SNAuth-SPMAODV with IPSec to secure network layer for Mobile adhoc networks in Military Scenario

[1]D.Devi Aruna [2]Dr.P.Subashini
[1]Research Scholar, Avinashilingam institute for Home Science and Higher Education for Women, Coimbatore
[2]Associate Professor, Department of Computer Science, Avinashilingam institute for Home Science and Higher Education for Women, Coimbatore

ABSTRACT

Mobile Ad Hoc Network (MANET) is a collection of multi-hop wireless mobile nodes that communicate with each other without centralized control or established infrastructure. Establishing an optimal and efficient route between the communicating parties is the primary concern of the routing protocols of MANET. Any attack in routing phase may disrupt the overall communication and the entire network can be paralyzed. Thus, security in network layer plays an important role in the security of the whole network in military communication environments. The primary focus of this work is to estimates the applicability of IPSec into Mobile Ad Hoc Networks (MANET's) to provide security services for both routing information and data message at network layer. This paper considers military scenarios and evaluates the performance of Security-enhanced-Multipath AODV (Ad hoc On-demand Distance Vector Routing) routing protocol called SNAuth-SPMAODV (Secure Neighbor Authentication Strict Priority Multipath Ad hoc On-demand Distance Vector Routing) with IPSec 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 protocol discovers multiple paths between sender and receiver nodes without introducing extra packets into the network and authenticates the neighbor offering robustness in a secured MANET. 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 different parameter metrics.

KEYWORDS

Mobile adhoc network, Denial of Service attack, Strict priority algorithn, Secure neighbor authentication,Internet protocol Security.

1. INTRODUCTION

In recent years, Mobile Adhoc Network (MANET) has received marvelous attentions due to self-design, self maintenance, and cooperative environments [11]. 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 have 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. Particularly Denial of Service attack is one such severe attack against ad hoc routing protocols which is a challenging one to defend against. The vital goal of the security solutions for MANETs is to provide security services, such as confidentiality, integrity, anonymity, authentication and availability, to mobile users [6]. To achieve the goals, the security solutions spanning the entire protocol stack. DoS attacks can be launched against any layer in the network protocol stack [17]. The proposed work focuses on MANET's network layer security and the primary goal is to develop a security mechanism for protecting both the routing information and the data message at network layer.

The paper is organized in such a way that Chapter 2 discusses about the available literature. Chapter 3 discusses the proposed method, Chapter 4 discusses problem statement Chapter 5 discusses simulation model and Chapter 6 gives the conclusion.

2. REVIEW OF LITERATURE

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

2.1 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 [12].

S ↔A↔ B↔ M ↔C↔ D↔ X

Figure 1: Denial of Service attack

2.2 Route Selection

Proactive routing protocols generate routes and store them for later use. On- demand routing protocols only generate routes when necessary. The later 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 [3].

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 [14]. This protocol is composed of two mechanism (1) Route Discovery and (2) Route Maintenance. AODV uses **R**oute **Req**uest (RREQ), **R**oute **Rep**ly (RREP) control messages in Route Discovery phase and **R**oute **Err**or (RERR) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in [15]. 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. At this stage eventually, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be received. Figure 2 depicts the traversal of control messages.

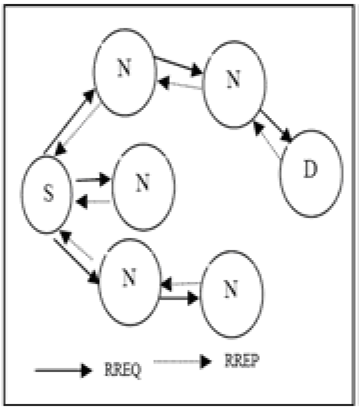

Figure 2: Traversal of Control Messages

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.

2.3 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.

2.4 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 <RESPONSE 1, 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 <RESPONSE 2, 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 RESPONSE 2 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

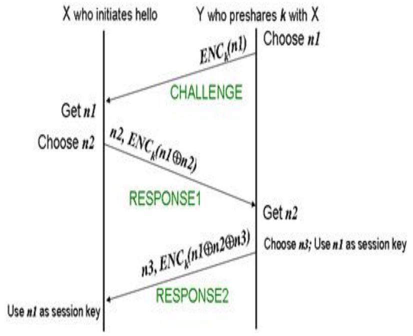

Figure 3: Challenge-Response Protocol-Three way handshake

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.

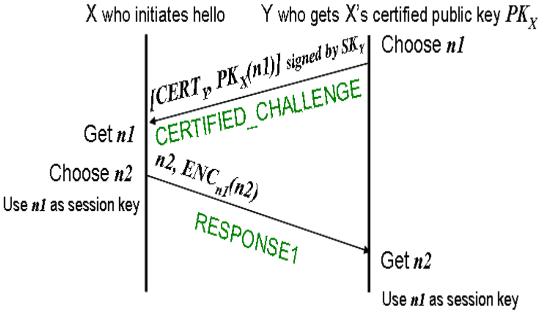

Figure 4: Challenge-Response Handshake

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'.

2.5 IPsec in MANETs for Network Layer Security

IP security (IPSec) developed by Internet Engineering Task Force (IETF) is a suite of protocols used to secure traffic at the IP layer. The main protocol components of IPSec are Authentication Header (AH) and Encapsulating Security Payload (ESP), which describe the IP header extensions for carrying cryptographically protected data, and Internet Key Exchange (IKE). IPSec is based on Security Associations (SAs). A security association is a simple connection whose traffic is protected by security service designated by parameters such as the encryption algorithm, keys, and lifetime[1]. SA is uniquely identified by a tuple of Security Parameter Index (SPI), destination IP address, and IPSec protocol (AH or ESP). IPSec protocol is based on the establishment of Security Association between packet sender and receiver. SA is set up in the IKE phase by Diffie- Hellman (DH) algorithm. This preconfigured shared secret can then be available in most MANET systems, and is essential for adopting IPSec secure communications and membership verification. Upon the establishment of membership management mechanism and the corresponding trust model in MANET, IPSec can be an appropriate choice for MANET network layer to protect both routing information and data message. For IPsec to work, communication entities must share a public key. This key exchange process is accomplished through key management mechanisms that refer to the creation, distribution, installation, authentication, and access control of the keying material. A number of cryptographic algorithms are also specified in IPsec for authentication and encryption [2]. IPSec can be used in two different ways. It can be used end-to-end, in which case the source and destination hosts for a datagram are responsible for all cryptographic processing. It can also be used via gateways, in which case a system near the source host is responsible for applying cryptographic operations on behalf of the source, while a system near the destination is responsible for checking and decryption[6].

3. PROPOSED METHODOLOGY

Proposed method combines IPSec with SNAuth-SPMAODV.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. 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. In this context, several research approaches have concluded that the usage of IPSec is appropriate in MANETs. It is widely accepted that IPSec is one of the best security protocols available at present and it is mentioned as the most reliable and efficient network layer protocol. For many applications, security at the network layer has a number of advantages over security provided elsewhere in the protocol stack [6].

4. 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 and provide network layer security 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 I summarizes these differences in terms of a physical layer model [18]. 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 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*

5. SIMULATION MODEL

Using the QualNet network simulator [7], 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 [18]. 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,Throughput,IPSec-In Packet processed and IPSec- Out Packet Processed

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 Table2 (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

Following are the simulation results that demonstrate SNAuth-SPMAODV-IPSec outperforms with SNAuth-SPMAODV routing protocol in MANETs.

Fig.5 shows that Packet delivery ratio is higher in IPSec-SNAuth-SPMAODV compared to SNAuth-SPMAODV routing protocol

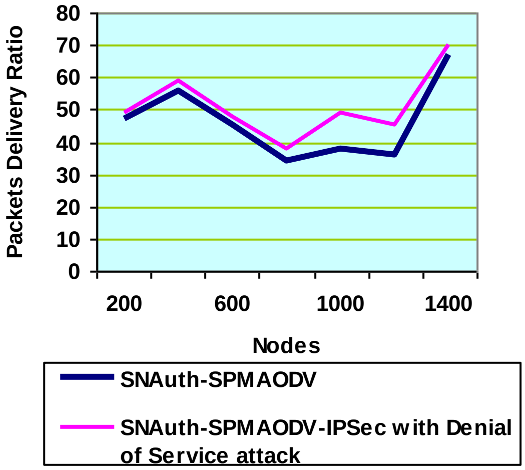

Fig.5.Packets Delivery Ratio is higher in IPSec SNAuth-SPMAODV compared SNAuth-SPMAODV

Fig.6 shows that Throughput is higher in IPSec-SNAuth-SPMAODV compared to SNAuth-SPMAODV.

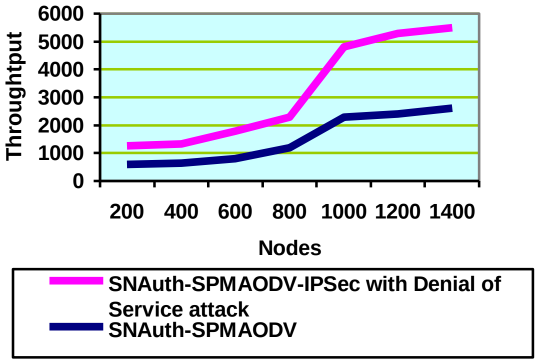

Fig.6Throughput is higher in IPSec- SNAuth-SPMAODV compared to SNAuth-SPMAODV.

Fig.7 shows that Avg.End-to-End delay is lower in IPSec- SNAuth-SPMAODV compared to SNAuth-SPMAODV.

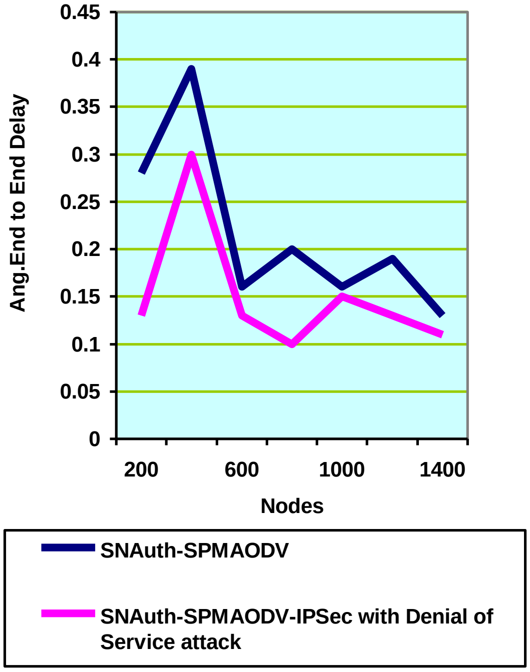

Fig.7. Avg.End-to-End delay is higher in IPSec- SNAuth-SPMAODV Compared SNAuth-SPMAODV

Fig.8 shows that IPSec-IN Packet Processed is higher in IPSec- SNAuth-SPMAODV compared to SNAuth-SPMAODV

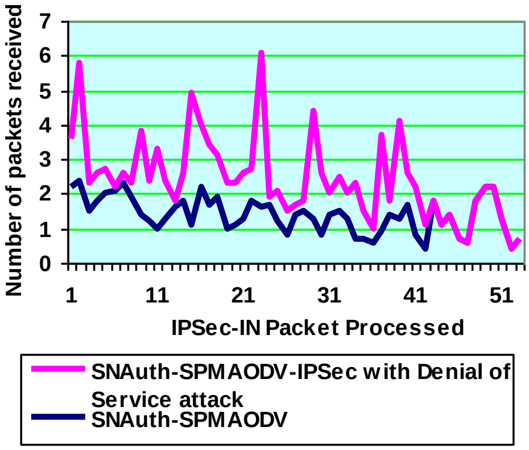

Fig.8. IPSec-IN Packet Processed is higher in IPSec- SNAuth-SPMAODV compared to SNAuth-SPMAODV

Fig.9 shows that IPSec-OUT Packet Processed is higher in IPSec- SNAuth-SPMAODV compared to SNAuth-SPMAODV

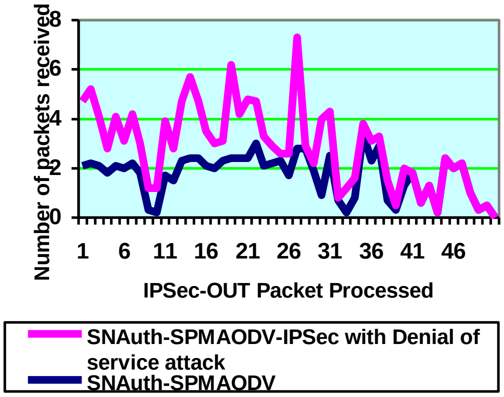

Fig.9. IPSec-OUT Packet Processed is higher in IPSec- SNAuth-SPMAODV compared to SNAuth-SPMAODV.

6. CONCLUSION

Mobile ad hoc networks (MANETs) can be applied to many situations without the use of any existing network infrastructure or centralized administration. In military 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 these particularities of military communication system has been considered for simulation, and the performance of proposed method has been evaluated on the assumed military environment. In simulation results, SNAuth-SPMAODV provide good performance with every measurement metric in high network density environment. This paper estimates the applicability of IPSec for MANET network layer to provide security services for both routing information and data message. The simulation results show that IPSec-SNAuth-SPMAODV outperforms with SNAuth-SPMAODV. The experiments are carried out using the simulator Qualnet version 4.5. This suggests that IPSec would be a better choice for MANET due to the reason that it can provide security protection for both routing information and data message simultaneously.

REFERENCES

1. Joshua D. Guttmann, Amy L. Herzog, and F. Javier Thayer,*"* *Authentication and Confidentiality via IPsec*" Springer LNCS, 30 June 2000.

2. Matt Blaze, John Ioannidis, Angelos D. Keromytis,*"Trust Management for IPsec"* Dept. of Electrical & Computer Engineering, Michigan Tech, Houghton, 1999, pp.103 – 118.

3. S. Corson and J. Macker, Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations (Internet-draft), in: *Mobile Ad-hoc Network (MANET) Working Group, IETF* (1998).

4. S. R. Das, R. Castaneda, J. Yan, and R. Sengupta, "Comparative performance evaluation of routing protocols for mobile, ad hoc networks," in Proceedings of 7th International Conference on Computer Communications and Networks (IC3N '98), USA, October 1998, pp.153 161

5. S. Ramanathan and M. Steenstrup, A survey of routing techniques for mobile communication networks, Mobile Networks and Applications (1996),pp 89–104.

6. Dr. G. Padmavathi, Dr. P.Subashini And Ms. D. Devi Aruna, "Hybrid Routing Protocols To Secure Network Layer For Mobile Ad Hoc Networks", IEEE, 2010.pp. 1 - 4

7. Qualnet Documentation, “Qualnet 5.0 Model Library, Network Security”, Available: Http:// Www.Scalablenetworks.Com/Products/Qualnet/ Downlaod....

8.Hoang Lan Nguyen, Uyen Trang Ngu,” A study of different types of attacks on multicast in mobile ad hoc networks” ,Elsevier journal –No. 6 (2008) pp 32–46.

9..M.K. Denko, “A Localized Architecture for Detecting Denial of Service (DoS) Attacks in Wireless AdHoc Networks”, In Proc. IFIP INTELLCOMM'05, Montreal, Canada, pp.135-146

10. 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

11.Dr.G.Padmavathi, Dr.P.Subashini, and Ms.D.Devi Aruna, Impact of Wormhole Attacks and Performance Study of Different Routing Protocols in Mobile Ad Hoc Networks, Journal of Information Assurance and Security, 2010,pp. 094-101

12. 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.

13. 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

14. A. Boukerche,” Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks”, Mobile Networks and Applications 9, Netherlands, 2004, pp. 333-342

15. A.E. Mahmoud, R. Khalaf & A, Kayssi,” *Performance Comparison of the AODV and DSDV Routing Protocols in Mobile Ad-Hoc Networks”,* Lebanon, 2007

16.Kamanshis Biswas and Md. Liakat Ali , “Security Threats in Mobile Ad Hoc Network” Department of Interaction and System Design School of Engineering, ,march2007, pp 9-26

17. 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, pp 6-10.

18. 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.

19. 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.

	Ms.D.Devi Aruna. received MCA Degree from Avinashilingam University for Women, Coimbatore in 2008 respectively and pursuing her Ph.D in same University. She has three years of research experience in UGC project. Her research interests are cryptography and Network Security. She has 17 publications at national and international level
	Dr. P. Subashini, Associate Professor, Dept. of Computer Science, Avinashilingam Deemed University have 19 years of teaching and research experience. Her research has spanned a large number of disciplines like Image analysis, Pattern recognition, neural networks, and applications to Digital Image processing. Under her supervision she has seven research project of worth one crore from various funding agencies like DRDO, DST and UGC