# LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Mobile Ad Hoc Network</td>
<td>2</td>
</tr>
<tr>
<td>1.2</td>
<td>Major Categories of Wireless Networks</td>
<td>3</td>
</tr>
<tr>
<td>1.3</td>
<td>Applications of MANET</td>
<td>5</td>
</tr>
<tr>
<td>1.4</td>
<td>Historical Byzantine Attacks in fall of Roman Empire</td>
<td>16</td>
</tr>
<tr>
<td>1.5</td>
<td>Byzantine Attacks</td>
<td>18</td>
</tr>
<tr>
<td>1.6</td>
<td>Byzantine Black Hole Attack</td>
<td>20</td>
</tr>
<tr>
<td>1.7</td>
<td>Colluding Byzantine Attacks</td>
<td>21</td>
</tr>
<tr>
<td>1.8</td>
<td>Byzantine Network Overlay Attack</td>
<td>22</td>
</tr>
<tr>
<td>2.1</td>
<td>SM(1) Algorithm by Lamport et al. with Commander as the Traitor</td>
<td>29</td>
</tr>
<tr>
<td>2.2</td>
<td>Multipath Message Transmission of SMT</td>
<td>34</td>
</tr>
<tr>
<td>2.3</td>
<td>Binary Search Used in ODSBR</td>
<td>37</td>
</tr>
<tr>
<td>2.4</td>
<td>Feed Back and Fault Detection Module of MANET Layers</td>
<td>46</td>
</tr>
<tr>
<td>3.1</td>
<td>Overall Architecture of Secure Communication</td>
<td>49</td>
</tr>
<tr>
<td>3.2</td>
<td>Multipath Message Transmissions</td>
<td>59</td>
</tr>
<tr>
<td>3.3</td>
<td>MANET with Worm Hole as Articulation Point</td>
<td>60</td>
</tr>
<tr>
<td>3.4</td>
<td>Connector Beacon Frames</td>
<td>61</td>
</tr>
<tr>
<td>3.5</td>
<td>Secure Data Dispersal</td>
<td>62</td>
</tr>
<tr>
<td>3.6</td>
<td>Comparison of Packets Received</td>
<td>66</td>
</tr>
<tr>
<td>3.7</td>
<td>Comparison of Packets Lost</td>
<td>66</td>
</tr>
<tr>
<td>4.1</td>
<td>Connected Graph</td>
<td>75</td>
</tr>
<tr>
<td>4.2</td>
<td>Simple Graph for studying Characteristic set</td>
<td>76</td>
</tr>
<tr>
<td>4.3</td>
<td>Networks without Adversaries</td>
<td>80</td>
</tr>
<tr>
<td>FIGURE NO.</td>
<td>TITLE</td>
<td>PAGE NO.</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>4.4</td>
<td>Wormhole or Colluding Node Attacks</td>
<td>82</td>
</tr>
<tr>
<td>4.5</td>
<td>Byzantine Black Hole Attack</td>
<td>83</td>
</tr>
<tr>
<td>5.1</td>
<td>Triple Layer Security against Byzantines Attacks</td>
<td>89</td>
</tr>
<tr>
<td>6.1</td>
<td>Network without Adversaries</td>
<td>98</td>
</tr>
<tr>
<td>6.2</td>
<td>Byzantine Wormhole Attack</td>
<td>98</td>
</tr>
<tr>
<td>6.3</td>
<td>Byzantine Black hole Attack</td>
<td>98</td>
</tr>
<tr>
<td>6.4</td>
<td>Disconnected Network by Wormhole Attack</td>
<td>101</td>
</tr>
<tr>
<td>6.5</td>
<td>Link status after Byzantine Black Hole Attack</td>
<td>101</td>
</tr>
<tr>
<td>6.6</td>
<td>Comparisons with System Not Resilient to Colluding Nodes</td>
<td>104</td>
</tr>
<tr>
<td>6.7</td>
<td>Comparison with System Resilient to Colluding Nodes</td>
<td>105</td>
</tr>
</tbody>
</table>