The security issues related to transport layer are authentication, secure end-to-end communication through data encryption, delays, packet loss and so on. The transport layer protocols in MANET provide end-to-end connection, reliable packet delivery, flow control, congestion control and Denial of Service attacks. The proposed model combines Transport layer protocol WTLS with SNAuth-SPMAODV to defend against Denial of Service (DoS) attack and it also provides authentication, privacy and integrity of packets in both network and transport layers of MANET.

6.1 Wireless Transport Layer Security (WTLS)

The transport layer protocols in MANET provide end-to-end connection, reliable packet delivery, flow control, congestion control and clearing of end-to-end connection. Like TCP protocol in the Internet model, the nodes in a MANET are also vulnerable to the Denial of Service (DoS) attacks. The extensive use of mobile communication has created an important demand for value-added services. WAP (Wireless Application Protocol) is a framework for developing applications to run over wireless networks. WAP is developed by an international industry-wide organization called the WAP Forum. WTLS (Wireless Transport Layer Security) is the security protocol of the WAP protocol suite. WTLS operates over the transport layer and provides end-to-end security, where one end is the mobile client, and the other end is the WAP gateway. WAP gateway acts as a proxy of the mobile client to access an application server hosted somewhere on the Internet (Saarinen, 1999).

6.1.1 WTLS Architecture

WTLS again can be divided into four specialized protocols. The handshake protocol is by definition responsible for client-server handshake during which the client and the server determine a set of security parameters to be used in the following message exchanges. These parameters contain the bulk encryption algorithm, the MAC algorithm, the compression algorithm, the 20-byte master secret, the 16-byte client random, the 16-byte server random, the time interval of key refresh, and the sequence number mode (http://www1.wapforum.org/tech/).

The alert protocol specifies the type of alert messages and the ways to handle them. There are three types of alerts: warning, critical, and fatal. Alerts can be initiated by either the client or the server whenever an error is detected during the handshake, authentication, decryption, or data integrity verification. Fatal alerts obviously lead to the termination of the connection. The application protocol defines the interface between the transaction layer and WTLS. The change cipher specific protocol is usually used in the end of the handshake when the client and the server have agreed upon the security parameters.

Handshake Procedure
The clients initiates the handshake by sending a Hello message together with some security settings such as the trusted certificates and supported encryption and MAC algorithms. Upon receipt of this message, the server sends server hello, server certificate, server key exchange messages. Some required parameters for generating the pre-master secret may not be found in the server certificate. The server key exchange message is to provide this kind of information. If the server needs to authenticate the client, it will also send a certificate request message. Following these messages is the server hello done message. Once the client receives the server hello done message stating the chosen algorithms, it will sends client certificate message if required. Client key exchange message contains the pre-master secret encrypted by the server’s public key. Then the client sends the finish message together with the message digest of all the previously exchanged information signed by the client to ensure that this sensitive information has not been tampered by any intruders. After verifying the message digest, the server responds with finish message and cipher change message if everything is fine. Otherwise, the connection will not be established.

There are also modified ways of handshakes serving different purposes. For example, if the client wants to resume a session, only the session ID is needed in the message exchanges. If both parties have the common session ID, the previously negotiated settings for this session can be reused. This special handshake can largely reduce the number of message exchanges.

**Method of Achieving Security**

Authentication is mainly achieved by the server and client certificates. Currently, WTLS supports X.509v3 and X9.68 certificates. Unlike traditional ones, these certificates have smaller sizes for wireless communications with narrow bandwidths. Key exchange can be achieved with RSA, Diffie-Hellman, or elliptic curve Diffie-Hellman algorithms. The client first suggests acceptable algorithms. The server decides which one actually to use.

The bulk encryption algorithms currently supported by WTLS are RC5 with 40, 56 or 128 bit keys, DES with 40 or 56 bit keys, 3DES, IDEA with 40, 56 or 128 bit keys, and ECC according to Jormalainen’s paper. ECC is the preferred algorithm due to its efficiency with relatively small key space. Steam ciphers are not accepted. The encryption key, IV, and MAC key are generated from the keystreams. Keystreams are previously calculated from the master secret, an expansion label, the packet sequence number, and the server and client random values using a pseudo-random function. The master secret is computed from the pre-master secret and the random values using a pseudo-random function. The sequence number makes the keystream vary between consecutive packets. To verify data integrity, WTLS supports SHA-1, MD5, and SHA_XOR_40, a rather incompetent algorithm that cannot really protect messages from unauthorized modifications (Wireless Application Protocol, http://www.wapforum.org).

**6.2 SNAuth-SPMAODV with WTLS**
The proposed method reduces dependency on single nodes and routes; it discovers multiple paths between sender and receiver nodes. It has the advantages of a multipath protocol without introducing extra packets into the network and authenticates the neighbor offering robustness in a secured MANET. It can be used to offset the dynamic and unpredictable configuration of ad-hoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth in military environment. The proposed model combines SNAuth-SPMAODV Routing 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. SNAuth-SPMAODV with WTLS is found to be a good security solution even with its known security problems.

6.3 Performance Evaluation

Impact of Network Density

This section examines the impact of network density on the performance of proposed method. The network density has been varied by changing the number of nodes deployed over a 1000m x 1000m area of each simulation scenario. Each node in the network moves with a random speed chosen between 0 and 20m/sec. For each simulation trial, 10 identical randomly selected source-destination connections (i.e. traffic flows) are used.

Average Packet Delivery Ratio (PDR)

From the Figure 6.1(a), it is shown that the proposed scheme (WTLS-SNAuth-SPMAODV) gives better Packet Delivery Ratio compared to SNAuth-SPMAODV without WTLS, with varying network size and malicious nodes. Hence the number of data packets dropping by malicious node has been minimized. Thus, SNAuth-SPMAODV with WTLS improves the average packet delivery ratio.
Figure 6.1(a) SNAuth-SPMAODV-WTLS-Avg.Packet delivery ratio versus number of nodes placed over 1000m x 1000m area

**Average Throughput**

Figure 6.1(b) demonstrates the throughput for SNAuth-SPMAODV (without WTLS) and SNAuth-SPMAODV with WTLS. It is clear that SNAuth-SPMAODV with WTLS has a good performance compared to SNAuth-SPMAODV without WTLS, with varying network size and malicious nodes. As shown in Figure 6.1(b), SNAuth-SPMAODV with WTLS outperforms compared to SNAuth-SPMAODV without WTLS when the network is relatively dense.

Figure 6.1(b) SNAuth-SPMAODV-WTLS-Throughput versus number of nodes placed over 1000m x 1000m area

**Average End-to-End Delay**
Figure 6.1(c) shows that the proposed method (WTLS-SNAuth-SPMAODV) gives lowest End to End delay than the SNAuth-SPMAODV without WTLS protocol. For example, in networks with 200 to 1400 nodes, WTLS-SNAuth-SPMAODV improves the performance significantly.

![Figure 6.1(c) SNAuth-SPMAODV-WTLS-Avg.End to End delay versus number of nodes placed over 1000m x 1000m area](image)

**Average Jitter**

Figure 6.1(d) depicts the performance of SNAuth-SPMAODV with WTLS for denial of Service attack without WTLS in terms of Average Jitter over varying network density. However, in a relatively dense network, SNAuth-SPMAODV with WTLS for denial of Service attack outperforms SNAuth-SPMAODV without WTLS.

![Figure 6.1(d) SNAuth-SPMAODV-WTLS-Average Jitter versus number of nodes placed over 1000m x 1000m area](image)

**Routing Overhead**

Figure 6.1(e) illustrates the routing overhead generated by the proposed protocols when the number of nodes is varied. The figure shows that the generated routing overhead in SNAuth-SPMAODV with WTLS for denial of Service attack without WTLS protocols increases with increased...
number of nodes. For instance, compared with SNAuth-SPMAODV with WTLS and SNAuth-SPMAODV without WTLS the generated routing overhead in SNAuth-SPMAODV can be reduced when the number of nodes is relatively small. For example, in figure 6.1(e), when the number of nodes is increased to 200 to 1400 nodes, the generated routing overhead in SNAuth-SPMAODV with WTLS could be less than SNAuth-SPMAODV without WTLS respectively.

Figure 6.1(e) SNAuth-SPMAODV-WTLS- Routing Overhead versus number of nodes placed over 1000m x 1000m area.

Impact of Offered Load

This section demonstrates the effects of offered load on the performance of SNAuth-SPMAODV with WTLS and without WTLS. In this scenario, 150 nodes are placed over 1000m x 1000m and each node is moving according to the random way point mobility model with a maximum speed of 20m/s. To investigate the impact of traffic load, the numbers of source-destination connections (or flows) have been varied 1 to 40 flows. The source destination pair for each of the connections is hosen at random and consists of a CBR flow from the source to destination.

Average Packet Delivery Ratio

Figure 6.2(a) depicts the performance of SNAuth-SPMAODV with WTLS and SNAuth-SPMAODV without WTLS in terms of Average Packet Delivery Ratio versus offered loads. The figure shows that the Average Packet Delivery Ratio for SNAuth-SPMAODV with WTLS increases with increased offered loads. In figure 6.2(a) for example, at a high offered load (e.g. 40 flows), in Average Packet Delivery Ratio SNAuth-SPMAODV with WTLS is increased by approximately 5% to 10% when compared against SNAuth-SPMAODV without WTLS respectively.
Figure 6.2(a) SNAuth-SPMAODV-WTLS-Avg.packet delivery ratio versus offered load for a network of 150 nodes placed in 1000m x 1000m area.

Average Throughput

Figure 6.2(b) depicts the results of the achieved average throughput versus offered load for SNAuth SPMAODV with WTLS for Denial of service attack and without WTLS. For example, at 40 flows, the network throughput in SNAuth-SPMAODV with WTLS is increased when compared with SNAuth-SPMAODV without WTLS respectively.

Figure 6.2(b) SNAuth-SPMAODV-WTLS-Avg.Throughput versus offered load for a network of 150 nodes placed in 1000m x 1000m area.

Average End-to-End Delay
The results in Figure 6.2(c) illustrate the performance of SNAuth-SPMAODV with WTLS and without WTLS in terms of end-to-end delay when the number of nodes in the network is varied. The performance difference among SNAuth-SPMAODV with WTLS and without WTLS is noticeable at offered loads greater than 25 flows. For example, at offered load of 40 flows, the delay incurred by SNAuth-SPMAODV with WTLS reduced when compared against WTLS respectively.

![SNAuth-SPMAODV-WTLS-Avg.End to End Delay versus offered load for a network of 150 nodes placed in 1000m x 1000m area.](image)

**Figure 6.2(c) SNAuth-SPMAODV-WTLS-Avg.End to End Delay versus offered load for a network of 150 nodes placed in 1000m x 1000m area.**

**Average Jitter**

The results presented in Figure 6.2(d) show the performance behavior of proposed method in terms of average jitter versus the offered load. As shown in the figure, the Average Jitter decreases with increased channel contention and packet collisions resulting from the increased number of source destination pairs. Across the offered loads, SNAuth-SPMAODV with WTLS achieved the lower jitter compared with SPMAODV without WTLS.

![SNAuth-SPMAODV](image)

**WTLS in SNAuth-SPMAODV with Denial of Service attack**

![SNAuth-SPMAODV](image)

**WTLS in SNAuth-SPMAODV with Denial of Service attack**
Routing Overhead

Figure 6.2(e) shows the effects of offered load on the performance of SNAuth-SPMAODV with and without WTLS in terms of routing overhead. The figure shows that the generated routing overhead for SNAuth-SPMAODV with WTLS increases with increased offered loads. In figure 6.2(e) for example, at a high offered load (e.g. 40 flows), the routing overhead in SNAuth-SPMAODV with WTLS is reduced when compared against SNAuth-SPMAODV without WTLS respectively.

Impact of Node Mobility

To evaluate the effects of node mobility on the performance of the proposed protocols, 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 1m/sec to 5m/sec are assumed to model human movements from a slow walk to a fast run while the speeds ranging from 10m/sec to 40m/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 150 nodes placed over a simulation area of 1000m x 1000m. The offered load has been fixed at 10 flows.

**Average Packet Delivery Ratio**

Figure 6.3 (a) illustrates the Packet Delivery Ratio generated by SNAuth-SPMAODV with and without WTLS when the mobility of nodes is varied. The figure shows that the Average Packet Delivery Ratio for SNAuth-SPMAODV with and without WTLS increases with increased node speed. From the figure shows that the generated Average Packet Delivery Ratio of SNAuth-SPMAODV with WTLS is much higher compared with that of SNAuth-SPMAODV without WTLS. SNAuth-SPMAODV with WTLS is increased by approximately 5% to 10% when compared against SPMAODV without WTLS respectively when the node mobility is increased from 1m/sec to 40m/sec.

[Figure 6.3(a) SNAuth-SPMAODV-WTLS-Avg.packet delivery ratio versus node mobility
for a network of 150 nodes placed in 1000m x 1000m area.]

**Average Throughput**

Figure 6.3 (b) describes the achieved Average throughput versus node mobility for SNAuth-SPMAODV with and without WTLS. The figure shows that Average throughput is achieved by SNAuth-SPMAODV with WTLS degrades as the maximum node speed increases. The figure also shows that for a given node speed, the SNAuth-SPMAODV with WTLS slightly outperformed SNAuth-SPMAODV without WTLS.
Figure 6.3(b) SNAuth-SPMAODV-WTLS-Avg.Throughput versus node mobility for a network of 150 nodes placed in 1000m x 1000m area.

End-to-End Delay

The results in Figure 6.3(c) depict the impact of node mobility on the performance of SNAuth-SPMAODV with and without WTLS in terms of end-to-end delay. The figure also shows the performance of SNAuth-SPMAODV with WTLS comparable with that of SNAuth-SPMAODV without WTLS when the mobility is relatively low. However, in a relatively high mobility (e.g. 40m/s) the SNAuth-SPMAODV with WTLS outperforms both SNAuth-SPMAODV without WTLS.
Average Jitter

Figure 6.3(d) plots the Average Jitter generated by proposed method against the maximum node speed. The results depict that Average Jitter decreases from the increased node speed. Across the node speed, SNAuth-SPMAODV with WTLS achieved the lower jitter compared with SNAuth-SPMAODV without WTLS.

Routing Overhead

In Figure 6.3(e), the routing overhead generated by SNAuth-SPMAODV with WTLS and without WTLS is plotted against the maximum node speed. As shown in the figure, the routing
overhead generated by SNAuth-SPMAODV with WTLS and without WTLS increases as the node mobility increases. However, the results in the figure show that SNAuth-SPMAODV with WTLS has a clear performance advantage over SNAuth-SPMAODV without WTLS across all node speeds.

Figure 6.3(e) SNAuth-SPMAODV-WTLS-Routing Overhead versus node mobility for a network of 150 nodes placed in 1000m x 1000m area.

6.4 Conclusion

The primary focus of this work is to provide transport layer security for authentication, securing end-to-end communications through data encryption and to provide security services for both routing information and data message at network layer. It also handles delay and packet loss. The proposed approach minimizes the packet dropping by Denial of Service attack (DoS) in the network by applying WTLS in SNAuth-SPMAODV routing protocols and compares the results with SNAuth-SPMAODV without WTLS protocols.