(IJIRSE) International Journal of Innovative Research in Science & Engineering
ISSN (Online) 2347-3207

Layerwise Security Framework with Snauth-SPMAODV to Defend Denial of Service Attack in Mobile Adhoc Networks for Hostile Environment

[1]D.Devi Aruna [2]Dr.P.Subashini
[1]Assistant Professor, Department of Computer Applications, Kumaraguru College of Technology
[2]Professor, Department of Computer Science, Avinashilingam institute for Home Science and Higher Education for Women, Coimbatore

Abstract-**Mobile Ad-hoc Networks (MANETs) have the ability to setup networks on the fly in a hostile environment where it may not possible to deploy a traditional network infrastructure. 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. There is no solution that provides layer wise security which is a major challenge for Mobile Adhoc networks. This research effort examines the theory, application, and results for a Layerwise Security (LaySec) framework that provides security for an ad-hoc network operating in a hostile environment. LaySec incorporates three security features (Secure neighbor authentication and Layerwise Security techniques and multipath routing) into its 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 simulation is done for different number of mobile nodes using network simulator Qualnet 5.0. From the simulation results, it is observed that the proposed approach has shown better results in terms Quality of Service parameter likely Average packet delivery ratio, Average throughput, Average end to end delay, Average jitter and Routing Overhead.**

Keywords – Mobile adhoc Networks, Denial of Service attack, Layer wise security protocols, secure neighbor authentication, Adhoc On demand Distance Vector (AODV) routing.

I. INTRODUCTION

Security has become a primary concern in order to provide protected communication in wireless as well as wired environment [1]. In recent years, Mobile Ad hoc Networks (MANETs) have received tremendous attention because of their self-configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multihop routing. Although security has long been an active research topic in wireline networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design [7]. These challenges include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve the goals, the security solution should provide complete protection, spanning the entire protocol stack [8]. DoS attacks can be launched against any layer in the network protocol stack. In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network[22]. The proposed Layerwise Security Framework is very robust against Denial of Service attacks in hostile environment.

The paper is organized in such a way that Chapter 2 discusses Review of Literature, Chapter 3 discusses proposed method, Chapter 4 discusses problem statement Chapter 5 discusses Experimental evaluation and Chapter 6 gives the conclusion.

II. REVIEW OF LITERATURE

This chapter briefly describes the Denial of Service attacks for MANET.

A. Denial of Service attack

In this type of 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 classic way is to flood packets to any centralized resource present in the network so that the resource is no longer available to nodes in the network, as a result of which the network no longer operate in the manner in which it is designed to operate. This may lead to a failure in the delivery of guaranteed 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 participate 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 critical services such as the key management service. For example, consider the following: In figure1 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 [3].

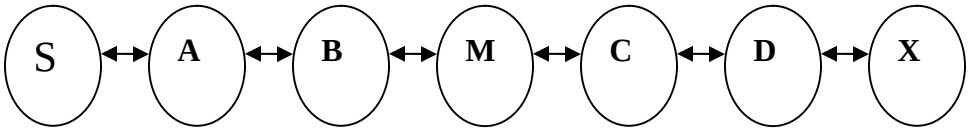

Figure 1: Denial of Service attack

B.Routing Protocols

The fundamental idea of a routing protocol is to deliver the messages from source to destination with enhanced performance in terms of delay and security [5]. Adhoc Routing protocols may be generally categorized as,

- Table driven Protocols and
- Source initiated demand driven Protocols

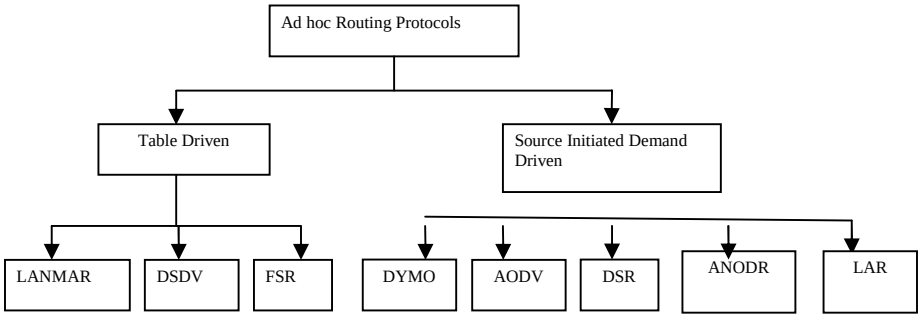

Figure2: categorization of ad hoc routing protocols

III. PROPOSED METHODOLOGY

This approach also aims in improving the performance in terms of QoS characteristics as metrics. The methodology is proposed in order to assure Layerwise security for Mobile Ad hoc Networks. The specific contributions are structured in six phases.

Phase I: Integration of SNAuth with SPMAODV
Phase II: SNAuth-SPMAODV with SIP for Application and Network layer Security
Phase III: SNAuth-SPMAODV with WTLS for Transport and Network Layer Security
Phase IV: SNAuth-SPMAODV with IPSec for Network Layer Security
Phase V: SNAuth-SPMAODV with CCMP-AES for Link and Network Layer Security
Phase VI: SNAuth-SPMAODV with DSSS for Physical and Network Layer Security

Integration of SNAuth with SPMAODV

SPMAODV provides multiple paths between sender and receiver nodes that 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. The proper selection of routes using a strict-priority multipath protocol can increase further the network throughput. The main idea of this phase to integrate strict priority multipath AODV with secure neighbor authentication that facilitate neighboring nodes exchange messages to discover and authenticate each other. Thus this phase provides security mechanism like message integrity, mutual authentication, and non-repudiation; defend against Denial of Service attacks and increase network throughput.

SNAuth-SPMAODV with SIP for Application and Network layer Security

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. It reduces dependency on single nodes and routes; it discovers multiple paths between sender and receiver nodes and it has the advantages of a multipath protocol without introducing extra packets into the network offering robustness in a secured MANET. It can be used to offset the dynamic and unpredictable configuration of adhoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth in hostile environment [15].

SNAuth-SPMAODV with WTLS for Transport and Network Layer Security

The primary focus of this phase 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 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[14]. SNAuth-SPMAODV with WTLS is found to be a good security solution even with its known security problems[9].

SNAuth-SPMAODV with IPSec for Network Layer Security

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 method uses a hybrid version of the IPSec protocol, which includes both AH and ESP modes. IPSec is a protocol suit for securing IP based communication focusing on authentication, integrity, confidentiality and support perfect security forward. The significant importance of the aforementioned protocol is that it offers flexibility, which cannot be achieved at higher or lower layer abstractions in addition to the symmetric cryptographic schemes[11]. These are 1000 times faster than asymmetric cryptographic schemes, a fact that makes IPSec appropriate to be used in handheld resources constrained devices such as PDAs.

SNAuth-SPMAODV with CCMP-AES for Link and Network Layer Security

SNAuth-SPMAODV combines with CCMP-AES model to defend against Denial of Service attack and it provide confidentiality and authentication of packets in both network and data link layers of MANETs[2]. The primary focus of this phase 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.

SNAuth-SPMAODV with DSSS for Physical and Network Layer Security

SNAuth-SPMAODV combines with DSSS to defend against Denial of Service attack. The physical layer protocol in MANETs is reliable for bit-level transmission between network nodes and network layer is responsible to provide security services for both routing information and data message[10]. 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.

IV . PROBLEM STATEMENT

This research investigates how to integrate Layerwise Security Technique with SNAuth-SPMAODV that will allow the MANET to function securely in hostile environment without degrading network performance. Most of such performance analyses are 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 research work 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 I summarizes these differences in terms of a physical layer model [12]. 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 [13].

TABLE I: 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*

V. EXPERIMENTAL EVALUATION

Using the Qualnet network simulator [6], comprehensive simulations are made to evaluate the proposed 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. The attackers are positioned around the center of the routing mesh in all experiments. To evaluate the performance of proposed method by 5 measurements: Average packet delivery ratio, Average throughput must be higher, Average end to end delay, Average jitter and Routing Overhead must be lower..

Experimental Results of Integration of SNAuth with SPMAODV

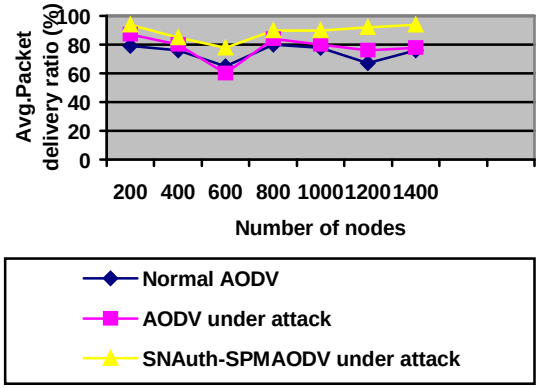

Figure 3(a)

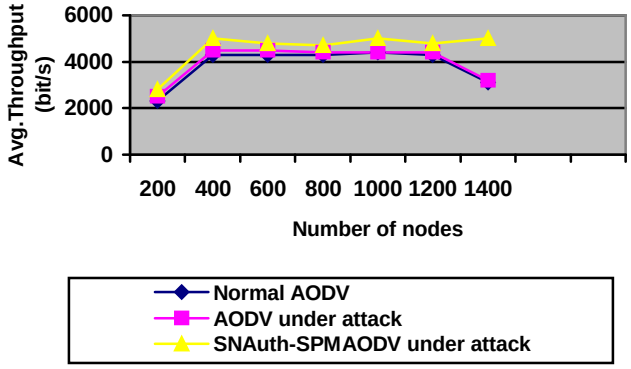

Figure 3(b)

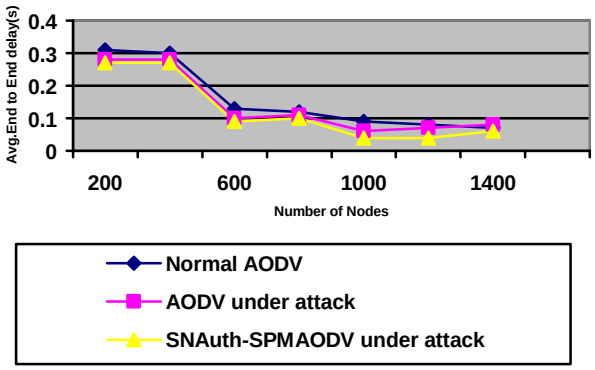

Figure 3(c)

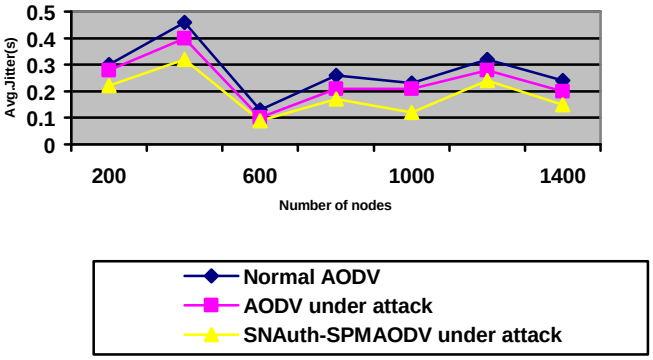

Figure 3(d)

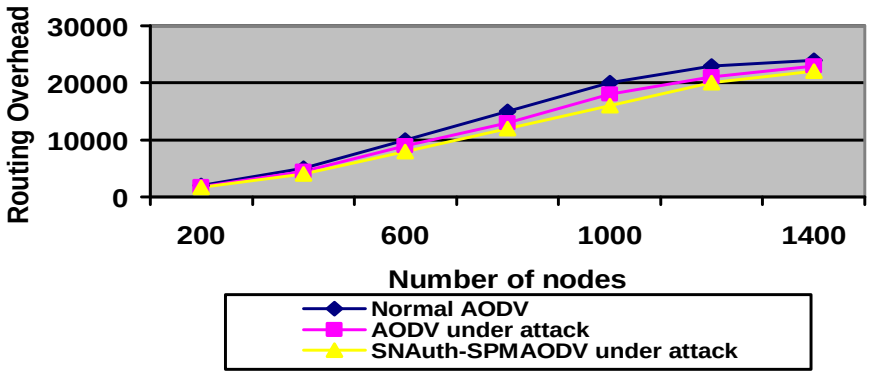

Figure 3(e)

Experimental Results of SNAuth-SPMAODV with SIP for MANET Application and Network layer Security

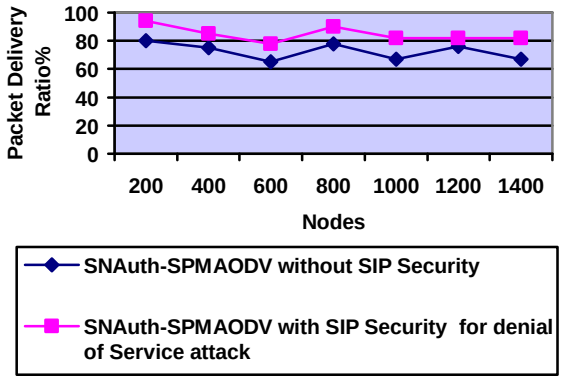

Figure 4(a)

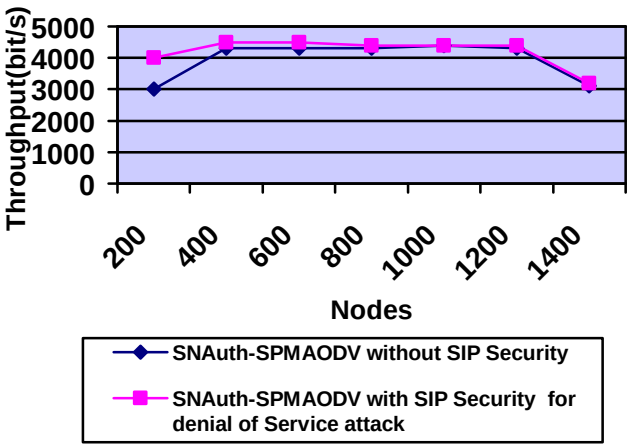

Figure 4(b)

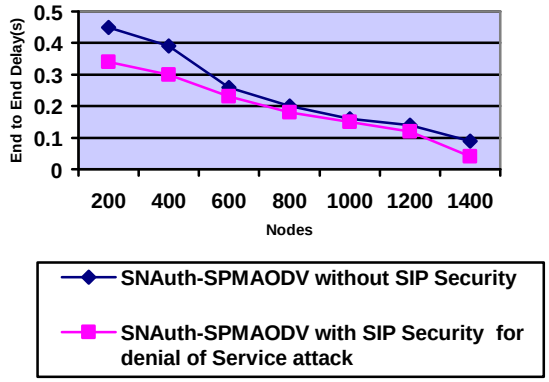

Figure 4(c)

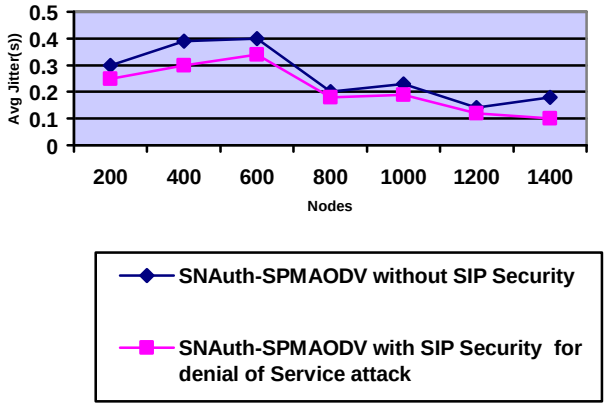

Figure 4(d)

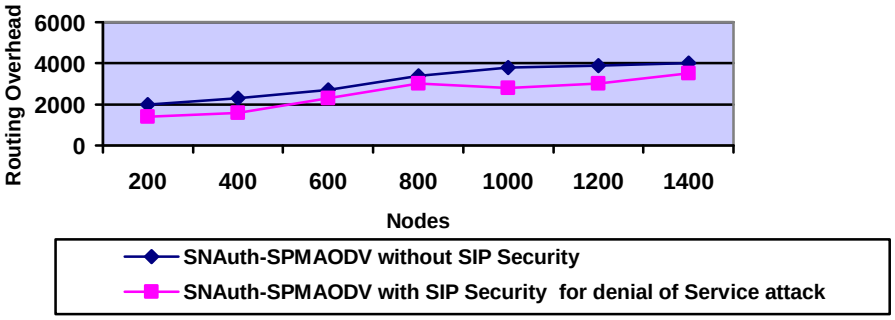

Figure 4(e)

Experimental Results of SNAuth-SPMAODV with WTLS for MANET transport and network layer security

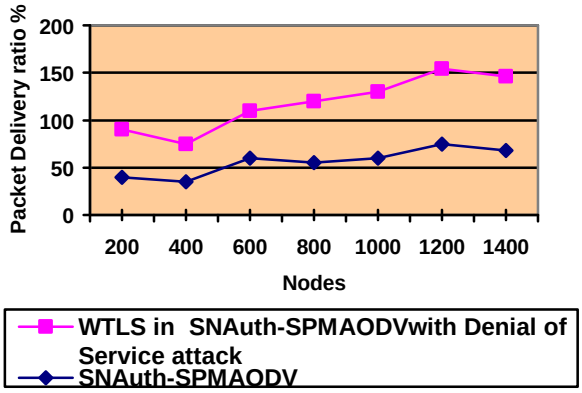

Figure 5(a)

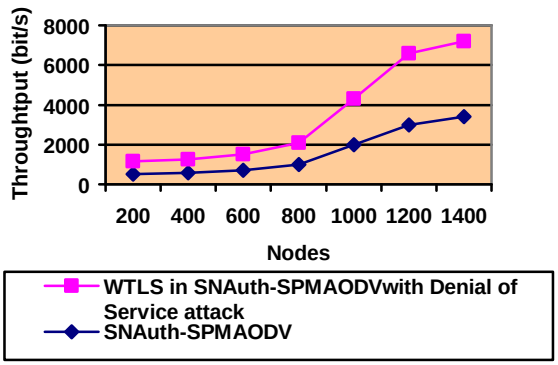

Figure 5(b)

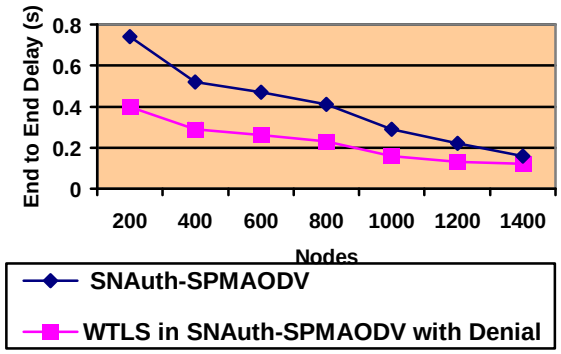

Figure 5(c)

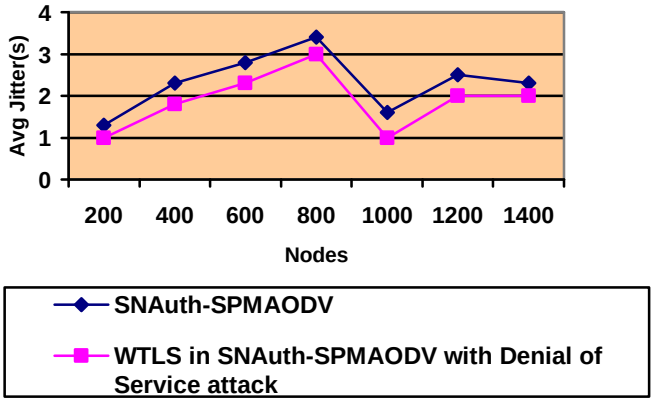

Figure 5(d)

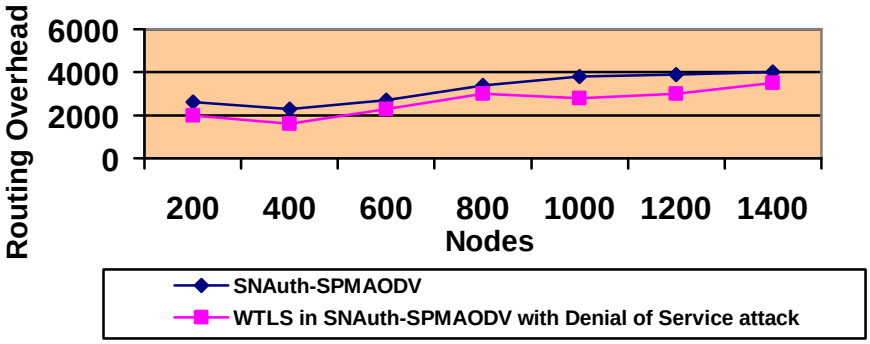

Figure 5(e)

Experimental Results of SNAuth-SPMAODV with IPSec for MANET for network layer security

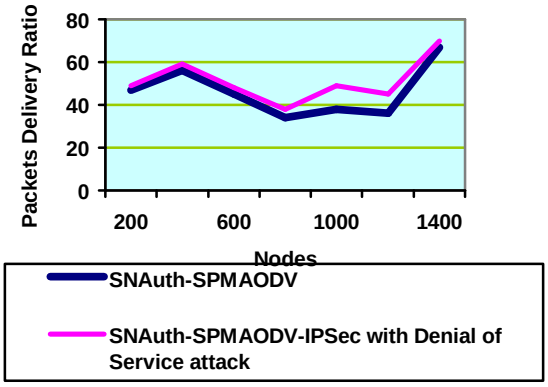

Figure 6 (a)

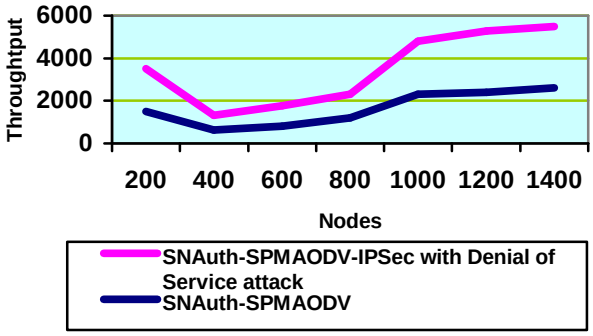

Figure 6(b)

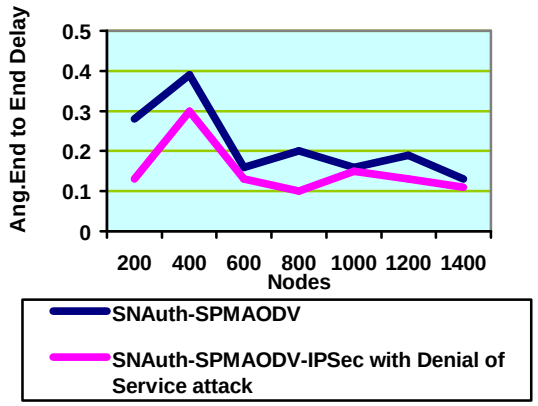

Figure 6(c)

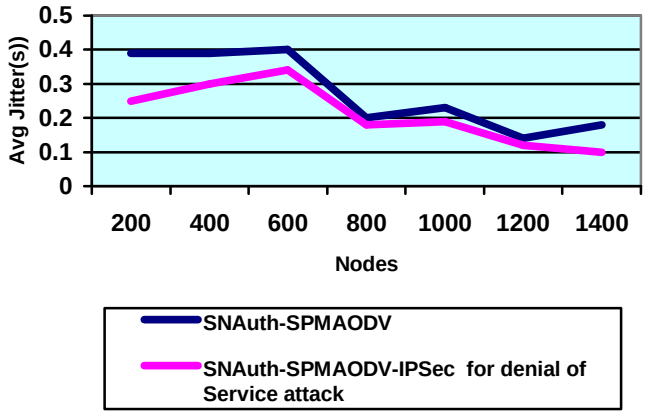

Figure 6(d)

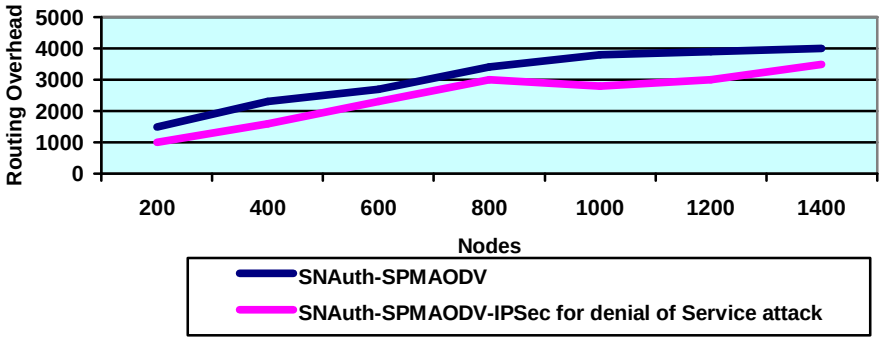

Figure 6(e)

Experimental Results of SNAuth-SPMAODV with CCMP-AES Model for Link layer and Network layer security

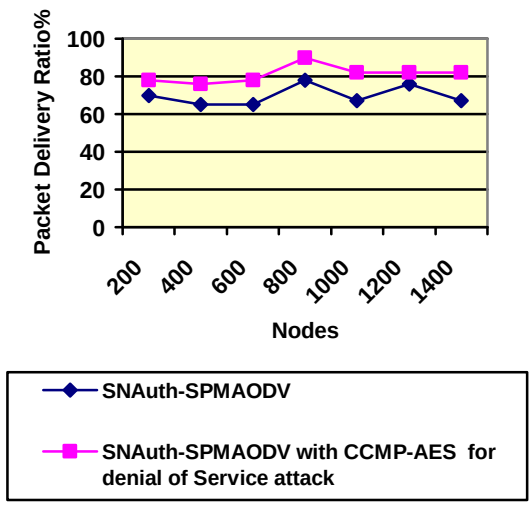

Figure 7(a)

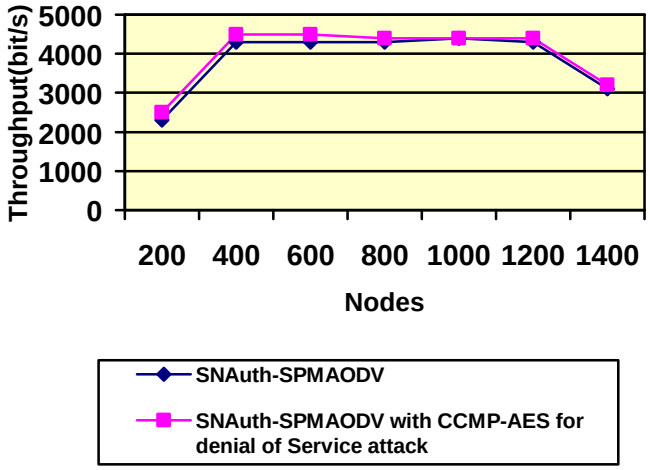

Figure 7(b)

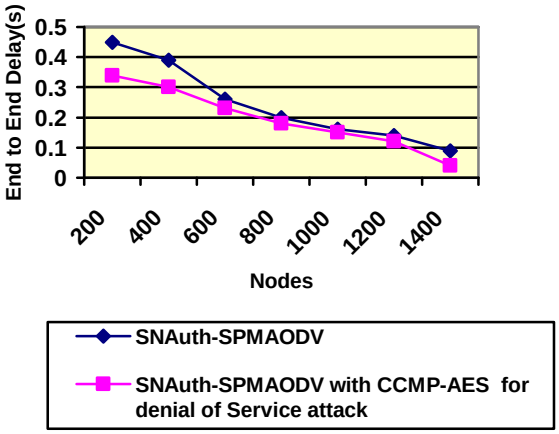

Figure 7(c)

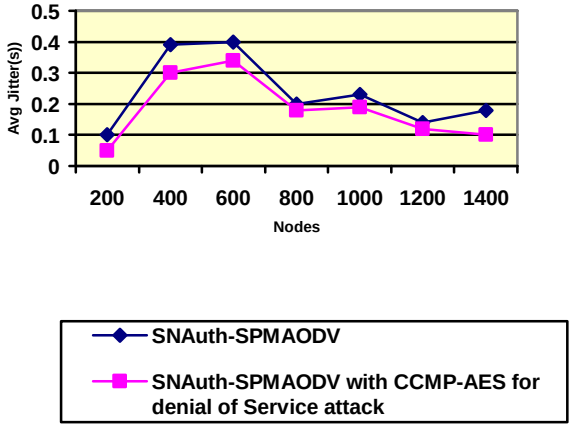

Figure 7(d)

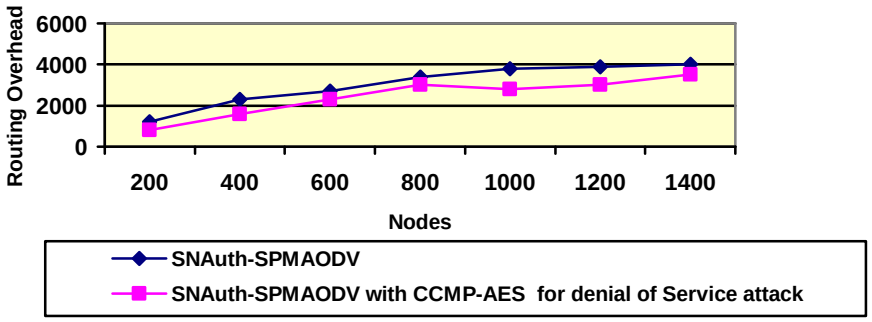

Figure 7(e)

Experimental Results of SNAuth-SPMAODV with DSSS for MANET Physical and network layer security

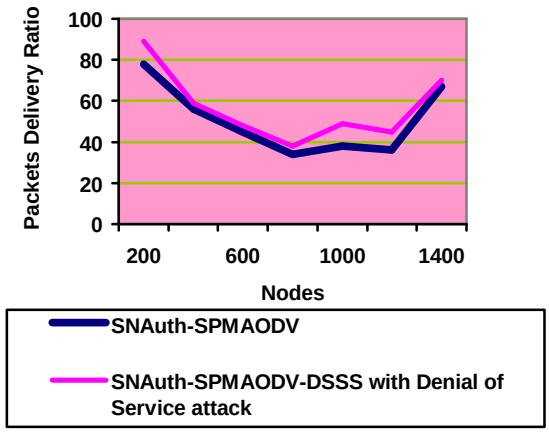

Figure8(a)

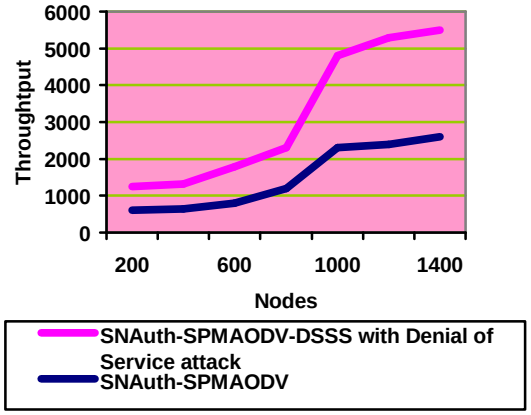

Figure8(b)

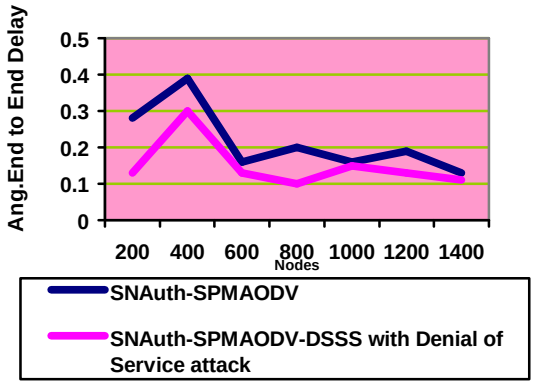

Figure8(c)

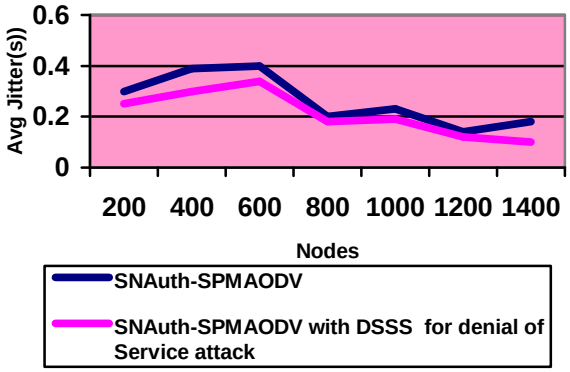

Figure8(d)

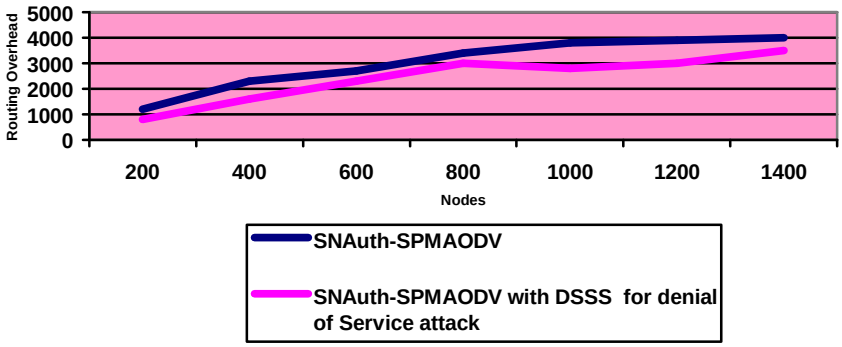

Figure8(e)

RESULTS AND DISCUSSION

Figure 3(a) shows that the packet delivery ratio is higher in SNAuth-SPMAODV compared to AODV under attack and Normal AODV.Figure 3(b) shows that throughput is higher in SNAuth-SPMAODV compared to AODV under attack and Normal AODV.Figure 3(c) shows that Average end to end Delay is lower in SNAuth-SPMAODV compared to AODV under attack and Normal AODV.Figure 3(d) shows that Average Jitter is lower in SNAuth-SPMAODV compared to AODV under attack and Normal AODV. Figure 3(e) shows that Routing Overhead is lower in SNAuth-SPMAODV compared to AODV under attack and Normal AODV. In simulation results, SNAuth-SPMAODV provides good performance with every measurement metric in high network density environment.
Figure 4(a) shows that the packet delivery ratio is higher in SNAuth-SPMAODV with SIP security compared to without SIP security. Figure 4(b) shows that throughput is higher in SNAuth-SPMAODV with SIP security compared to without SIP security. Figure 4(c) shows that Average end to end Delay is lower in SNAuth-SPMAODV with SIP security compared to without SIP security. Figure 4(d) shows that Average Jitter is lower in SNAuth-SPMAODV with SIP security compared to without SIP security. Figure 4(e) shows that Routing Overhead is lower in SNAuth-SPMAODV with SIP security compared to without SIP security. In simulation results, SNAuth-SPMAODV with SIP provides application and network layer security and it offers good performance with every measurement metric in high network density environment.

Figure 5(a) shows that the packet delivery ratio is higher in SNAuth-SPMAODV with WTLS compared to without WTLS.Figure 5(b) shows that throughput is higher in SNAuth-SPMAODV with WTLS compared to without WTLS.Figure 5(c) shows that Average end to end Delay is lower in SNAuth-SPMAODV with WTLS compared to without WTLS . Figure 5(d) shows that Average Jitter is lower in SNAuth-SPMAODV with WTLS compared to without WTLS. Figure 5(e) shows that Routing Overhead is lower in SNAuth-SPMAODV with WTLS compared to without WTLS. 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.

Figure 6(a) shows that the packet delivery ratio is higher in SNAuth-SPMAODV with IPSec compared to without IPSec.Figure 6(b) shows that throughput is higher in SNAuth-SPMAODV with IPSec compared to without IPSec.Figure 6(c) shows that Average end to end Delay is lower in SNAuth-SPMAODV with IPSec compared to without IPSec. Figure 6(d) shows that Average Jitter is lower in SNAuth-SPMAODV with IPSec compared to without IPSec.Figure 6(e) shows that Routing Overhead is lower in SNAuth-SPMAODV with IPSec compared to without IPSec. In simulation results, SNAuth-SPMAODV provide good performance with every measurement metric in high network density environment
Figure 7(a) shows that the packet delivery ratio is higher in SNAuth-SPMAODV with CCMP-AES compared to without CCMP-AES. Figure 7(b) shows that throughput is higher in SNAuth-SPMAODV with CCMP-AES compared to without CCMP-AES.Figure 7(c) shows that Average end to end Delay is lower in SNAuth-SPMAODV with CCMP-AES compared to without CCMP-AES. Figure 7(d) shows that Average Jitter is lower in SNAuth-SPMAODV with CCMP-AES compared to without CCMP-AES .Figure 7(e) shows that Routing Overhead is lower in SNAuth-SPMAODV with CCMP-AES compared to without CCMP-AES. 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.

Figure 8(a) shows that the packet delivery ratio is higher in SNAuth-SPMAODV with DSSS compared to without DSSS.Figure 8(b) shows that throughput is higher in SNAuth-SPMAODV with DSSS compared to without DSSS .Figure 8(c) shows that Average end to end Delay is lower in SNAuth-SPMAODV with DSSS compared to without DSSS. Figure 8(d) shows that Average Jitter is lower in SNAuth-SPMAODV with DSSS compared to without DSSS. Figure 8(e) shows that Routing Overhead is lower in SNAuth-SPMAODV with DSSS compared to without DSSS. Proposed model combines SNAuth-SPMAODV routing protocol with 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 proposed methods is robust against denial of service attack in each layers of MANET for hostile environment.

CONCLUSION

Mobile ad hoc networks (MANETs) can be applied to many situations without the use of any existing network infrastructure or centralized administration. In hostile environment, there is a need for the network to route packets through dynamically mobile nodes. MANETs can be considered as the solution for this highly mobile and dynamic military network. However it is not appropriate to directly apply conventional mobile ad hoc networks scheme to military network, since military communication system is different from conventional counter parts both in device's physical layer specification and networking environment. Therefore consider these particularities of military communication system through simulation, and evaluate the performance of Layerwise security framework on the assumed military environment. In simulation results, the proposed methods provide good performance with every measurement metric in high network density environment.

REFERENCES

[1] 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.

[2] D.Devi Aruna and Dr.P.Subashini, "CCMP-AES Model with SNAuth-SPMAODV Routing Protocol to Secure Link and Network Layer for Mobile Adhoc Networks in Military Scenario" International Journal of Engineering and Advanced Technology (IJEAT) Volume-1, Issue-4, April 2012,pp.230 -236.

[3] 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, pp 265-274.

[4] C.E. Perkins, E.M. Royer & S. Das"Ad Hoc on Demand Distance Vector (AODV) Routing," IETFInternet draft, March 2001

[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, pp.695 – 710, June 2006.

[6] Qualnet Documentation, "Qualnet 5.0 Model Library, Network Security", Available: Http:// Www.Scalablenetworks.Com/Products/Qualnet/Downlaod....

[7] Kamanshis Biswas and Md. Liakat Ali , "Security Threats in Mobile Ad Hoc Network" Department of Interaction and System Design School of Engineering, pp.9-26, march2007

[8] 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 , pp 6-10, 2007.

[9] The WAP Forum, "Wireless Transaction Protocol", Version 10-Jul-2001,

[10] IEEE Standard 802.3, "Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD), Access Method and Physical Layer Specifications," Edition, pp 1 – 302, 2000.

[11] Dr. G. Padmavathi, Dr. P.Subashini and Ms. D. Devi Aruna, "Hybrid Routing Protocols to Secure Network Layer for Mobile Ad Hoc Networks", IEEE, pp. 1– 4, 2010,.

[12] 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.

[13] 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.

[14] Zhang W., Lou L.W., and Fang Y., "Securing mobile ad hoc networks with certificateless public keys," IEEE Transactions on Dependable and Secure Computing,3(4), 386–399, 2006.

[15] Zapata, and Asokan M.G,"Securing Ad hoc Routing Protocols"In: Proc. of the ACM workshop on Wireless security, Atlanta, USA, 1-10, 2002.

[16] Zhou.L., and Haas Z., "Securing Ad Hoc Networks," IEEE Network Magazine, 1999.

[17] Yi S., and Kravets R., "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks". Pre-Proceedings of the 2nd Annual PKI Research Workshop. 2003,

[18] Yi. S., Naldurg.Z,, and Kravets.R, ,"Security-Aware Ad Hoc Routing for Wireless Networks" Proceedings of Second ACM International Symposium on Mobile Ad Hoc Networking and Computing, Urbana, 299-302, 2001.

[19] Sun J.Z., "Mobile Ad-Hoc Networking: An Essential Technology for Pervasive Computing," Proceedings of International conference on info-tech and info-net,3,.316-321, 2001.

[20] Rosenberg.J ," SIP: Session initiation protocol" RFC 3261, IETF,2002.

[21] Rosenberg.J and Schulzrinne H.,"An extension to the session initiation protocol (SIP) for symmetric response routing" RFC 3581, IETF,2003.

[22] Rai A.K., Tewari R.R., and Upadhyay S.K., "Different Types of Attacks on Integrated MANET-Internet Communication" International Journal of Computer Science and Security (IJCSS), 4(3), 265-274. 2010.