Securing Transport and Network layer using SNAuth-SPMAODV with WTLS in Mobile adhoc networks 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 peer-to-peer wireless network where nodes can communicate with each other without any infrastructure. Due to this nature of MANET, it is possible that there could be some malicious and selfish nodes that try to compromise the routing protocol functionality and makes MANET vulnerable to Denial of Service attack in military communication environments. The ultimate goal of the security solutions for MANET is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability to mobile users. To achieve the goals, the security solution should provide complete protection across the entire protocol stack. The primary focus of this work 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. This paper considers military scenarios and evaluate 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 WTLS to minimize the packet dropping by Denial of Service attack**

(DoS) in the network by applying WTLS in SNAuth-SPMAODV routing protocols and compared the results without WTLS protocols. 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 results demonstrates the success of the proposed approach and maximizes the overall performance of MANET in presence of Denial of Service attack.

Keywords- Mobile adhoc network, Denial of Service attack, Strict priority algorithn, Secure neighbor authentication Transport layer security.

1. INTRODUCTION

In recent years, Mobile ad hoc Networks start gaining attention from the industrial and academic research community due to their wide deployment and inherent nature of solving practical real world applications [9]. 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 in 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. 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[10]. 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. The network is automatically self configuring and self maintaining nature. Generally, wireless networks are vulnerable to several attacks [12]. Particularly most challenging attack to defend against is a Denial of Service attack. taken for proposed Method.

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

2. REVIEW OF LITERATURE

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

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 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 [11].

S ↔A↔ B↔ M ↔C↔ D↔ X

Figure 1: Denial of Service attack

B. Route Selection

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

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 [5]. 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[7]. 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.

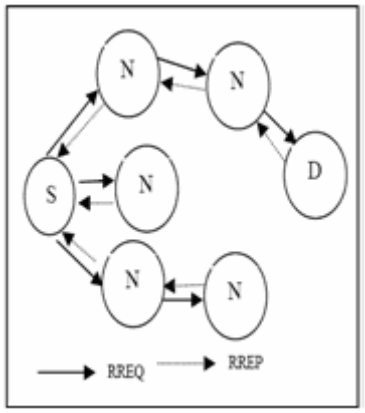

Fig 2: Traversal of Control Messages

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[7]. 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 selects a random nonce n3 and sends out a confirmation response <RESPONSE2, Y, n3, ENC_k (n1 XOR n2 XOR n3)> to X.

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

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

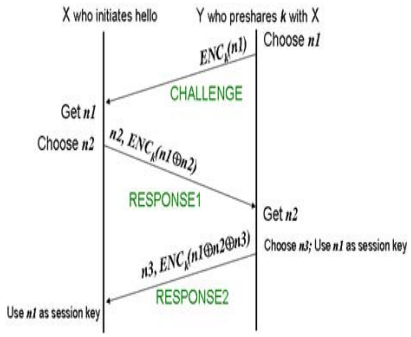

Fig 3: Challenge-Response Protocol-Three way handshake

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 Three Way Challenge-Response Handshake.

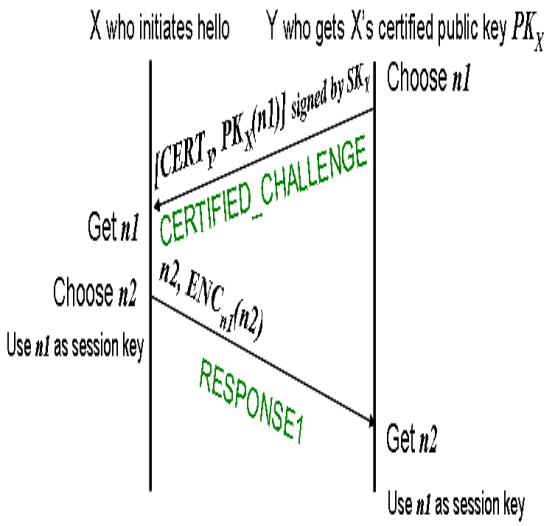

Fig 4: Challenge-Response Handshake

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'.

G.Transport Layer security in Mobile Adhoc Networks

The security issues associated to transport layer are authentication, end-to-end Communications through data encryption, handling delays and packet loss. The MANET transport layer protocols provide end-to-end connection, reliable packet delivery, flow control and congestion control. The nodes in a MANET are also susceptible to the Denial of Service (DoS) attacks. The wide use of mobile communication has created an important demand for value-added services. WAP (Wireless Application Protocol) is a framework for developing applications to run over wireless networks. WAP is developed by an international industry-wide organization called the WAP Forum. WTLS (Wireless Transport Layer Security) is the security protocol of the WAP protocol suite. WTLS operates over the transport layer and provides end-to-end security, where one end is the mobile client, and the other end is the WAP gateway[1]. WAP gateway acts as a proxy of the mobile client to access an application server hosted somewhere on the Internet. The communication beyond the WAP gateway is conducted using the regular Internet (TCP/IP) protocol suite. A set of handshake messages is exchanged in order to set up a secure environment between the mobile client and the server (WAP gateway). Cryptographic algorithms, keys and related parameters are negotiated during the handshake. Once the handshake messages are exchanged and session key is generated, all WTLS and upper layer protocol messages can be exchanged in encrypted form. In this way, confidentiality and integrity are provided. Authentication is an optional service in WTLS [2]. Authentication is provided if the parties provide digital certificates during the handshake. Certificates are digital identities that contain public-keys to be used during the key exchange. Certificates are issued by trusted Certification Authorities (CA) with a digital signature on the certificate content. Validation of a certificate means the legitimacy of the enclosed public-key. A party, who does not have a certificate, should use an unapproved public-key. Therefore, that party cannot be authenticated. Certificate validation, authentication and session key exchange use asymmetric public-key cryptosystems that require computation-intensive processes, and are therefore slow. Speed is inversely proportional to the key size used in public-key cryptosystems. Since the processing power of mobile clients is limited, relatively smaller keys are selected for WTLS. Moreover, data transfer rate is also limited in mobile communication environment and using smaller keys would help to save bandwidth[3].

Public-key cryptosystems in WTLS

Public-key cryptosystem operations employ two different, but related keys: public-key and private-key. Public-key operations are for encryption and signature verification. Private-key operations are for decryption and signature issuance. Key exchange operations are also public-key cryptosystem operations, but their nature depends on the cryptosystem used. Public-key cryptosystems are used in the WTLS handshake for key exchange and certificate verification purposes. Authentication is mechanically provided when key exchange is performed using certified keys. WTLS supports two public-key cryptosystems: RSA (Rivest- Shamir-Adleman) and ECC (Elliptic Curve Cryptography).

Public-key cryptosystems is used for key exchange and certificate verification. Regular DH (Diffie-Hellman) [6] method is proposed as another key exchange mechanism in WTLS standard. However, the standard proposes only DH method for completely anonymous handshakes, in which neither client nor server use certificates to authenticate themselves. Anonymous handshakes are vulnerable to man-in-the-middle-attacks, where an adversary impersonates both parties. Therefore, we do not consider anonymous handshakes as secure methods and do not include them in our performance evaluation. Besides DH, WTLS also propose anonymous versions of RSA and ECDH methods that disregard as well. Certificate verification is a public-key operation. Where both RSA and ECC can be used. If ECC is to be used, ECDSA (Elliptic Curve Digital Signature Algorithm) is employed. If RSA is to be used, its verification feature is employed. Certificate generation, which is signature issuance, is not a part of WTLS protocol.

Key exchange suites of WTLS

WTLS uses the term key exchange group to specify the public-key cryptosystem pair to be used for certificate validation and key exchange. WTLS supports numerous alternative key exchange suites. However, only two of them offer an acceptable level of security; namely, ECDH_ECDSA and RSA key exchange suites.

1. ECDH_ECDSA: ECDSA is used for certificate verification. Certificates that include ECDH parameters are used for key exchange.
2. RSA: RSA cryptosystem is used for both certificate verification and key exchange.

3. PROPOSED METHODOLOGY

The proposed method reduces dependency on single nodes and routes; it discovers multiple paths between sender and receiver nodes. It has the advantages of a multipath protocol without introducing extra packets into the network and authenticates the neighbor offering robustness in a secured MANET. It can be used to offset the dynamic and unpredictable configuration of ad-hoc networks. They can also provide load balancing by spreading traffic along multiple routes, fault-tolerance by providing route resilience, and higher aggregate bandwidth in military environment. 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. SNAuth-SPMAODV with WTLS is found to be a good security solution even with its known security problems.

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 transport 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 I summarizes these differences in terms of a physical layer model [14]. 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 [8], 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.

Results and Analysis

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

TABLE 2: NETWORK SIZES AND AREAS

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

6. EXPERIMENTAL RESULTS

6.1 Packet Delivery Ratio

From the Figure 5, it is shown that the proposed scheme (WTLS-SNAuth-SPMAODV) gives better Packet Delivery Ratio compared to SNAuth-SPMAODV without WTLS, with varying network size and malicious nodes. Hence the number of data packets dropping by malicious node has been minimized

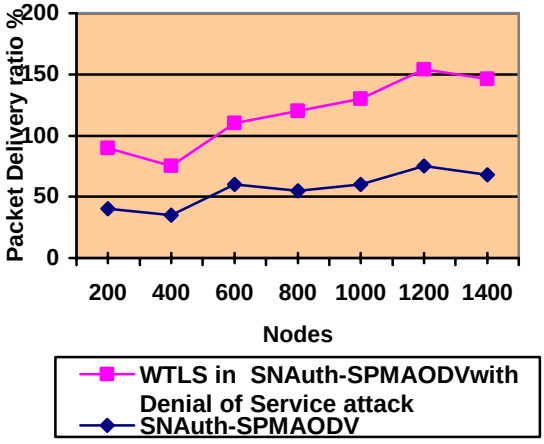

Fig 6.1-WTLS- SNAuth-SPMAODV Packet delivery ratio

6.2 Throughput

Figure 6 demonstrates the throughput for SNAuth-SPMAODV (without WTLS) and SNAuth-SPMAODV with WTLS. It is clear that SNAuth-SPMAODV with WTLS has a good performance compared to SNAuth-SPMAODV without WTLS, with varying network size and malicious nodes.

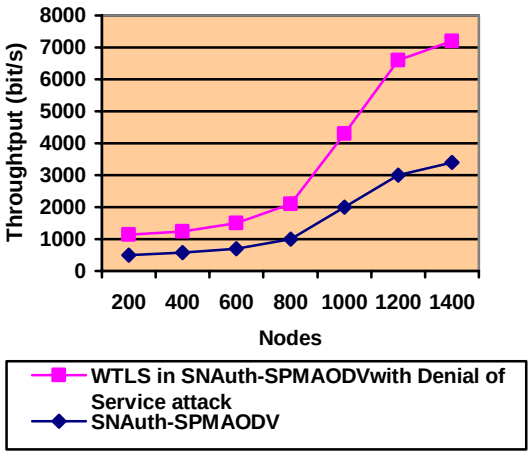

Fig 6.2 -WTLS-AODV Throughput

6.3 Total Packet Dropped

There are several reasons for packet drops. In the given situation as we have increased number of nodes and malicious nodes. Figure 7 shown that the proposed method (SNAuth-SPMAODV with WTLS) gives lowest packet dropped than the SNAuth-SPMAODV without WTLS protocol.

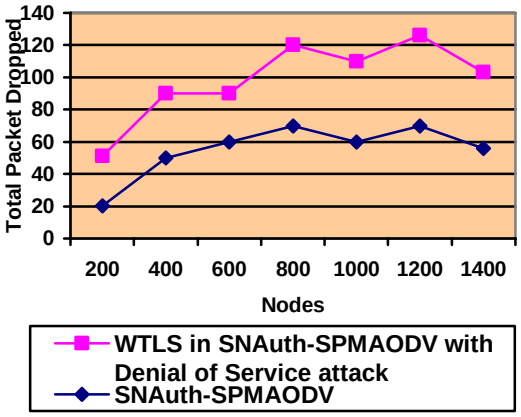

Fig 6.3-WTLS-AODV Total packet dropped

6.4 Routing Overhead

Figure 8 show that Routing Overhead is lower in SNAuth-SPMAODV with WTLS for Denial of service attack and without WTLS with varying network size and malicious nodes. Hence the Routing Overhead by malicious node has been minimized

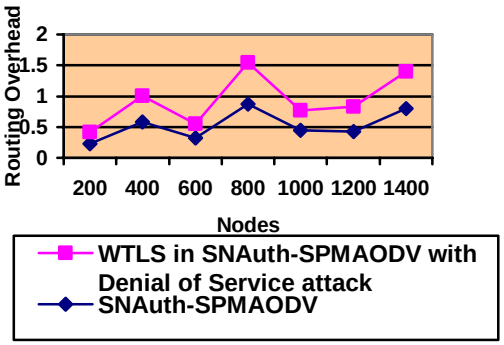

Fig 6.4-WTLS-AODV Routing Overhead

7. CONCLUSION

Mobile Ad Hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure. Secure, reliable and efficient routing operations in MANET a challenging task. Hence the suitable key management solution clubbed with the routing protocol may be a better option. The primary focus of this work 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 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. The simulation results demonstrate the success of the proposed approach and maximize the overall performance of MANET in presence of Denial of Service attack.

REFERENCES

1. K. Sundresses, V. Anantharaman, H. Y. Hsieh, and R. Sivakumar. ATP,*" A Reliable Transport Protocol for Ad Hoc Networks***"**. In Proceedings of ACM MOBIHOC 2003, June 2003, pp. 64-75,

2.Kahraman, Gokhan," *An Investigation of WAP Transaction Protocol Performance for Packet Radio Network's***,** Master Thesis, Electrical and Electronics Engineering, Graduate School of Natural and Applied Sciences, The Middle East Technical University, Ankara, Turkey, April 2002

3. The WAP Forum, **"***Wireless Transaction Protocol"*, Version 10-Jul-2001, http://www.wapforum.org

4. B. Aerobic, R. Curtmola, H. Rubens, D. Holmer, and C. Nita-Rotaru, **"***On the survivability of routing protocols in ad hoc wireless networks*," IEEE, 2005.

5. 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

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

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

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

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

9. 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

10.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.

11. 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

12.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.

13. Wenjia Li and Anupam Joshi,"Security Issues in Mobile Ad Hoc Network" - A Survey, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County , 2007, page 6-10.

14. 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.

15. 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.