

Securing Physical and network layer using SNAuth-SPMAODV with DSSS for Mobile adhoc networks in Military Scenario

D.Devi Aruna¹ Dr.P.Subashini²

¹Research Scholar, Avinashilingam institute for Home Science and Higher Education for Women, Coimbatore

²Associate Professor, Department of Computer Science, Avinashilingam institute for Home Science and Higher Education for Women, Coimbatore

Abstract-A mobile ad hoc network is an infrastructure less network, fast emerging today for deployment in variety of applications. 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 network and physical layer which is a challenging one to defend against in military communication environments.. The physical layer protocol in MANETs is responsible for bit-level transmission between network nodes and network layer is responsible to provide security services for both routing information and data message. This paper consider military scenarios and evaluate 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 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.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. SNAuth-SPMAODV with DSSS is found to be a good security solution even with its known security problems. The simulation is done using network simulator Qualnet 5.0 for different number of mobile nodes. The proposed model has shown improved results in terms of Average throughput, Average end to end delay, Average packet delivery ratio, Routing overhead and Average jitter.

Keywords- Mobile adhoc network,Denial of Service attack,Strict priority algorithm,Secure neighbor authentication, Direct Sequence Spread Spectrum

1. INTRODUCTION

In recent years, Mobile ad hoc Networks has started gaining attention from the industrial and academic research community due to their wide deployment and inherent nature of solving practical real world applications[5]. Many military and commercial applications have emerged due to the simplicity of the networks and widespread adoption of the technology. Most of the previous ad hoc network researchers have focused on problems such as routing and reliable communication, made a trusted environment. However, many applications in reality run only in untrusted environments and secured routing became a challenging one. Applications that may require secure communications include emergency response operations, military or police networks, safety critical business operations such as oil drilling platforms or mining operations[10]. For example, in emergency response operations such as the one after a natural disaster like a flood, tornado, hurricane and earthquake, when regular communication networks are damaged due to natural disasters, emergency rescue teams have to rely upon ad hoc networks for communication. To fend off malicious attackers in these emergency situations, many safety critical applications require secure communication. Ad hoc networks generally use a wireless radio communication channel. The main advantage of such networks is low cost deployment and maintenance. Today, the nodes and wireless hardware are inexpensive and readily available [11]. The network is automatically self configuring and self maintaining nature. Generally, wireless networks are vulnerable to several attacks. Particularly Denial of Service attack is one such severe attack against network and physical layer which is a challenging one to defend against. The physical layer protocol in MANETs is responsible for bit-level transmission between network nodes and network layer is responsible to provide security services for both routing information and data message [3]. The 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.

Securing Physical and network layer using SNAAuth-SPMAODV with DSSS for Mobile adhoc networks in Military Scenario

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 Chapter 5 discusses simulation model and Chapter 6 gives experimental results, Chapter 7 discusses 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 a 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 figure 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 [6].

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[7]. 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[8].

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 till it breaks, after which a new route setup is initiated [9]. 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 [9]. 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.

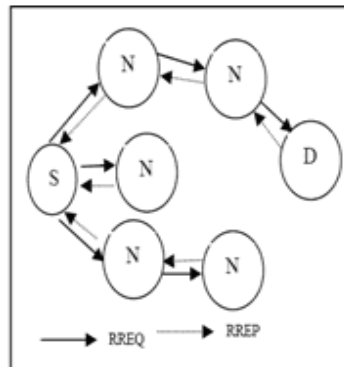


Figure 2: Traversal of Control Messages

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. 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 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

Securing Physical and network layer using SNAuth-SPMAODV with DSSS for Mobile adhoc networks in Military Scenario

selects a random nonce n_3 and sends out a confirmation response $\langle \text{RESPONSE2}, Y, n_3, \text{ENC}_k(n_1 \text{ XOR } n_2 \text{ XOR } n_3) \rangle$ to X.

d. Upon receiving the RESPONSE2 message, X decrypts $\text{ENC}_k(n_1 \text{ XOR } n_2 \text{ XOR } n_3)$ and obtains $n_1 \text{ XOR } n_2 \text{ XOR } n_3$. If this matches the result of XORing n_1 that is previously decrypted, its own n_2 and n_3 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

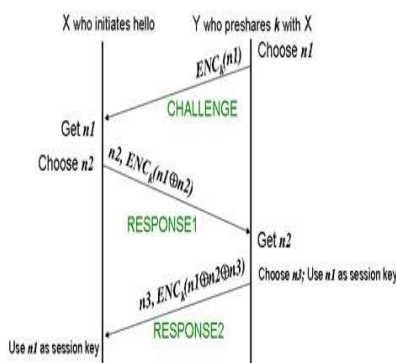


Figure 3: Challenge-Response Protocol-Three way handshake

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 n_1 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 $\text{CERT}_x = [X, \text{certified public key } PK_x, \text{certificate valid time}]$ in a CERTIFIED_HELLO message. For Y's CHALLENGE, Y uses PK_x to encrypt n_1 and obtains ciphertext $PK_x(n_1)$. Y must also add its own certificate $\text{CERT}_y = [Y, \text{certified public key } PK_y, \text{certificate valid time}]$ and sign the entire message with its own private key SK_y . 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.

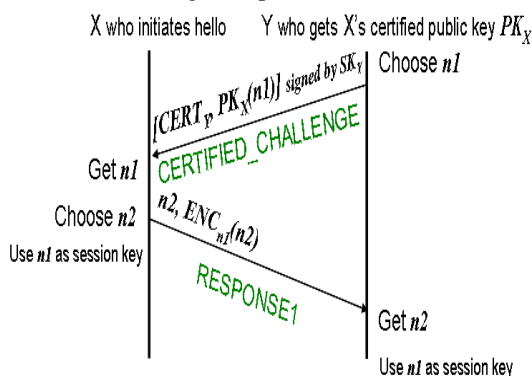


Figure 4: Challenge-Response Handshake

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'.

G.Direct Sequence Spread Spectrum (DSSS) is a modulation technique. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated[3].

Features

DSSS phase-modulates a sine wave pseudo randomly with a continuous string of pseudo noise (PN) code symbols called "chips", each of which has a much shorter duration than an information bit. That is, each information bit is modulated by a sequence of much faster chips. Therefore, the chip rate is much higher than the information signal bit rate.

DSSS uses a signal structure in which the sequence of chips produced by the transmitter is known *a priori* by the receiver. The receiver can then use the same PN sequence to counteract the effect of the PN sequence on the received signal in order to reconstruct the information signal.

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 and physical layer security in military environment. Most of such performance analysis 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 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.

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

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 provide physical layer security 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



Securing Physical and network layer using SNAuth-SPMAODV with DSSS for Mobile adhoc networks in Military Scenario

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 [14], 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 ratio, average end-to-end delay, routing overhead and Throughput.

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

EXPERIMENTAL RESULTS

Packet Delivery Ratio

From the Figure 5, it is shown that the proposed scheme (SNAuth-SPMAODV with DSSS) gives better Packet Delivery Ratio compared to SNAuth-SPMAODV with varying network size.

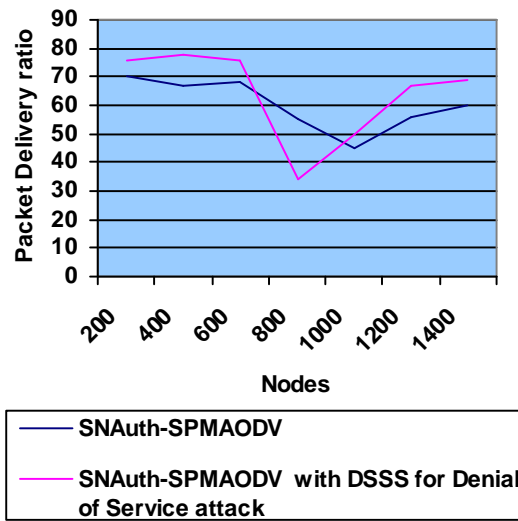


Figure 5 - SNAAuth-SPMAODV with DSSS Packet delivery ratio

Throughput

Figure 6 demonstrates the throughput for SNAAuth-SPMAODV with DSSS. It is clear that it has a good performance compared to SNAAuth-SPMAODV with DSSS with varying network size and malicious nodes.

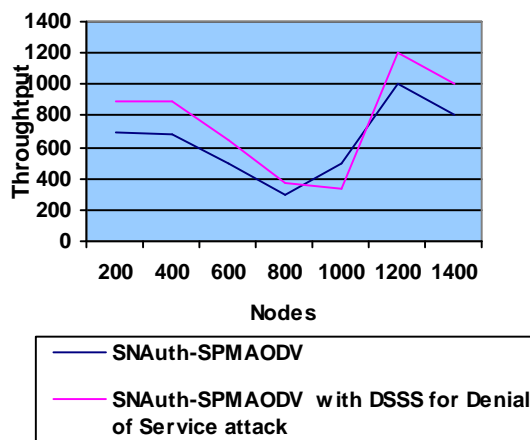


Figure 6 - SNAAuth-SPMAODV with DSSS Throughput

Routing Overhead

Figure 7 shows that Routing Overhead is lower in SNAAuth-SPMAODV with DSSS for Denial of service attack and SNAAuth-SPMAODV with varying network size and malicious nodes. Hence the Routing Overhead by malicious node has been minimized.

Securing Physical and network layer using SNAuth-SPMAODV with DSSS for Mobile adhoc networks in Military Scenario

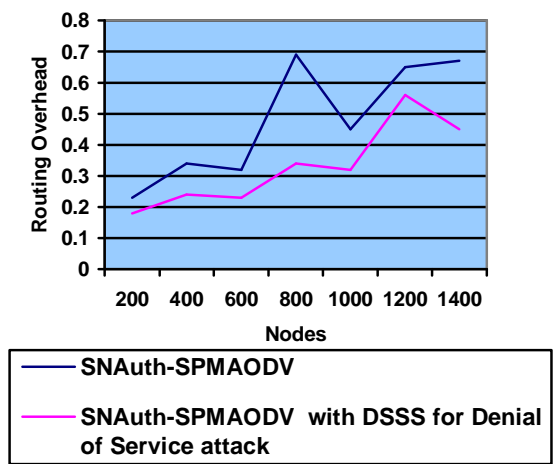


Figure 7- SNAuth-SPMAODV with DSSS Routing Overhead

8.4 Avg.End to End Delay

Figure 8 show that Avg.End to End Delay is lower in SNAuth-SPMAODV with DSSS for Denial of service attack and SNAuth-SPMAODV with varying network size and malicious nodes.

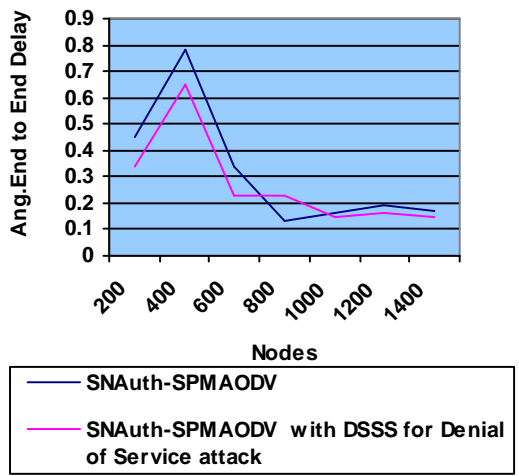


Figure 8- SNAuth-SPMAODV with DSSS Avg.End to End delay

Avg.Jitter

Figure 9 show that Avg.Jitter is lower in SNAuth-SPMAODV with DSSS for Denial of service attack and SNAuth-SPMAODV with varying network size and malicious nodes.

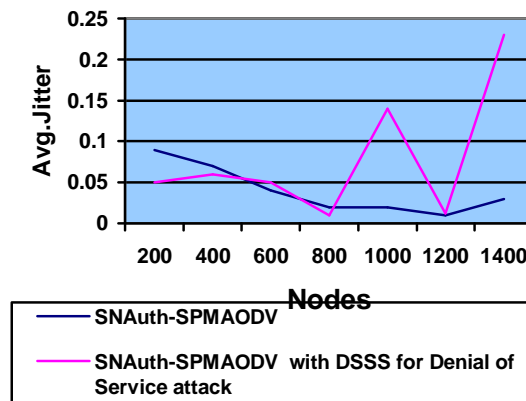


Figure 9- SNAAuth-SPMAODV with DSSS Avg.jitter

CONCLUSION



Mobile Adhoc network is a collection of mobile nodes without infrastructure. 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 network and physical layer which is a challenging one to defend against. The physical layer protocol in MANETs is responsible for bit-level transmission between network nodes and network layer is responsible to provide security services for both routing information and data message. The proposed model combines SNAAuth-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. SNAAuth-SPMAODV with DSSS is found to be a good security solution even with its known security problems.

REFERENCES

1. IEEE Standard 802.3, "Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD), Access Method and Physical Layer Specifications," 2000 Edition, pp 1 - 302.
2. IEEE Standard 802.11b-1999 (Supplement to ANSI/IEEE Standard 802.11, 1999 Edition).
3. Dr. G. Padmavathi, Dr. P. Subashini And Ms. D. Devi Aruna, "DSSS with ISAKMP key Management Protocol to secure physical layer for Mobile Adhoc network" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012, pp 69 - 76.
4. Hao Yang, Haiyun Lou, 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
5. 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.
6. 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.
7. C.E. Perkins, E.M. Royer & S. Das, Ad Hoc On Demand Distance Vector (AODV) Routing, IETF Internet draft, draft-ietf-manet-aodv-08.txt, March 2001
8. A. Boukerche, "Performance Evaluation of Routing Protocols for Ad Hoc Wireless Networks", Mobile Networks and Applications 9, Netherlands, 2004, pp. 333-342
9. A.E. Mahmoud, R. Khalaf & A. Kayssi, "Performance Comparison of the AODV and DSDV Routing Protocols in Mobile Ad-Hoc Networks", Lebanon, 2007
10. Kamanshis Biswas and Md. Liakat Ali, "Security Threats in Mobile Ad Hoc Network" Department of Interaction and System Design School of Engineering, march 2007, pp 9-26,
11. 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
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.

Securing Physical and network layer using SNAAuth-SPMAODV with DSSS for Mobile adhoc networks in Military Scenario

14. Qualnet Documentation, "Qualnet 5.0 Model Library, Network Security", Available: [Http://
www.Scalablenetworks.Com/Products/Qualnet/Downlaod...](http://www.Scalablenetworks.Com/Products/Qualnet/Downlaod...)

	<p>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.</p>
	<p>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</p>