CCMP-AES Model with SNAuth-SPMAODV Routing Potocol to Secure Link and Network Layer for Mobile Adhoc Networks in Military Scenario

D. Devi Aruna, P. Subashini

Abstract— Mobile Adhoc network is a special kind of wireless networks. It is a collection of mobile nodes without having aid of established infrastructure. Mobile Adhoc network are vulnerable to attacks compared to wired networks due to limited physical security, volatile network topologies, power-constrained operations, intrinsic requirement of mutual trust among all nodes. During deployment, security emerges as a central requirement due to many attacks that affects the performance of the ad hoc networks. Particularly Denial of Service attack is one such severe attack against ad hoc routing protocols which is a challenging one to defend against in military communication environments. The proposed model combines SNAuth-SPMAODV with CCMP-AES mode to defend against Denial of Service attack and it also provides confidentiality and authentication of packets in both routing and link layers of MANET. 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 unauthorized party along the route from the source to the destination. The simulation is done for different number of mobile nodes using network simulator Qualnet 5.0. The proposed model has shown better results in terms of total bytes received, packet delivery ratio, throughput, End to End delay and Average jitter.

Keywords-MANET, Mobile adhoc network, Denial of Service attack, Strict priority algorithn, Secure neighbor authentication, Advanced encryption standard.

I. INTRODUCTION

In recent years, Mobile Adhoc Network (MANET) has received marvelous attentions due to self-design, self-maintenance, and cooperative environments [9]. In MANET, all the nodes are mobile nodes and the topology will change rapidly. Here, the mobile devices such as PDAs and laptops are used to route the data packets. In MANET, all the nodes actively discover the topology and the message is transmitted to the destination over multiple hop. The important characteristics of MANETs are lack of infrastructure, dynamic topology, multi-hop communication and distributed coordination among all the nodes. The potential deployment of MANET exists in many scenarios, for example in situations where the infrastructure is not feasible such as disaster relief and cyclone, etc. The MANET has potential of realizing a free, ubiquitous, and omni directional communication. The wireless channels can be accessible by both legitimate users and malicious users. In such environments, there is no guarantee that a route between the two nodes will be free for the malicious users, which will not comply with the employed protocol. The malicious users will attempt to harm the network operations. During deployment, security emerges as a central requirement due to many attacks that affect the performance of the ad hoc network [15]. Particularly Denial of Service attack is one such severe attack against ad hoc routing protocols which is a challenging one to defend against. 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.

Manuscript received March 31, 2012

D. Devi Aruna, Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore, India
(e-mail: deviaruna2007@gamil.com).

Dr. P. Subashini, Avinashilingam institute for Home Science and Higher Education for Women, Coimbatore, India,
(e-mail: mail.p.sbashini@gmail .com).

II. REVIEW OF LITERATURE

This chapter briefly describes the denial of service attack and routing protocols for MANETS.

A.Denial of Service attack

An attacker attempts to prevent legitimate and authorized users from the services offered by the network. A denial of service (DoS) attack can be carried out in many ways. The typical way is to flood packets to any centralized resource present in the network so that the resource is no longer accessible to nodes in the network, as a result of which the network no longer function in the manner in which it is designed to operate. This may lead to a failure in the delivery of certain services to the end users. Due to the unique characteristics of ad hoc wireless networks, there exist many more ways to launch a DoS attack in such a network, which would not be possible in wired networks. DoS attacks can be launched against any layer in the network protocol stack.

On the physical and MAC layers, an adversary could employ jamming signals which disrupt the on-going transmissions on the wireless channel. On the network layer, an adversary could take part in the routing process and exploit the routing protocol to disrupt the normal functioning of the network. For example, an adversary node could contribute in a session but simply drop certain number of packets, which may lead to degradation in the QoS being offered by the network. On the higher layers, an adversary could bring down serious services such as the key management service. For example, consider the following: In fig.1 assume a shortest path that exists from S to X and C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial of service attack. Suppose S wishes to communicate with X and that S has an unexpired route to X in its route cache. S transmits a data packet towards X with the source route S --> A --> B --> M --> C --> D --> X contained in the packet's header. When M receives the packet, it can alter the source route in the packet's header, such as deleting D from the source route. Consequently, when C receives the altered packet, it attempts to forward the packet to X. Since X cannot hear C, the transmission is unsuccessful [10].

S ↔A↔ B↔ M ↔C↔ D↔ X

Figure 1. Denial of Service attack

B. Route Selection

Proactive routing protocols generate routes and store them for later use. On- demand routing protocols only generate routes when necessary. The latter is used more often in MANETs because they require fewer resources. The mostly used on-demand routing protocols are Ad-hoc On-demand Distance Vector (AODV) Unless modified, the protocol use single routes between sender and receiver nodes. Multipath routing reduces dependency on single nodes and routes, offering robustness in a secured MANET.

C.Adhoc On demand Routing protocol (AODV)

AODV routing protocol is based on DSDV and DSR algorithm and is a state-of-the-art routing protocol that adopts a purely reactive strategy: it sets up a route on demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated [5]. This protocol is composed of two mechanism (1) Route Discovery and (2) Route Maintenance. AODV uses Route Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in [6]. In general, the nodes participating in the communication can be classified as source node, an intermediate node or a destination node. With each role, the behavior of a node actually varies. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors. This RREQ message will further be forwarded (again broadcasted) by the intermediate nodes to their neighbors. This process will continue until the destination node or an intermediate node having a fresh route to the destination[7]. At this stage eventually, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be received. Fig. 2 depicts the traversal of control messages.

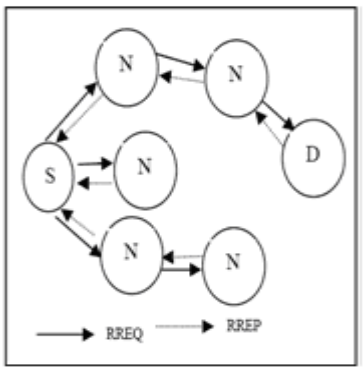

Figure 2: Traversal of Control Messages

D. Multipath Routing

Ad-hoc wireless routing protocols like AODV are mainly designed to discover and use a single route between a sender and receiver node[13]. However, multiple paths between sender and receiver nodes 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.

Several multipath routing protocols based on DSR have been proposed, such as Split Multipath Routing (SMR) and Multipath Source Routing (MSR). Each of these multipath routing protocols broadcast data over all paths simultaneously. This technique has all the advantages previously mentioned, but it also introduces more packets into the MANET.

E. Strict-Priority Routing

Using multiple paths in ad-hoc networks to achieve higher bandwidth is not as straightforward as in wired networks. Because ad-hoc networks communicate over a wireless medium, radio interference may be a factor when a node communicating along one path interferes with a node communicating along another path, limiting the achievable throughput. Still, simulations have shown that broadcast multipath routing creates more overhead but provides better performance in congestion and capacity than unipath routing, provided the route length is within a certain upper bound which is derivable. Additionally, the proper selection of routes using a strict priority multipath protocol can increase further the network throughput.

F.Secure Neighbor Authentication

The secure neighbor authentication has two variants. The first variant is based on pair-wise shared secrets, and the second variant is based on certification.

In secure neighbor authentication (SNAuth), every mobile node establishes an authenticated neighborhood on the move. Periodically, every mobile node X broadcasts its identity packet <SNAuth- HELLO, X> to its neighborhood.

1. In the pair-wise shared secret variant of SNAuth, Y, a neighboring receiver of the identity broadcast initiates a 3-way challenge-response handshake to authenticate X, the sender of the identity broadcast.

a. Suppose X and Y share a pair-wise secret k. Now Y selects a random nonce n1, encrypts n1 with k, sends the encrypted result ENC_k (n1) to X by a message <CHALLENGE, Y, ENC_k (n1)>.

b. If the receiver of the challenge message is indeed X, then it can decrypt ENC_k (n1) and sees n1. X selects another random nonce n2, encrypts ENC_k (n1 XOR n2), and sends back <RESPONSE1, X, n2, ENC_k (n1 XOR n2)> as the response to the challenger Y.

c. When Y receives the response, Y decrypts ENC_k (n1 XOR n2) and obtains n1 XOR n2. If Y can get the same result from XORing n2 in the response and its own challenge n1, then X passes the test with success. Otherwise, Y does not send any packet to X and does not receive packets from X except the response packets, until a correct <RESPONSE1> packet from X can pass the test. Upon detecting a success, Y puts X in its secure neighbor list. Y selects a random nonce n3 and sends out a confirmation response <RESPONSE2, Y, n3, ENC_k (n1 XOR n2 XOR n3)> to X.

d. Upon receiving the RESPONSE2 message, X decrypts ENC_k (n1 XOR n2 XOR n3) and obtains n1 XOR n2 XOR n3. If this matches the result of XORing n1 that is previously decrypted, its own n2 and n3 in the RESPONSE2 packet, then X inserts Y into its secure neighbor list. (This three-way handshake is required because X needs to verify that Y actually knows k)

e. End of the challenge-response protocol. Figure 3 shows Challenge-Response Protocol-Three way handshake

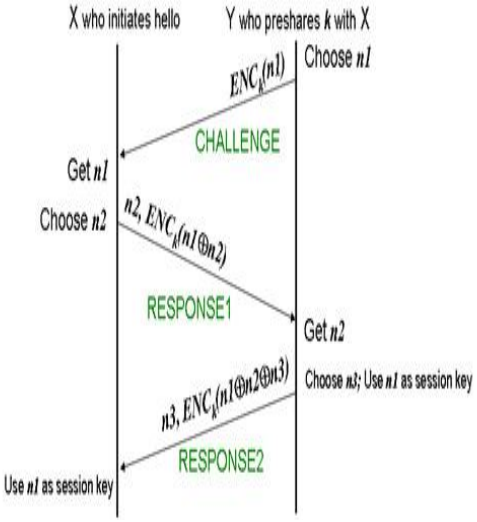

Figure 3: Challenge-Response Protocol-Three way handshake

In the above description, all nonce length is currently set to 128-bit long. Encryption block length is 128-bit. Key k can be 128-bit, 192-bit, or 256-bit. Session key means that the key n1 is used until the time when the next HELLO received by Y from X successfully passes the test again.

2. A slightly different challenge-response scheme is used if Y does not pre-share a master secret k with X. Here X must broadcast its certificate $CERT_x$ = [X, certified public key PK_x, certificate valid time] in a CERTIFIED_HELLO message. For Y's CHALLENGE, Y uses PK_x to encrypt n1 and obtains ciphertext PK_x (n1). Y must also add its own certificate $CERT_y$ = [Y, certified public key PK_y, certificate valid time] and sign the entire message with its own private key SKY. It recommend the public key cryptosystem in use be an Elliptic Curve Cryptosystem (ECC), because ECC features shorter certificate length and ciphertext length, thus incurring less communication overhead. Figure 4 shows Challenge-Response Handshake.

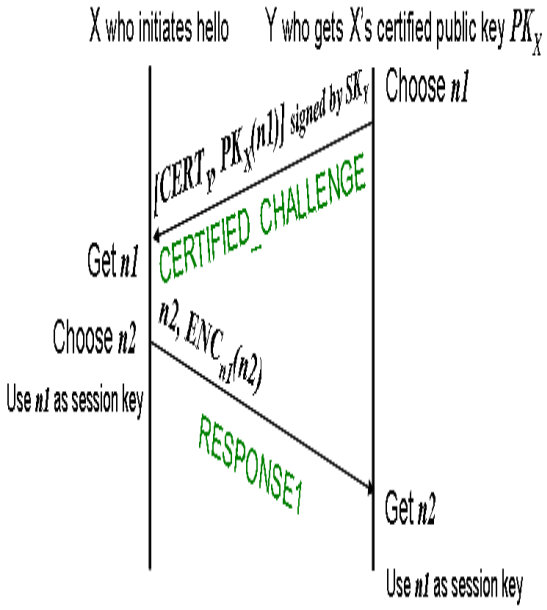

Figure 4: Three Way Challenge-Response Handshake

When every neighboring receiver of X finishes the authentication and key-agreement process, node X obtains a secure snapshot of its neighborhood. In the neighborhood, every other node is authenticated and shares an IPsec security association with the node X. As the SNAuth protocol runs on every mobile node, the statement is true if node X is replaced with any node X'.

G.CCMP-AES Model

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol. The CCMP algorithm is based on the U.S. federal government's Advanced Encryption Standards (AES)[2]. CCMP offers enhanced security compared with similar technologies such as Temporal Key Integrity Protocol (TKIP). CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes the vulnerability of black hole attack.CCMP is a Robust security network association (RSNA) data confidentiality and integrity protocol[3].

CCMP is based on the Counter Mode with CBC-MAC(CCM) of the AES encryption algorithm. CCM is a generic authenticate-and-encrypt block cipher mode. A unique temporal key (for each session) and a unique nonce value (a value that's used only once for each frame) are required for protecting the Medium Access Control Protocol Data Unit (MPDU). CCMP uses a 48-bit Packet Number (PN) to protect the MPDUs.CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following algorithm [4].Figure 5 shows CCMP encapsulation algorithm

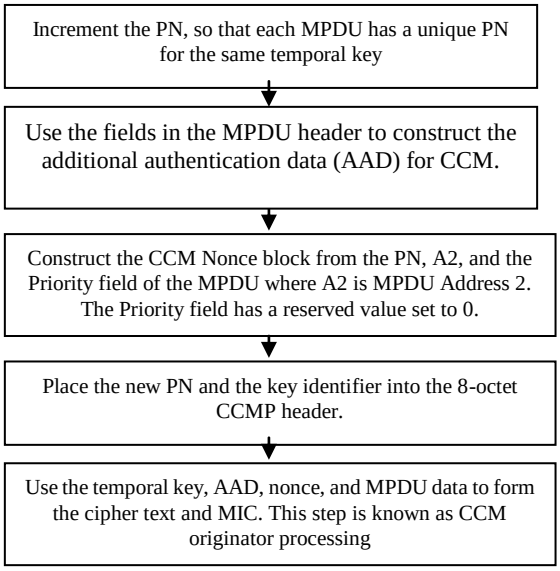

Figure 5: CCMP encapsulation algorithm

CCMP decrypts the payload of a cipher text MPDU and decapsulates plaintext MPDU using the following algorithm[3].

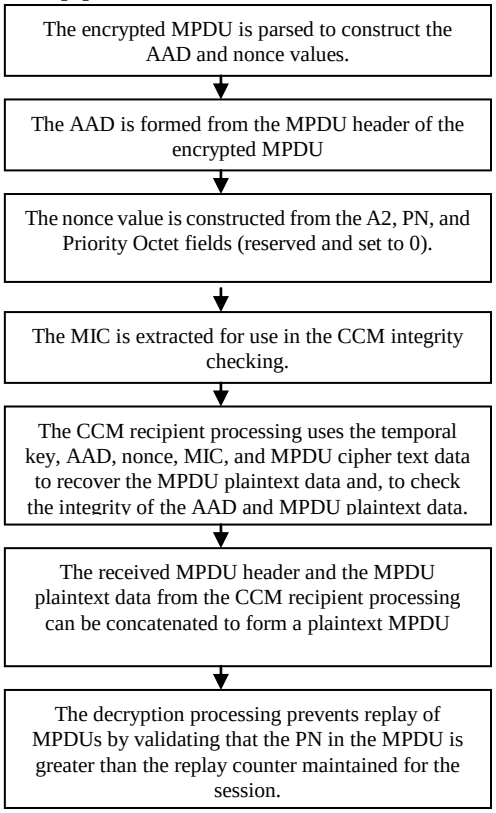

Figure 6 CCMP decapsulation algorithm.

The decapsulation process succeeds when the calculated Message Integrity Code (MIC) matches the MIC value obtained from decrypting the received encrypted MPDU. The original MPDU header is concatenated with the plaintext data resulting from the successful CCM recipient processing to create the plaintext MPDU.

The proposed model 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, such as 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.

III. PROBLEM STATEMENT

This research investigates how to integrate security policies of a MANET with secure neighbor authentication that will allow the MANET to function securely in a military environment without degrading network performance. The specific problem to be addressed is how to use secure neighbor authentication of nodes in a multipath routing algorithm in MANET protected from Denial of service attack in military environment. Most of such performance analysis is normally done on commercial settings. For instance, wireless LAN technologies in the 2.4 GHz ISM frequency band are generally assumed, offering data rates up to 2 Mbps within the range of 250 m. This paper is motivated by the observation that such propagation and network models assumed by the current ad hoc networking simulations are quite different from real world military environments. In fact, a few hundred MHz frequency band (i.e., VHF or even HF) is used with very low data transmission rates (e.g., 384 Kbps) for the military scenarios. Table 1 summarizes these differences in terms of a physical layer model[16]. Networking environments such as network size, nodes' mobility model, and traffic patterns are quite different as well. For instance, the size of military networks is often far greater than that of their conventional counter parts both in the number of nodes and dimensions of the geographical areas.

Table 1: physical layer model for military environments

Parameters	**Military devices**	**Conventional devices**
Frequency	30, 88, 300 *MHz*	2.4, 5 *GHz*
Propagation limits	-115 *dBm*	-110 *dBm*
Radio propagation model	Two-ray ground	Line-of-sight
Data rates	9.6~384 *Kbps*	2~54 *Mbps*

Transmit power	37 *dBm*	15 *dBm*
Receive sensitivity	-100 *dBm*	-90 *dBm*

IV. PROPOSED METHODOLOGY

A MANET is a collection of mobile routers that move dynamically in unpredictable directions. The links connecting the nodes are wireless and thus are not as dependable as wired links. The links are also susceptible to capacity constraints. A MANET environment is characterized by numerous security threats because the wireless links are vulnerable to Denial of service attack. 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.

V. SIMULATION MODEL

Using the QualNet network simulator [18], comprehensive simulations are made to evaluate the protocol. Qualnet provides a scalable simulation environment for multi-hop wireless ad hoc networks, with various medium access control protocols such as CSMA and IEEE 802.11. channel and physical layer settings are modified to apply more realistic military scenarios. Note that PRC-999K device is used as a reference model. 802.11 DCF and UDP protocols are used for MAC and a transport protocols, respectively. Also, CBR traffic is utilized in the study. As the TCP-based application protocols such as telnet or FTP show unstable performance in mobile wireless communication, it can not evaluate precise performance of routing protocol itself. CBR application model sends one packet per second, which represents relatively low traffic patterns in military environments. Each packet size is 512 Bytes. In military environments, operational network size is very large as compare to conventional case. Nodes in the simulation are assumed to move according to the "random way point" mobility model. Pause time is fixed to 20 seconds. The attackers are positioned around the center of the routing mesh in all experiments.

To evaluate the performance of proposed method by 4 measurements: Packet delivery radio, average end-to-end delay, routing overhead and Throughput.

A. Results and Analysis

In this set of simulations, analyze performance of SNAuth-SPMAODV when the network size varies from 100 nodes to 1400 nodes. The network sizes and the respective network areas are shown in Table 2 (approximately a walking Speed of soldiers). The size and the area are selected such that the node density is approximately constant, to properly evaluate proposed method.

Table 2: Network sizes and areas

Nodes	Area (m)
100	1400×1400
200	2000×2000
400	2800×2800
600	3500×3500
800	4000×4000
1000	4500x4500
1200	4900x4900
1400	5300x5300

Comparison of SNAuth-SPMAODV and CCMP-AES Models for SNAuth-SPMAODV routing protocol with Denial of Service attack.

The different parameters are considered for evaluation. Average packet delivery ratio, Average throughput, Total Bytes Received should be higher and Average end-to-end delay, Average delay jitter must be lower.

Figure7 shows that total byte received is higher in CCMP-AES with SNAuth-SPMAODV with Denial of Service attack compared to SNAuth-SPMAODV.

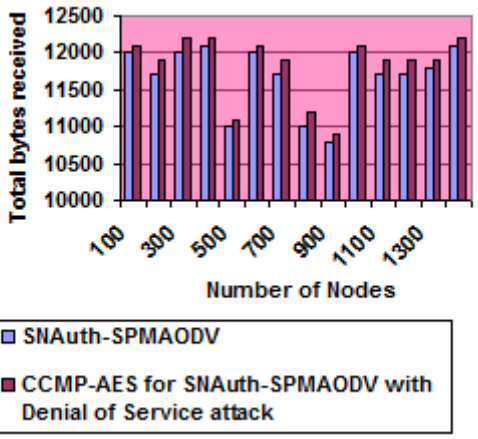

Figure 7: Comparison of Total bytes received of SNAuth-SPMAODV and SNAuth-SPMAODV for CCMP-AES with Denial of Service attack

Figure 8 shows that total packet received is higher in CCMP-AES with SNAuth-SPMAODV with Denial of Service attack compared to SNAuth-SPMAODV.

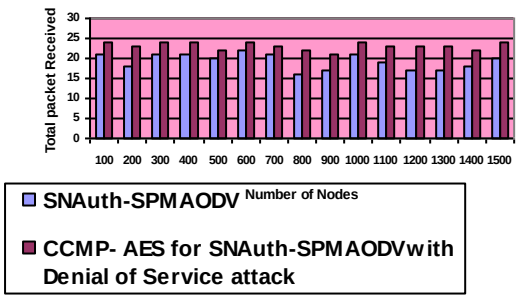

Figure 8: Comparison of Total packet received of SNAuth-SPMAODV and SNAuth-SPMAODV for CCMP-AES with Denial of Service attack

Figure 9 shows that End to End Delay is lower in CCMP-AES with SNAuth-SPMAODV with Denial of Service attack compared to SNAuth-SPMAODV.

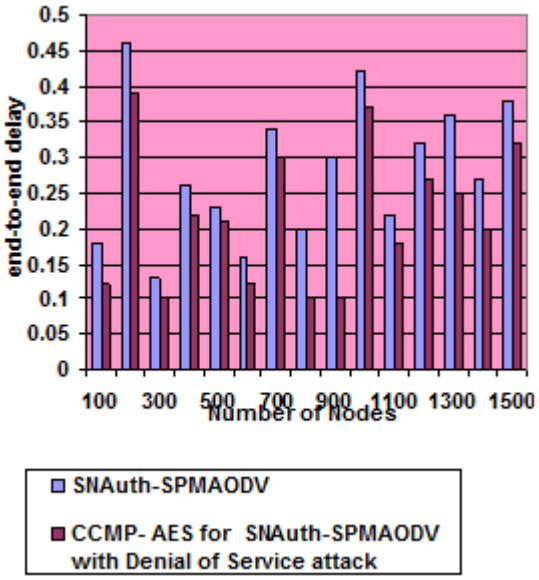

Figure 9: Comparison of End to End delay of SNAuth-SPMAODV and SNAuth-SPMAODV for CCMP-AES with Denial of Service attack

Figure 10 shows that Throughput is higher in CCMP-AES with SNAuth-SPMAODV with Denial of Service attack compared to SNAuth-SPMAODV

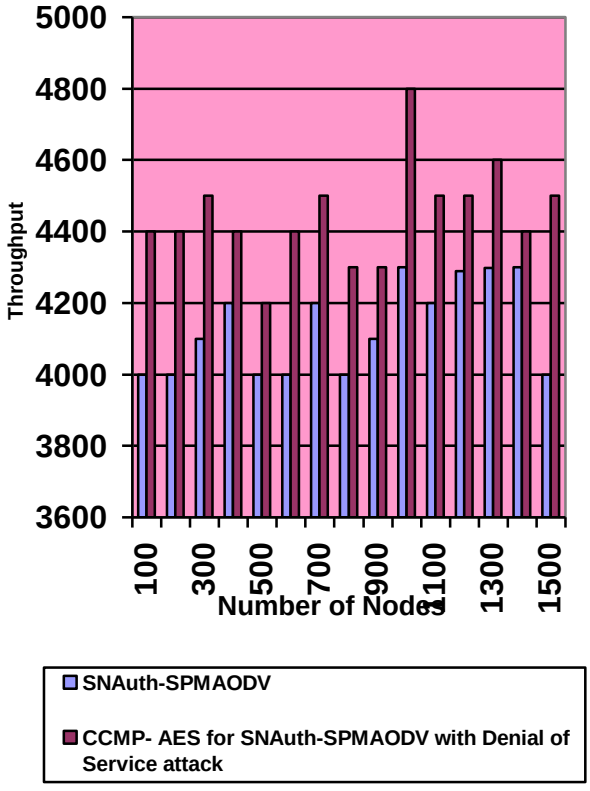

Figure 10: Comparison of Throughput SNAuth-SPMAODV and SNAuth-SPMAODV for CCMP-AES with Denial of Service attack

Figure 11 shows that Average Jitter is lower in CCMP-AES with SNAuth-SPMAODV with Denial of Service attack compared to SNAuth-SPMAODV.

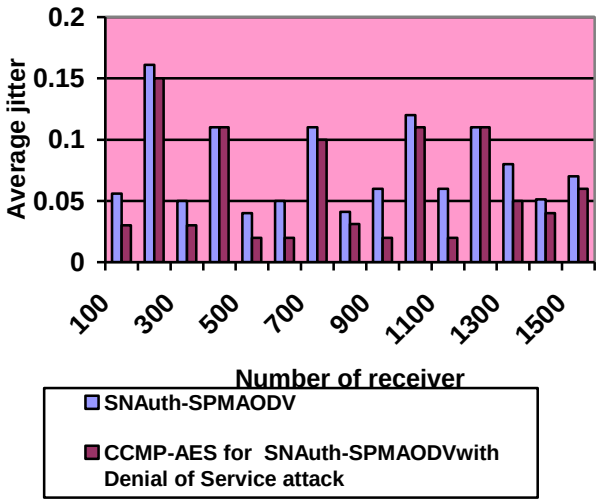

Figure 11: Comparison of a Average Jitter of SNAuth-SPMAODV and SNAuth SPMAODV for CCMP-AES with Denial of Service attack

From the simulation result it is observed that proposed model is robust against black hole attacks and it also provides confidentiality and authentication of packets in both routing and link layers of MANET.

VI. CONCLUSION

Mobile Adhoc network is a special kind of wireless networks. It is a collection of mobile nodes without having aid to establish infrastructure. During deployment, security emerges as a central requirement due to many attacks that affects the performance of the ad hoc networks. Particularly Black hole attack is one such severe attack against ad hoc routing protocols which is a challenging one to defend against. The proposed model combines the On demand routing protocol DSR with CCMP-AES model to defend against black hole 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. The proposed model has shown better results in terms of packet delivery ratio, throughput, End to End delay and jitter.

REFERENCES

1. Changhua He and John C Mitchell, *"Security Analysis and Improvements for IEEE 802.11i"*, in the Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS'05), 2005.

2. Specification for the Advanced Encryption Standard (AES), FIPS 197, U.S. National Institute of Standards and Technology. November 26, 2001. [Online] Available at: http://www.nist.gov/aes.
3. D. Whiting, R. Housley, and N. Ferguson, "*AES Encryption & Authentication Using CTR Mode & CBC-MAC*", IEEE Doc. 802.11-02/144r2, Mar 2002.
4. M. Junaid , Dr Muid Mufti and M.Umar Ilyas, "*Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol*", *In the Proceedings Of World Academy Of Science, Engineering And Technology* Volume 11, February 2006,pp 228-233
5. Asad Amir Pirzada Chris McDonald and Amitava Datta: "*Performance Comparison of Trust-Based Reactive Routing Protocols*" IEEE Transactions on Mobile Computing, Vol. 5, Issue 6,June 2006, pp695 – 710.
6. P. Chenna Reddy and Dr. P. ChandraSekhar Reddy, "*Performance Analysis of Adhoc Network Routing Protocols"*, International Symposium on Ad Hoc and Ubiquitous Computing, 2006. ISAUHC '06. August 2007 ,pp.186 - 187
7. Geetha Jayakumar and Gopinath Ganapathy ,"*Performance Comparison of Mobile Ad-hoc Network Routing Protocol*", *IJCSNS International Journal of Computer Science and Network Security*, VOL.7 No.11, November 2007,pp 77-83.
8. Hao Yang, Haiyun Loo, Fan Ye, Sogwu Lu and Lixia Zhog, Security in mobile ad hoc networks, challenges and solution, Wireless Communication, IEEE Volume I, issue 1, Feb 2004, pp .38 – 47.
9. 9.Dr.G.Padmavathi, Dr.P.Subashini, and Ms.D.Devi Aruna, Impact of Wormhole Attacks and Performance Study of Protocols in Mobile Ad Hoc Networks, Journal of Information Assurance and Security , Pages 094-101,2010, pp. 094-101.
10. Abhay Kumar Rai, Rajiv Rwandan Tewari & Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet Communication, International Journal of Computer Science and Security (IJCSS) Volume 4, Issue 3, July 2010, Pages 265-274.
11. C.E. Perkins, E.M. Royer & S. Das, Ad Hoc On Demand Distance Vector (AODV) Routing, IETFInternet draft, draft-ietf-manet-aodv-08.txt, March 2001
12. A. Boukerche," Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks", Mobile Networks and Applications 9, Netherlands, 2004, pp. 333-342
13. A.E. Mahmoud, R. Khalaf & A, Kayssi," *Performance Comparison of the AODV and DSDV Routing Protocols in Mobile Ad-Hoc Networks",* Lebanon, 2007
14. Kamanshis Biswas and Md. Liakat Ali , "Security Threats in Mobile Ad Hoc Network" Department of Interaction and System Design School of Engineering, ,March2007, Page9-26.
15. Wenjia Li and Anupam Joshi,"Security Issues in Mobile Ad Hoc Network" - A Survey, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County ,2007, page 6-10,.
16. Jong mu Choi and Young bae Ko. A Performance Evaluation For Ad Hoc Routing Protocols In Realistic Military Scenarios. In *Proceedings of The 9th CDMA International Conference*, October 2004.
17. Georgios Kioumourtzis, Christos Bouras, and Apostolos Gkamas, performance evaluation of ad hoc routing protocols for military communications, international journal of network management, Wiley InterScience 2011.
18. Qualnet Documentation, "Qualnet 5.0 Model Library, Network Security", Available:Http://Www.Scalablenetworks.Com/Products/Qualnet/Downlaod....