows the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of Average Packet Delivery Ratio versus node mobility.
The figure shows that the Average Packet Delivery Ratio for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased node speed. Layerwise Security Framework with SNAuth-SPMAODV is increased by approximately 8% when compared against AODV and SNAuth-SPMAODV respectively.

Figure 10.3(a) Layerwise Security Framework with SNAuth-SPMAODV-Avg. Packet delivery ratio versus node mobility for a network of 200 nodes placed in 1500m x 1500m area.

**Figure 10.3(b)** depicts the achieved Average throughput versus node mobility for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV. The figure shows that Average throughput is achieved by Layerwise Security Framework with SNAuth-SPMAODV degrades as the maximum node speed increases. The figure also shows that for a given node speed, the Layerwise Security Framework with SNAuth-SPMAODV slightly outperformed AODV.
The result in Figure 10.3(c) displays the impact of node mobility on the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of end-to-end delay. The figure also shows the performance of Layerwise Security Framework with SNAuth-SPMAODV degrade comparable with AODV and SNAuth-SPMAODV when the mobility is relatively low (e.g. 9m/s and 12 m/s). However, in a relatively high mobility (e.g. 18m/s) the Layerwise Security Framework with SNAuth-SPMAODV outperforms both the AODV, SNAuth-SPMAODV.
Figure 10.3(c) Layerwise Security Framework with SNAuth-SPMAODV-Avg.End to End delay versus node mobility for a network of 200 nodes placed in 1500m x 1500m area.

Average Jitter

Figure 10.3(d) shows Average Jitter plotted against the node speed. As shown in the figure, the Average Jitter decreases from the increased node speed. Across the node speed, Layerwise Security Framework with SNAuth-SPMAODV achieves the lower jitter compared with AODV, SNAuth-SPMAODV.
Routing Overhead

In Figure 10.3(e), the routing overhead generated by Layerwise Security Framework with SNAuth-SPMAODV outperforms both AODV and SNAuth-SPMAODV when plotted against the maximum node speed. As shown in the figure, the routing overhead generated by Layerwise Security Framework with SNAuth-SPMAODV outperforms compared with AODV and SNAuth-SPMAODV increases as the node mobility increases. However, the results in the figure show that Layerwise Security Framework with SNAuth-SPMAODV has a clear performance advantage over SNAuth-SPMAODV and AODV across all node speeds.
Figure 10.3 (e) Layerwise Security Framework with SNAuth-SPMAODV-Routing overhead versus node mobility for a network of 200 nodes placed in 1500m x 1500m area.

Case Study 2: Hostile Environment

This military case study two shows a battlefield in an unknown territory. Therefore, the proposed framework concentrates on a way to defend against Denial of Service attack in MANET layers. As with the first scenario, scenario two configures a military alliance consisting of three armies (army1, army2, army3), and each one of them has a specific priority upon the other. For instance, the
army1 is categorized as priority one (highest), while the, army2 is categorized as priority three. In addition, new elements are defined in this scenario (army4). This categorization is used to provide authorization and authentication to other nodes. The second scenario study illustrates a Layerwise Security Framework with SNAuth-SPMAODV in military environment with modified channel and physical layer settings to provide a secure military system to defend against Denial of Service attack.

**Simulation setup for Hostile Environment (Scenario Two)**

The LaySec framework is simulated using Qualnet 5.0. This simulated environment is defined by the following parameters as shown in Table 10.3 and Table 10.4.

In this case study, the propagation model used is shadowing model. Each node participating in the network is transmits within the 350m transmission range and each simulation runs for a period of 15000sec. Flows of Variable Bit Rate (VBR) unicast data packets, each with size 512 bytes and sending rate of 4 packets/sec have been used as it is important to challenge the proposed method with identical offered loads and environmental conditions in order to enable direct and fair comparison among SNAuth-SPMAODV and AODV. The maximum speed max V is varied for each simulation scenario from 4m/sec to 24 m/sec and pause time of 0 seconds is considered to allow constant mobility. Other simulation parameters used in this research study have been widely adopted in existing performance evaluation studies of MANETs and are summarized below in Table 10.3 and Table 10.4.

**Simulation Metrics**

**TABLE 10.3. SIMULATION METRICS OF LAYSEC FRAMEWORK (Case Study 2)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
</table>

### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Military devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>30-300 MHz</td>
</tr>
<tr>
<td>Propagation limits</td>
<td>-125 dBm</td>
</tr>
<tr>
<td>Radio propagation model</td>
<td>Shadowing</td>
</tr>
<tr>
<td>Data rates</td>
<td>200 Kbps</td>
</tr>
<tr>
<td>Transmit power</td>
<td>50 dBm</td>
</tr>
<tr>
<td>Receive sensitivity</td>
<td>-155 dBm</td>
</tr>
<tr>
<td>Reference model</td>
<td>PRC-999K device</td>
</tr>
</tbody>
</table>

### Performance Evaluation

The performance analysis of Layerwise security framework with SNAuth-SPMAODV has been conducted using the simulation setup for Hostile Environment as outlined in Table 10.3 and 10.4. The simulation scenarios consist of three different settings, each specifically designed to assess the impact of a particular network operating condition on the performance of the protocols. First, the impact of network density or size is assessed by deploying a different number of mobile nodes over a space of 2000m x 2000m. The second simulation scenario investigates the effects of an offered load on the performance of the routing protocols by varying the number of source destination pairs (flows for short) for each simulation scenario. Lastly, the simulation scenario evaluates the performance impact of node mobility by varying the maximum node speed of a fixed number of mobile nodes in a fixed area of 2000m x 2000m.

### Impact of Network Density

In this section, the performance impact of network density on the proposed model is examined. The network density has been varied by changing the number of nodes deployed over a

---

**TABLE 10.4: PHYSICAL LAYER MODEL FOR HOSTILE ENVIRONMENTS (Case Study 2)**

<table>
<thead>
<tr>
<th>Simulator</th>
<th>Qualnet 5.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmitter range</td>
<td>350 meters</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>2 Mbps</td>
</tr>
<tr>
<td>Interface queue length</td>
<td>150 packets</td>
</tr>
<tr>
<td>Traffic type</td>
<td>VBR</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Simulation time</td>
<td>15000 sec</td>
</tr>
<tr>
<td>Number of trials</td>
<td>30</td>
</tr>
<tr>
<td>Topology size</td>
<td>2000m x 2000m</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>50 to 300</td>
</tr>
<tr>
<td>Maximum speed</td>
<td>4m/sec 8m/s, 12m/sec, 24m/sec</td>
</tr>
</tbody>
</table>
2000m x 2000m area in each simulation scenario. Each node moves with a random speed between 4 and 24m/sec. For each simulation trial, 20 identical randomly selected source-destination connections (i.e. traffic flows) are used.

**Average Packet Delivery Ratio (PDR)**

In Figure 10.4 (a), the Average Packet Delivery Ratio of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV for different network sizes of 100 to 300 nodes are placed in a topology area of 2000m x 2000m. Packet delivery ratio shows how successfully a protocol performs in delivering packets from source to destination.

![Figure 10.4(a) Layerwise Security Framework with SNAuth-SPMAODV-Avg. Packet delivery ratio versus number of nodes placed over 2000m x 2000m area](image)

Figure 10.4(a) shows the PDR of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV. Layerwise Security Framework with SNAuth-SPMAODV shows that high PDRs are observed even for networks with more than 200 nodes compared to AODV. For all network sizes from 100 nodes to 300 nodes, Layerwise Security Framework with SNAuth-SPMAODV consistently delivers about 9% more data packets than AODV.

**Average Throughput**

The network throughput is the average rate of successful message delivery over a communication channel.
Figure 10.4(b) shows the throughput of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV. Layerwise Security Framework with SNAuth-SPMAODV shows high throughput even for networks with more than 200 nodes compared to AODV. The network throughput of Layerwise Security Framework with SNAuth-SPMAODV could be increased when compared against AODV, SNAuth-SPMAODV in a relatively dense network.

**Average End-to-End Delay**

Figure 10.4(c) shows an average end-to-end delay of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV according to the increase of network density. Layerwise Security Framework with SNAuth-SPMAODV exhibits the lowest end-to-end delay most of the time. AODV has much higher end-to-end delay than proposed method. Layerwise Security Framework with SNAuth-SPMAODV keeps up bad performance in delay as the network density becomes high (e.g., 300 nodes)
Figure 10.4(c) depicts the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of Average Jitter over varying network density. Layerwise Security Framework with SNAuth-SPMAODV performs poorly in dense networks (eg 250 to 300 nodes). However, in a relatively sparse network, Layerwise Security Framework with SNAuth-SPMAODV outperforms when compared with SNAuth-SPMAODV and AODV.

**Average Jitter**

Figure 10.4(d) shows the end-to-end delay for a network placed in a 2000m x 2000m area. The figure compares AODV with a Denial of Service attack, SNAuth-SPMAODV, and Layerwise Security Framework with SNAuth-SPMAODV. The Layerwise Security Framework performs better in sparse networks but worse in dense networks compared to SNAuth-SPMAODV and AODV.
Routing Overhead

Figure 10.4(e) illustrates the routing overhead generated by the proposed framework when the number of nodes is varied. The figure shows that the generated routing overhead in AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased number of nodes. The performance advantage of Layerwise Security Framework with SNAuth-SPMAODV over SNAuth-SPMAODV and AODV is further increased in dense networks.
Security Framework with SNAuth-SPMAODV - Routing Overhead versus number of nodes placed over 2000m x 2000m area.

Impact of Offered Load

In this section, the effects of offered load on the performance of the proposed framework have been investigated. Simulation runs have been conducted for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV where the offered load is varied by increasing the number of source-destination pairs (flows, for short) from 4 to 24. The topology for each simulation scenario consists of 250 nodes placed randomly on a flat area of 2000m x 2000m, each moving with the random waypoint mobility with speed between 4 and 24m/sec.

Average Packet Delivery Ratio

Figure 10.5 (a) depicts the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of Average Packet Delivery Ratio versus offered loads. The figure shows that the Average Packet Delivery Ratio for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased offered loads. It can also be noticed from the figure that for a given offered load, the generated Average Packet Delivery Ratio of Layerwise Security Framework with SNAuth-SPMAODV is much higher compared with that of AODV, SNAuth-SPMAODV.
Figure 10.5(a) Layerwise Security Framework with SNAuth-SPMAODV-Avg. packet delivery ratio versus offered load for a network of 250 nodes placed in 2000m x 2000m area.

**Average Throughput**

Figure 10.5(b) reports the results of the network throughput versus offered load for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV. For example, at 24 flows; the network throughput in Layerwise Security Framework with SNAuth-SPMAODV is increased when compared AODV and SNAuth-SPMAODV respectively.

![Layerwise Security Framework with SNAuth-SPMAODV-Avg. packet delivery ratio versus offered load for a network of 250 nodes placed in 2000m x 2000m area.](image)

**Layerwise Security Framework with SNAuth-SPMAODV under Denial of Service attack**

Figure 10.5 (b) Layerwise Security Framework with SNAuth-SPMAODV-Avg. Throughput versus offered load for a network of 250 nodes placed in 2000m x 2000m area.
**Average End-to-End Delay**

Figure 10.5(c) shows the impact of offered load on the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of end-to-end delay. For example, at offered load of 24 flows, the delay incurred by Layerwise Security Framework with SNAuth-SPMAODV is reduced when compared against AODV, SNAuth-SPMAODV respectively.

![Chart showing end-to-end delay versus offered load](image)

**Figure 10.5(c)** Layerwise Security Framework with SNAuth-SPMAODV-Avg. End to End Delay versus offered load for a network of 250 nodes placed in 2000m x 2000m area.

**Average Jitter**

Figure 10.5(d) shows Average Jitter plotted against the offered load. Across the offered loads 16 and 20 flows Layerwise Security Framework with SNAuth-SPMAODV achieved slightly higher jitter.
compared with SNAuth-SPMAODV and AODV. At offered load of 4 to 12 flows, the jitter incurred by Layerwise Security Framework with SNAuth-SPMAODV is reduced when compared against AODV and SNAuth-SPMAODV respectively.

Figure 10.5(d) Layerwise Security Framework with SNAuth-SPMAODV-Avg. Jitter versus offered load for a network of 250 nodes placed in 2000m x 2000m area.

Routing Overhead

Figure 10.5(e) depicts the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of routing overhead versus offered loads. The figure shows that the generated routing overhead for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased offered loads. In figure10.5(e), for example, at a high offered load (e.g. 24 flows), the routing overhead in Layerwise Security Framework with SNAuth-SPMAODV is reduced when compared against AODV, SNAuth-SPMAODV respectively.
4.7.3 Impact of Node Mobility

To evaluate the effects of node mobility on the performance of the proposed framework, different maximum node speeds in the network have been considered. The speeds are chosen over a range in order to simulate human slow walk speed and vehicular speed. The speeds ranging from 4m/sec to 24m/sec are assumed to model human movements from a slow walk to a fast run while the speeds ranging from 4m/sec to 24m/sec are assumed to model vehicular motion, from slow movements in urban areas to fast movements on highways. Each simulation run consists of a network of 250 nodes placed over a simulation area of 2000m x 2000m. The offered load has been fixed at 20 flows.

Average Packet Delivery Ratio

Figure 10.6(a) shows the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of Average Packet Delivery Ratio versus node mobility. The figure shows that the Average Packet Delivery Ratio for AODV,
SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV increases with increased node speed. Layerwise Security Framework with SNAuth-SPMAODV is increased by approximately 5% to 10% when compared against AODV and SNAuth-SPMAODV respectively.

![Graph showing packet delivery ratio versus node mobility](image)

**Figure 10.6(a)** Layerwise Security Framework with SNAuth-SPMAODV-Avg Packet delivery ratio versus node mobility for a network of 250 nodes placed in 2000m x 2000m area.

Average Throughput

Figure 10.6 (b) depicts the achieved Average throughput versus node mobility for AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV. The figure also shows that for a given node speed, the Layerwise Security Framework with SNAuth-SPMAODV slightly outperformed AODV.
End-to-End Delay

The result in Figure 10.6(c) displays the impact of node mobility on the performance of AODV, SNAuth-SPMAODV and Layerwise Security Framework with SNAuth-SPMAODV in terms of end-to-end delay. The figure also shows the performance of Layerwise Security Framework with SNAuth-SPMAODV comparable with that AODV, SNAuth-SPMAODV when the mobility is relatively low. However, in a relatively high mobility (e.g. 24m/s) the Layerwise Security Framework with SNAuth-SPMAODV outperforms when compared to AODV and SNAuth-SPMAODV.
Figure 10.6(c) Layerwise Security Framework with SNAuth-SPMAODV-Avg. End to End delay versus node mobility for a network of 250 nodes placed in 2000m x 2000m area.

Average Jitter

Figure 10.6(d) shows Average Jitter plotted against the node speed. As shown in the figure, the Average Jitter decreases from the increased node speed. Across the node speed, Layerwise Security Framework with SNAuth-SPMAODV achieved the lower jitter compared with AODV, SNAuth-SPMAODV.
Routing Overhead

In Figure 10.6(e), the routing overhead generated by Layerwise Security Framework with SNAuth-SPMAODV outperforms both the AODV and SNAuth-SPMAODV when plotted against the maximum node speed. As shown in the figure, the routing overhead generated by Layerwise Security Framework with SNAuth-SPMAODV outperforms both the AODV, SNAuth-SPMAODV increases as the node mobility increases. However, the results in the figure show that Layerwise Security Framework with SNAuth-SPMAODV has a clear performance advantage over SNAuth-SPMAODV and AODV across all node speeds.
Conclusion

In this chapter, two different case studies have been provided with specific concentration on a military case study in an unknown and an unsecure territory with different channel and physical layer settings for each scenario. Scenario one defines three Army countries in a battlefield and this scenario shows the implementation and evaluation of Layerwise Security Framework with SNAuth-SPMAODV to defend against Denial of Service attack. Meanwhile, scenario two defines three Army countries with new elements and this scenario shows the implementation and evaluation of Layerwise Security Framework with SNAuth-SPMAODV to defend against Denial of Service attack.

Summary of Research

In recent years, Mobile Ad hoc Network (MANET) has received much attention due to self-design, self-maintenance, and cooperative environments. In MANET, all the nodes are mobile nodes and the topology changes rapidly without any predefined infrastructure. With the increase of portable devices as well as progress in wireless communication, ad hoc networking is gaining importance with
the increasing number of widespread applications. Ad hoc networking can be deployed wherever there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use. The potential deployments of MANETs exist in many scenarios, for example in situations where the infrastructure is not feasible such as disaster relief, cyclone, battlefield etc.

Their natural characteristics make them vulnerable to passive and active attacks. Particularly, Denial of Service attack is one such severe attack against MANET Layers which is a challenging one to defend against. Hence security is an important challenge while deploying MANET. So security issues are analyzed for individual layers namely application layer, transport layer, network layer, link layer and physical layer. The ultimate goal of the security solution for MANETs is to provide security services, such as confidentiality, integrity, authentication, non-repudiation, and availability. In order to achieve these goals, the security solution should provide complete protection spanning the entire protocol stack. Key management is the central component of security. The security keys must be generated and distributed to the communicating nodes in a secure manner so that unauthorized users cannot compromise the information exchanged. There is no solution that provides layer wise security which is a major challenge for Mobile Adhoc networks.

The goal of this research is to incorporate three security features (Secure neighbor authentication and Layerwise Security techniques and Multipath routing) into LaySec framework while maintaining network performance sufficient to operate in hostile environment. It uses Layerwise security techniques to protect nodes from multilayer attacks called Denial of Service attacks. It uses secure neighbor authentication to provide neighboring nodes exchange messages to discover and authenticate each other. The Adhoc On demand Distance Vector (AODV) protocol is modified to utilize all discovered routes instead of the shortest route to balance the network load across multiple paths. The multiple security levels of LaySec make it very robust against Denial of Service attacks in hostile environment.

The proposed methods are:

The integration of strict priority Multipath AODV with secure neighbor authentication that facilitates neighboring nodes exchange messages to discover and authenticate each other. Thus this phase defend against Denial of Service attacks and increase network throughput. It provides security mechanism like message integrity, mutual authentication, and non-repudiation.

The proposed Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing) with Session Initiation Protocol (SIP) provides application layer and network layer security and it is robust against Denial of Service attack.
The proposed SNAuth-SPMAODV with Wireless Transport Layer Security (WTLS) to defend against Denial of Service (DoS) attack and it also provides authentication, privacy and integrity of packets in routing, end-to-end communications through data encryption, packet loss and transport and network layers of MANET.

The proposed Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing) with IPSec is robust against Denial of Service attack and it also provides security services for both routing information and data message at network layer in MANET.

The proposed SNAuth-SPMAODV combines with CCMP-AES model to defend against Denial of Service attack and it provides confidentiality and authentication of packets in both network and data link layers of MANETs.

The proposed model combines SNAuth-SPMAODV routing protocol and spread spectrum technology Direct Sequence Spread Spectrum (DSSS) to defend against signal jamming denial-of-service attacks in physical layer and network layer for MANET.

From the simulation results it is observed that the proposed approaches have shown better results in terms of Average packet delivery ratio, Average throughput, Average end to end delay, Average jitter and Routing Overhead. The proposed Layerwise Security framework maintaining network performance is sufficient to operate in hostile environment. The multiple security levels of LaySec make it very robust against Denial of Service attacks in hostile environment.

**Recommendations for Future Research**

This Proposed Layerwise Security Framework makes it very robust against Denial of Service attacks that can be well suited for hostile environment. This research has been conducted via simulation. One possible area of future research would be to implement this framework in a test bed of mobile network devices. Another area of future research is the use of LaySec to secure ad-hoc networks of mobile sensors deployed in a hostile environment. In future, LaySec Framework can be incorporated to defend other severe attacks in hostile environment.