The primary focus of this work is to provide security mechanisms while transmitting data frames in a node to node manner. The security protocol CCMP-AES working in data link layer keeps data frame from eavesdropping, interception, alteration, or dropping from an unauthorized party along the route from the source to the destination.

8.1 CCMP-AES Model

CCMP-AES is based on the Rijndael block cipher algorithm which has a well-designed mathematical structure (Junaid et al., 2006). The overhead in terms of basic operations for iterative block cipher encryption is relatively low compared to other block ciphers as well as its comparatively better efficiency in terms of low memory requirements makes AES suitable to be deployed in wireless devices. The Specification for Enhanced Security over Wireless Networks, IEEE 802.11i, requires a strong encryption standard, and naturally, the use of AES is strongly desired. Therefore, a combination of Counter (CTR) mode encryption and CBC-MAC authentication is proposed in the standard. While CTR-AES encrypts data transferred (i.e. achieves confidentiality) using an encryption key, CBC-MAC provides integrity of data and authentication of the sender by calculating the Message Integrity code (MIC) for message authentication with an authentication key. AES itself is a very strong cipher, but counter mode makes it difficult for an eavesdropper to spot patterns, and the CBC-MAC message integrity method ensures that messages have not been tampered with. If the correct MIC sizes, key sizes and MAC algorithms are used, then it is impossible to inject spoofed packets with a valid MAC into the WLAN (Whiting et al., 2002).

8.1.1 Strengths of AES-CCMP

Although AES-CCMP is a well-known and reliable security ensuring both authentication and integrity of the data, having been widely scrutinized and documented to avoid potential implementation loopholes, there is no perfect security algorithm. The following points summarize the key advantages of the security protocol:

(i) AES-CCMP readily handles messages in which certain parts are intended to be authenticated only and not encrypted, and this is done without any additional cipher text overhead. It can use a single key to provide authentication and integrity. Thus, it reduces key management overhead and minimizes the time spent computing AES key schedules.

(ii) AES-CCMP encryption and decryption use only the forward AES block cipher function rather than the more costly and processing-intensive inverse AES cipher. Using only the AES forward cipher leads to significant savings in code and hardware size.
(iii) AES-CCMP is powerful and offers greater data privacy by encrypting parts of the 802.11 header. It computes the CBC-MAC over the IEEE 802.11 header length, selected parts of the IEEE 802.11 MAC Payload Data Unit (MPDU) header, and the plaintext MPDU data, whereas the old IEEE 802.11 WEP mechanism provides no protection to the MPDU header.

(iv) CCMP implementation allows parallel implementation and further streamlining of AES-CCMP in hardware or software. CTR mode offers several advantages, since there is no computational dependency between successive cipher blocks, \( C_i \) and \( C_j \). This enables effective utilization of the software and hardware efficiency by enabling parallelized computation, i.e. one can be computing blocks \( C_1, C_2, \ldots \) all at the same time, limited only by the amount of hardware. Hence, CTR mode encryption is fast and bulk data can be encrypted quickly due to parallelized computing. Pipelining CBCMAC and CTR-mode can be used to increase throughput [26]. CTR mode is simple, as both encryption and decryption depend on a single cipher function.

(v) AES-CCMP mechanism protects users from replay attacks because it uses packet sequence numbers, while it uses temporal key which is derived from the robust 4-way handshake scheme. IEEE802.11i standard specifies that 1st CBC-MAC IV and Counter value (Ctr) of CTR mode are never repeated with the same TK as key stream reuse must not occur.

(vi) There are no patent issues regarding the use of AES-CCMP and all intellectual property rights to CCMP have been released into the public domain.

8.2 SNAuth-SPMAODV with CCMP-AES

The proposed model SNAuth-SPMAODV combines with CCMP-AES model to defend against Denial of Service attack and it provide confidentiality and authentication of packets in both routing and data link layers of MANETs. The primary focus of this work is to provide security mechanisms applied in transmitting data frames in a node-to-node manner through the security protocol CCMP-AES working in data link layer. It keeps data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination.

8.3 Performance Evaluation

8.3.1 Impact of Network Density

This section presents the performance impact of network density on proposed method over number of nodes. The network density has been varied by deploying 200 to 1400 nodes over a fixed area of 1000m x 1000m. Each node in the network moves with a speed randomly chosen between 0 and 20m/sec. 10 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 the node density, while the y-axis represents the results of the performance metric of interest.
**Average Packet Delivery Ratio (PDR)**

Figure 8.1 (a) represents the Average Packet Delivery Ratio of SNAuth-SPMAODV with CCMP-AES and without CCMP-AES for different network sizes. In figure 8.1(a) shows SNAuth-SPMAODV with CCMP-AES shows high packet delivery ratio that are observed for networks with more than 1000 nodes compared to SNAuth-SPMAODV without CCMP-AES. SNAuth-SPMAODV with CCMP-AES which consistently delivers about 10 % more data packets than SNAuth-SPMAODV without CCMP-AES.

![Average Packet Delivery Ratio](image)

**Figure 8.1 (a) SNAuth-SPMAODV-CCMP-AES-Avg.Packet delivery ratio versus number of nodes placed over 1000m x 1000m area.**

**Average Throughput**

Figure 8.1(b) shows the effects of network density on the performance of proposed method in terms of average throughput. Figure 8.1(b) illustrate that throughput is higher in SNAuth-SPMAODV with CCMP-AES for Denial of service attack and without CCMP-AES.
Figure 8.1(b) SNAuth-SPMAODV-CCMP-AES-Avg.Throughput versus number of nodes placed over 1000m x 1000m area.

Average End-to-End Delay

Figure 8.1(c) shows the average end-to-end delay incurred by proposed methods for different network densities. The delay incurred by proposed protocols decreases to a minimum when the number of nodes is increased from 400 to 1400 nodes. The results in Figure 8.1(c) show that, in a dense network, SNAuth-SPMAODV with CCMP-AES for denial of Service attack outperforms SNAuth-SPMAODV without CCMP-AES by reducing the delay. SNAuth-SPMAODV with CCMP-AES keep up good performance in delay as the network density becomes high.
Average Jitter

Figure 8.1(d) shows the effects of network density on the performance of proposed method in terms of average jitter. The performance of SNAuth-SPMAODV with CCMP-AES for denial of Service attack without CCMP-AES in terms of Average Jitter over varying network density. SNAuth-SPMAODV with CCMP-AES outperforms compared to SNAuth-SPMAODV without CCMP-AES.

Routing Overhead

Figure 8.1(e) demonstrates the routing overhead generated by the proposed method when the number of nodes is varied. The figure shows that the generated routing overhead in SNAuth-SPMAODV with CCMP-AES for denial of Service attack without CCMP-AES protocols increases with
increased number of nodes. For example, in figure 8.1(e), when the number of nodes is increased to 800 to 1200 nodes, the generated routing overhead in SNAuth-SPMAODV with CCMP-AES could be less than SNAuth-SPMAODV without CCMP-AES respectively.

8.3.2 Impact of Offered Load

This section demonstrates the effects of offered load on the performance of the proposed protocol. Simulation runs have been conducted for SNAuth-SPMAODV with CCMP-AES and without CCMP-AES where the offered load is varied by increasing the number of source-destination pairs (flows, for short) from 1 to 40. The topology for each simulation scenario consists of 150 nodes placed randomly on a flat area of 1000m x 1000m, each moving with the random waypoint mobility with speed between 0 and 20m/sec.

Average Packet Delivery Ratio

Figure 8.2(a) shows the performance of SNAuth-SPMAODV with CCMP-AES and SNAuth-SPMAODV without CCMP-AES in terms of Average Packet Delivery Ratio versus offered loads. Figure 8.2(a) show that packet delivery ratio is higher in SNAuth-SPMAODV with CCMP-AES for Denial of service attack and without CCMP-AES.
Figure 8.2(a) SNAuth-SPMAODV-CCMP-AES-Avg.packet delivery ratio versus offered load for a network of 150 nodes placed in 1000m x 1000m area.

Average Throughput

Figure 8.2(b) reports the results of the network throughput versus offered load for SNAuth-SPMAODV with CCMP-AES for Denial of service attack and without CCMP-AES. For example, at 40 flows, the network throughput in SNAuth-SPMAODV with CCMP-AES is increased when compared with SNAuth-SPMAODV without CCMP-AES respectively.
Figure 8.2 (b) SNAuth-SPMAODV-CCMP-AES-Avg.Throughput versus offered load for a network of 150 nodes placed in 1000m x 1000m area.

**Average End-to-End Delay**

Figure 8.2(c) shows the impact of offered load on the performance of SNAuth-SPMAODV with CCMP-AES and without CCMP-AES in terms of end-to-end delay. For example, at offered load of 40 flows, the delay acquired by SNAuth-SPMAODV with CCMP-AES is reduced when compared against SNAuth-SPMAODV without CCMP-AES.

Figure 8.2 (c) SNAuth-SPMAODV-CCMP-AES-Avg.End to End Delay versus offered load for a network of 150 nodes placed in 1000m x 1000m area.

**Average Jitter**
In Figure 8.2(d) shows that Average Jitter is plotted against the offered load. SNAuth-SPMAODV with SNAuth-SPMAODV with CCMP-AES achieved the lower jitter compared with SPMAODV without SNAuth-SPMAODV with CCMP-AES when the number of flows varies from 1 to 40.

![Graph showing Average Jitter versus node mobility](image)

**Figure 8.2 (d) SNAuth-SPMAODV-CCMP-AES-Avg.Jitter versus node mobility for a network of 150 nodes placed in 1000m x 1000m area.**

**Routing Overhead**

Figure 8.2(e) shows the impact of node mobility on the performance of proposed method in terms of the routing overhead is plotted against offered load. The figure shows that the generated routing overhead for SNAuth-SPMAODV with CCMP-AES increases with increased offered loads. In figure 4.6(d) for example, at a high offered load (e.g. 30 flows), the routing overhead in SNAuth-SPMAODV with CCMP-AES is reduced when compared against SNAuth-SPMAODV without CCMP-AES.
8.3.3 Impact of Node Mobility

To assess 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 30m/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 8.3(a) explains the performance of SNAuth-SPMAODV with CCMP-AES and without SNAuth-SPMAODV with CCMP-AES in terms of Average Packet Delivery Ratio versus node mobility. It can also be seen from the figure that for a given node mobility the generated Average Packet Delivery Ratio of SNAuth-SPMAODV with SNAuth-SPMAODV with CCMP-AES is much higher compared with that of SNAuth-SPMAODV without CCMP-AES. SNAuth-SPMAODV with CCMP-AES is increased by approximately 5% when compared against SNAuth-SPMAODV without CCMP-AES respectively.
Figure 8.3 (a) SNAuth-SPMAODV-CCMP-AES-Avg. Packet delivery ratio versus node mobility for a network of 150 nodes placed in 1000m x 1000m area.

Average Throughput

Figure 8.3(b) depicts the average throughput incurred by proposed method for different maximum speed. The figure shows that Average throughput is achieved by SNAuth-SPMAODV with CCMP-AES outperforms as the maximum node speed increases. The figure also shows that for a given node speed, the SNAuth-SPMAODV slightly outperformed SNAuth-SPMAODV without with CCMP-AES.

Figure 8.3(b) SNAuth-SPMAODV-CCMP-AES-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 8.3(c) depict the impact of node mobility on the performance of SNAuth-SPMAODV with and without CCMP-AES in terms of end-to-end delay. However, in a relatively high mobility (e.g. 20m/s) the SNAuth-SPMAODV with CCMP-AES outperforms both SNAuth-SPMAODV without CCMP-AES.

![End-to-End Delay Diagram](image)

**Figure 8.3(c) SNAuth-SPMAODV-CCMP-AES-Avg.End to End delay versus node mobility for a network of 150 nodes placed in 1000m x 1000m area.**

**Average Jitter**

In Figure 8.3 (d) shows Average Jitter is plotted against the node speed. As shown in the figure, the Average Jitter decreases from the increased node speed. When the node speed, SNAuth-SPMAODV with CCMP-AES achieved the lower jitter compared with SPMAODV without CCMP-AES.
Routing Overhead

In Figure 8.3(e), the routing overhead generated by SNAuth-SPMAODV with CCMP-AES and without CCMP-AES is plotted against the maximum node speed. As shown in the figure, the routing overhead generated by SNAuth-SPMAODV with CCMP-AES and without CCMP-AES increases as the node mobility increases. The SNAuth-SPMAODV with CCMP-AES has significantly reduced the routing overhead when compared against SNAuth-SPMAODV without CCMP-AES respectively at relatively high node mobility (e.g., 25m/sec).
8.4 Conclusion

The proposed model combines SNAuth-SPMAODV with CCMP-AES model to defend against Denial of Service attack and it provides confidentiality and authentication of packets in both routing and link layers of MANETs. The primary focus of this work is to provide security mechanisms applied in transmitting data frames in a node-to-node manner through the security protocol CCMP-AES working in data link layer and it keeps data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination.