SNAuth-SPMAODV with SIP to secure application and network layer in Mobile adhoc network for 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*-A mobile ad-hoc network (MANET) is a wireless network where nodes can communicate with each other without infrastructure. Due to this nature of MANET, some malicious and selfish nodes that try compromise the routing protocol functionality and makes MANET vulnerable to Denial of Service attack in military communication environments. This paper considers military scenarios and evaluates the performance of security-enhanced-Multicast 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 Session Initiation Protocol (SIP) provides application layer and network layer security and authenticates the neighbor is robust against Denial of Service attack.The SNAuth-SPMAODV protocol has been implemented and simulated on Qualnet 5.0.The performance metrics used to evaluate the proposed method such as packet delivery ratio, end to end delay, throughput, routing overhead and jitter.**

Keywords - Mobile adhoc network, Denial of Service attack, Strict priority algorithn, Secure neighbor authentication, Session Initiation Protocol Security.

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[2]. 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 [9]. DoS attacks can be launched against any layer in the network protocol stack particularly application layer which is a challenging one to defend against. In this type of attack, an attacker attempts to prevent legitimate and authorized users from the services offered by the network [8]. The proposed method provides application layer security and is robust against denial of service attack. The objective is to test the performance of SNAuth-SPMAODV with SIP security and without SIP security.

Table 1 describes the security issues in each layer [9]. The paper is organized in such a way that Chapter 2 discusses

Review of literature Chapter 3 discusses the proposed method, Chapter 4 discusses problem statement and Chapter 5 gives simulation model Chapter 6 gives the conclusion.

TABLE 1: LAYERWISE SECURITY CHALLENGES

Layer	Security issue
Application Layer	Detecting And Preventing Viruses, Worms, Malicious Codes, And Application Abuses.
Transport Layer	Authentication And Securing End-To-End Communications Through Data Encryption.
Network layer	Protecting The Ad Hoc Routing And Forwarding Protocols.
Link Layer	Protecting The Wireless Mac Protocol And Providing Link- Layer Security Support
Physical Layer	Preventing Signal Jamming Denial-Of-Service Attacks.

2. 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].

S ↔A↔ B↔ M ↔C↔ D↔ X

Fig 1: Denial of Service attack

3. PROPOSED METHOD

This chapter briefly describes the proposed method which combines Secure Neighbor Authentication Strict Priority Multicast Ad hoc On-demand Distance Vector Routing (SNAuth-SPMAODV) and Session Initiation protocol (SIP).

Route Selection

Proactive routing protocols generate routes and store them for later use. On- demand routing protocols only generate routes when necessary [4]. 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.

A. 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 till it breaks, after which a new route setup is initiated [4]. 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 [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 [5]. 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

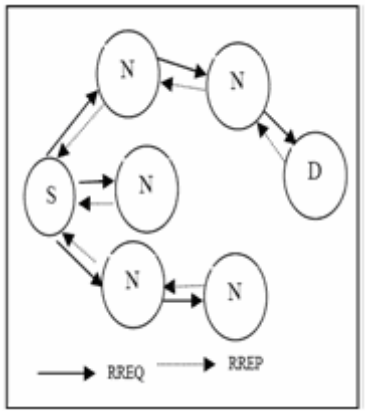

Figure 2: Traversal of Control Messages

B.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[6]. 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 .

C.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 certain upper bound which is derivable. Additionally, the proper selection of routes using a strict priority multipath protocol can increase further the network throughput.

D. 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 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

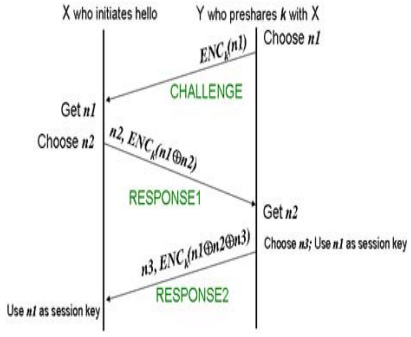

Figure 3: Challenge-Response Protocol-Three way handshake

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.

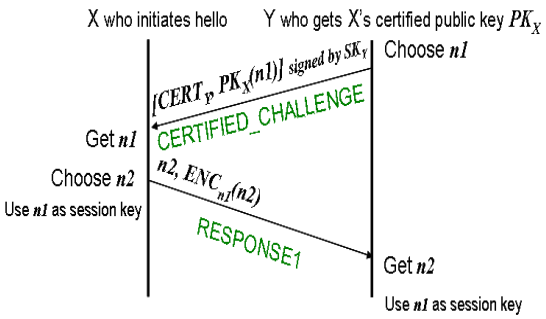

Fig 4: Challenge-Response Handshake

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'.

E. Session Initiation Protocol

Session Initiation Protocol (SIP) is an application layer control protocol used for establishing, modifying and tearing down multimedia sessions, both unicast and multicast. It has been standardized within the IETF for the invitation to multicast conferences and Internet telephone calls .The most important SIP operation is that of inviting new participants to a call. To achieve this functionality we can distinguish different SIP entities[11]:

Proxy server: A proxy server receives a request and then forwards it towards the current location of the callee either directly to the callee or to another server that might be better informed about the actual location of the callee.

Redirect server: A redirect server receives a request and informs the caller about the next hop server. The caller then contacts the next hop server directly.

User Agent (UA): A logical entity in the terminal equipment that can act as both a User Agent Client (UAC) and a User Agent Server (UAS).

Register: The register server is mainly thought to be a database containing locations as well as user preferences as indicated by the user agents. In detail, a SIP call setup is essentially a 3-way handshake between a caller (UAC) and a callee (UAS). For instance, the main legs are an INVITE (to initiate a call) message, a 200 OK (to communicate a definitive successful response) message and an ACK (to acknowledge the response) message. However, implementations can make use of provisional responses, such as 180 RINGING message. 180 RINGING message indicates that the callee (UAS) receiving the INVITE message is trying to alert the user. The call setup is followed by the actual media transfer (speech and video) using the Real-time Transport Protocol (RTP). The release of the call is made by means of the BYE message and the successful call release can be communicated through a 200 OK message [10].

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 provide application layer security and is robust against denial of service attack and it 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.

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 application layer security in military environment. 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 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 2 summarizes these differences in terms of a physical layer model[13]. 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 2: 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. 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.

Comparison of SNAuth-SPMAODV with SIP and without SIP for denial of service attack.

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 Table3 (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 3: 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

Figure 5 shows that throughput is higher in SNAuth-SPMAODV with SIP security for Denial of service attack and without SIP Security.

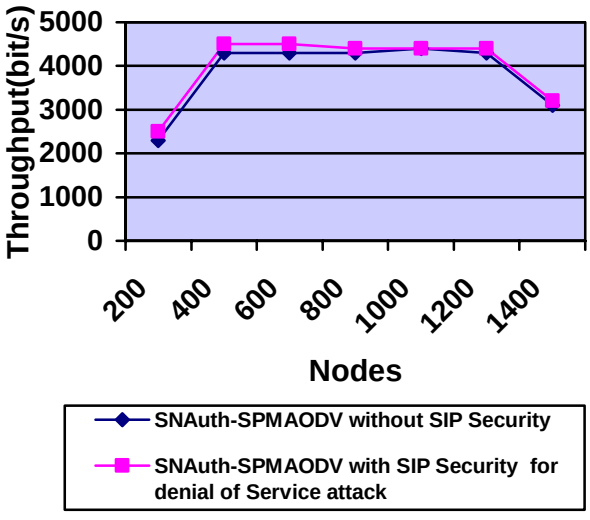

Figure 5: Comparison of Throughput of SNAuth-SPMAODV with SIP Security for Denial of service attack and without SIP Security

Figure 6 show that packet delivery ratio is higher in SNAuth-SPMAODV with SIP security for Denial of service attack and without SIP Security.

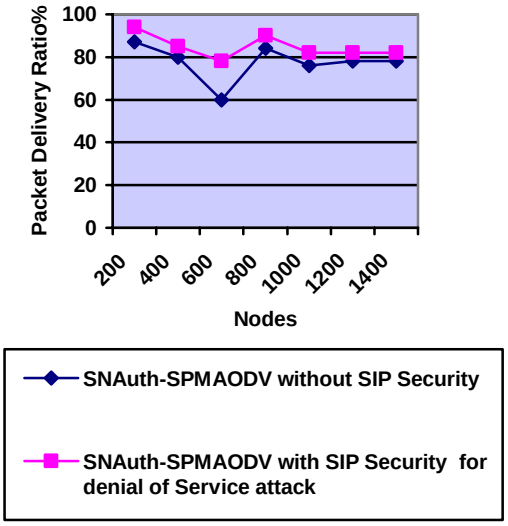

Figure 6: Comparison of Packet delivery ratio of SNAuth-SPMAODV with SIP Security and without SIP Security

Figure 7 show that End to End delay is lower in SNAuth-SPMAODV with SIP security for Denial of service attack and without SIP Security.

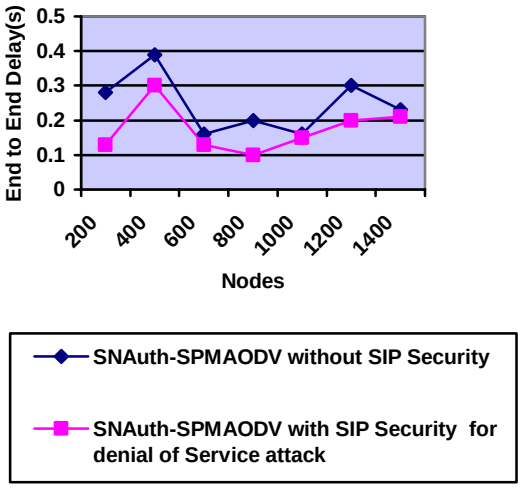

Figure 7: Comparison of End to End delay of SNAuth-SPMAODV with SIP Security and without SIP Security

Figure 8 show that Routing Overhead is lower in SNAuth-SPMAODV with SIP security for Denial of service attack and without SIP Security.

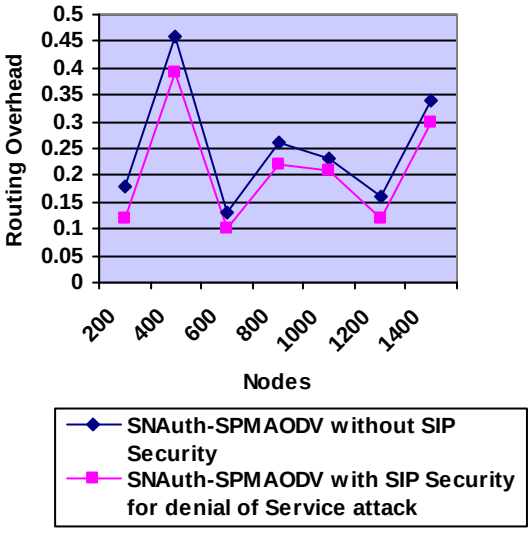

Figure8: Comparison of routing overhead of SNAuth-SPMAODV with SIP Security and without SIP Security

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 consider these particularities of military communication system to out simulation, and evaluate the performance of proposed method on the assumed military environment. 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.

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. 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,

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

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

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

8.4. 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,

9. 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,

10.J. Rosenberg et al.: "SIP: Session initiation Protocol" ,RFC 3261,June 2002. www.ietf.org.

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 12 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

11. Li and Louise Lamont "Support of Multimedia SIP Applications in Mobile Ad hoc Network: Service Discovery and Networking Architecture" IEEE GLOBECOM, 2005, pp 3682-3286

12..Xiaoyan Zhang, Xiaofeng Du, Zygmunt Haas, "Performance Evaluation of Sip-Based Session Establishment Over DSR-Routed Manets," MILCOM- 2006, pp.1-7.

13. 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.

14. 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.