ZRP with WTLS Key Management Technique to Secure Transport and Network Layers in Mobile Adhoc Networks

Dr.G.Padmavathi[1], Dr.P.Subashini[2], and Ms.D.Devi Aruna[3]

[1]Professor and Head, Department of Computer Science,
Avinashiligam University for Women, Coimbatore – 641 043
ganapathi.padmavathi@gmail.com

[2]Associate Professor, Department of Computer Science,
Avinashilingam University for Women, Coimbatore – 641 043
mail.p.subashini@gmail.com

[3]Project fellow, Department of Computer Science,
Avinashiligam University for Women, Coimbatore – 641 043
deviaruna2007@gmail.com

ABSTRACT

A mobile ad hoc network (MANETs) is a self-organizing network that consists of mobile nodes that are connected through wireless media. A number of unique features, such as lack of infrastructural or central administrative supports, dynamic network topologies, open communication channels, and limited device capabilities and bandwidths, have made secure, reliable and efficient routing operations in MANET a challenging task. 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 need for 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. It also handles delay and packet loss. The MANET transport layer protocols provide end-to-end connection, reliable packet delivery, flow control and congestion control. The proposed model combines Zone Routing Protocol(ZRP) with Wireless Transport Layer Security(WTLS) provides authentication, privacy and integrity of packets in both routing and transport layers of MANET and also to defend against Denial of Service(DoS) attack.ZRP with WTLS 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 and Average jitter.

KEYWORDS

MANET,WTLS,ZRP,Denial of Service attack.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) have received marvelous attention because of their self-maintenance capabilities. While early research effort assumed a friendly environment and paying attention on problems such as multihop routing and wireless channel access, security has become a main concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has extensive been an active research topic in wireline networks, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include shared wireless medium, stringent resource constraints, open network architecture and highly dynamic network topology. So, the existing security solutions for wired networks do not directly apply to the MANET domain.

DOI : 10.5121/ijwmn.2012.4109

The vital goal of the security solutions for MANETs is to provide security services, such as confidentiality, integrity, authentication, anonymity, and availability, to mobile users. To achieve the goals, the security solution need for complete protocol stack. DoS attacks can be launched against any layer in the network protocol stack particularly transport 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 Table 1 describes the security issues in each layer. The proposed model combines hybrid routing protocol ZRP with WTLS to defend against DoS attack and it also provides *authentication, privacy and integrity* of packets in both routing and transport layer of MANET. The primary focus of this work is to provide transport layer security for authentication, securing end-to-end communications through data encryption, handling delays, packet loss and so on. The MANET transport layer protocols provide end-to-end connection, congestion control, reliable packet delivery and flow control.

Table 1: Layer wise Security Challenges

Layer	**Security issues**
Application layer	Detecting and preventing viruses, worms, malicious codes, and application abuses
Transport layer	Authenticating 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

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

II. REVIEW OF LITERATURE

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

1. Denial of Service attack

An attacker attempts to stop authorized and legitimate users from the services obtainable by the network. A denial of service (DoS) attack can be carried out in many ways. The typical way is to flood packets to any centralized resource present in the network so that the resource is no longer accessible to nodes in the network, as a result of which the network no longer function in the manner in which it is designed to operate. This may lead to a failure in the delivery of certain services to the end users. 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 contribute 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 serious 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 [6][7][9].

S ↔A↔ B↔ M ↔C↔ D↔ X

Figure 1. Denial of Service attack

2. Related Work

The following list of papers show the relative work carried out for MANET attacks and the possible solutions.

1) Wormhole Attack Detection in Wireless Sensor Networks: This paper discusses the nature of wormhole attack and existing methods of defending mechanism and then proposes round trip time (RTT) and neighbor numbers based wormhole detection mechanism [14].

2) Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks: The main characteristic of the proposed system is its capability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then it proceeds to protect the network [16].

3) A Distributed Security Scheme for Ad Hoc Networks: It discusses the DoS attack like flooding using AODV protocol and concludes with an direct enhancement to make the limit-parameters adaptive in nature. [13].

4) A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments: This considers an integrated protocol called secure routing against collusion (SRAC), in which a node makes a routing decision based on its trust of its neighboring nodes [15].

5) Detecting Network Intrusions via Sampling: A Game Theoretic Approach: This paper discusses the problem of detecting an intruding packet in a communication network [12].

The majority of the related study covers only few network layer attacks,In the proposed approach, attempts to identify transport layer attacks and it provides authentication and secure end-to-end communication.

III. PROPOSED METHOD

This chapter briefly describes proposed method combines Zone Based Routing protocol (ZRP) and transport Layer security in Mobile Adhoc Networks.

Routing protocols can be classified mainly into three types proactive, reactive and hybrid routing protocols. Proactive routing protocols maintain routing information all the time and always update the routes by broadcasting update messages. However, reactive routing is started only if there is a demand to reach another node. Reactive protocols acquire routing information

only when it is actually needed. Hybrid protocols combine the advantages of proactive and of reactive routing. The widely used hybrid routing protocol Zone Based Routing protocol (ZRP) is taken for the proposed work. It is considered to be the most suited one for ad hoc networks [2][3]. A brief description of the ZRP routing protocol is given below.

1. Zone Routing Protocol (ZRP)

Zone Routing Protocol (ZRP) uses both a proactive and a reactive routing .ZRP was first introduced by Haas in 1997. ZRP is proposed to decrease the reactive routing protocols latency caused by route discovery and to reduce the proactive routing protocols control overhead. ZRP defines a zone around each node consisting of its k-neighborhood (e. g. k=3). In ZRP, the distance and a node, all nodes within hop distance from node belong to the routing zone of node. It is formed by two sub-protocols, a proactive routing protocol: Intra-zone Routing Protocol (IARP), is used inside routing zones and a reactive routing protocol: Inter-zone Routing Protocol (IERP), is used between routing zones, respectively. A route to a destination within the local zone can be established from the proactively cached routing table of the source by IARP; therefore, if the source and destination is in the same zone, the packet can be delivered immediately.

Route discovery happens reactively when routes beyond the local zone. The source node sends a route requests to its border nodes, containing its own address, the destination address and a unique sequence number. Border nodes are nodes which are exactly the maximum number of hops to the defined local zone away from the source. The border nodes check their local zone for the destination. If the requested node is not a member of this local zone, the node adds its own address to the route request packet and forwards the packet to its border nodes. If the destination is a member of the local zone of the node, it sends a route reply on the reverse path back to the source. The source node uses the path saved in the route reply packet to send data packets to the destination [5][10].

Advantages: Provides scalability.

Disadvantages: Routing security in mobile Adhoc networks.

2. Transport Layer security in Mobile Adhoc Networks

The MANET transport layer protocols provide end-to-end connection, reliable packet delivery, flow control and congestion control. The security issues associated to transport layer are handling delays, authentication, end-to-end Communications through data encryption, and packet loss. 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 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 WAP gateway and the other end is the mobile client. WAP gateway acts as a proxy of the mobile client to access an application server hosted anywhere 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 server (WAP gateway) and mobile client. 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. 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. Authentication, certificate validation, 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. Furthermore, data transfer rate is also limited in mobile communication environment and using smaller keys would help to save bandwidth [1][2].

Public-key cryptosystems in WTLS

Public-key cryptosystem operations use two different keys: public-key and private-key. Public-key operations are for signature verification and encryption. Private-key operations are for signature issuance and decryption. 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: ECC (Elliptic Curve Cryptography) and RSA (Rivest- Shamir-Adleman).Public-key cryptosystems is used for key exchange and certificate verification .If RSA is to be used for key exchange, If ECC is to be used, ECDH (Elliptic Curve Diffie-Hellman) key exchange method is employed. Regular DH (Diffie-Hellman) [6] method is proposed as another key exchange mechanism in WTLS standard. 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 we disregard as well. Certificate verification is a public-key operation. Both RSA and ECC can be used. If RSA is to be used, its verification feature is employed. If ECC is to be used, ECDSA (Elliptic Curve Digital Signature Algorithm) is employed. [3].

Key exchange suites of WTLS

WTLS supports numerous alternative key exchange suites. However, only two of them offer an acceptable level of security:

RSA and ECDH_ECDSA key exchange suites.

1. ECDH_ECDSA: ECDSA is used for certificate verification.

2. RSA: RSA cryptosystem is used for both key exchange and certificate verification

IV. EXPERIMENTATION AND EVALUATION

Qualnet5.0 network simulator is used for experimentation. Mobility scenarios are generated using a Random waypoint model by varying 10 to 50 nodes moving in a terrain area of 1500m x 1500m. The image of the network as it appears in Qualnet 5.0 is presented in Figure-2. The simulation parameters are summarized in Table 2.

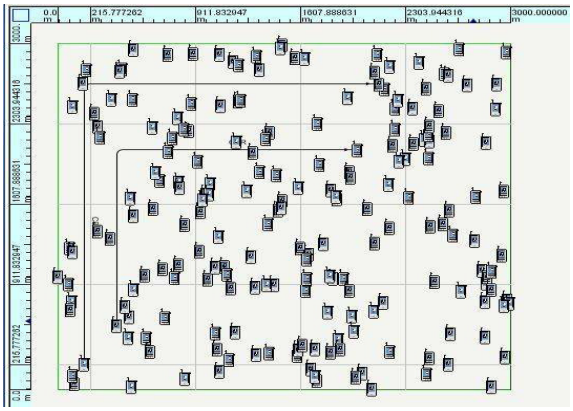

Figure2. The image of the network as it appears in Qualnet 5.0

Table2. Simulation Parameters

Parameter	**Value**
Simulator	Qualnet 5.0
Simulation time	100 s
Number of nodes	50
Traffic Model	CBR
Pause time	2 (s)
Maximum mobility	60 m/s
No. of sources	15
Terrain area	1500m x 1500m
Transmission Range	250m

The simulation is done to investigate the performance of the network with various parameters. The metrics used to evaluate the performance are:

1) Average packet delivery ratio
2) Average end-to-end delay
3) Average delay jitter
4) Average throughput

Average packet delivery ratio: The packet delivery ratio (PDR) of a receiver is defined as the ratio of the number of data packets actually received over the number of data packets transmitted by the senders.

Average end-to-end delay: The end-to-end delay of a packet is defined as the packet takes a time to travel from the source to the destination. The average end-to-end delay is the average of the end-to-end delays taken over all the received packets Eqn (1) is used to find the end to end delay of the packet.

$$delay = \frac{1}{nbx} \sum_{i \in x} \sum_{iey} \frac{delay_j}{nby} \quad \text{---- (1)}$$

x: is the set of destination nodes that received data packets.

nbx: is the number of receiver nodes

y: is the set of packets received by node i as the final destination.

Average delay jitter: Delay jitter is the variation (difference) of the inter-arrival times between the two successive packets received. Each receiver calculates the average per-source delay jitter from the received packets originated from the same source. The receiver then takes the average over all the sources to obtain the average per-receiver delay jitter.

Average throughput: The throughput of a receiver (per-receiver throughput) is defined as the ratio of the number of bits received over the time difference between the first and the last received packets. The average throughput is the average of the per-receiver throughputs taken over all the receivers. Eqn (2) is used to find the throughput of the packet.

$$Throuhput(\%) = \frac{\text{Re}ceivedpackets}{Sentpackets} * 100 \text{ ---(2)}$$

Performance comparison of routing protocol ZRP and WTLS for ZRP routing protocol with Denial of Service attack

The different parameters are considered for evaluation. Average packet delivery ratio, Average throughput, should be higher and Average end-to-end delay, Average delay jitter must be lower.Figure 3 shows that Average packet delivery ratio is higher in WTLS with ZRP with Denial of Service attack compared to ZRP. Figure 4 shows that Throughput is higher in WTLS with ZRP with Denial of Service attack compared to ZRP. Figure 5 shows that Average Jitter is lower in WTLS with ZRP with Denial of Service attack compared to ZRP. Figure 6 shows that End to End Delay is lower in WTLS with ZRP with Denial of Service attack compared to ZRP.

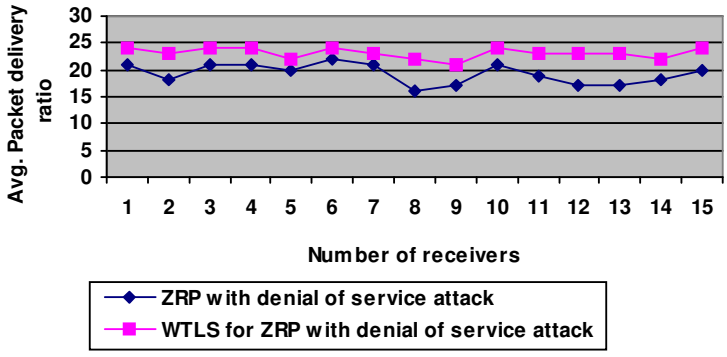

Figure 3. Comparison of Average packet delivery ratio of ZRP and ZRP for WTLS with Denial of Service attack

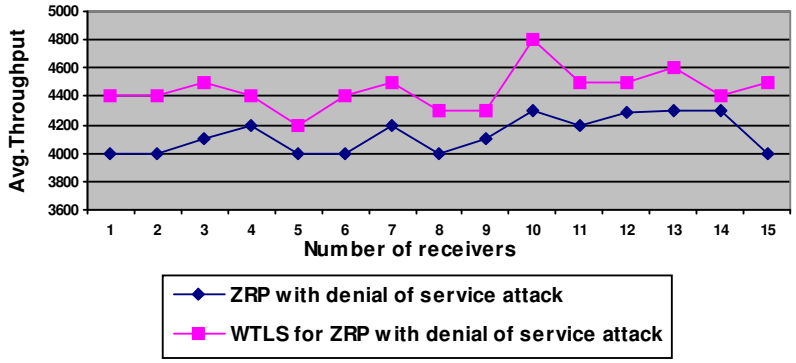

Figure 4. Comparison of Throughput of ZRP and ZRP for WTLS with Denial of Service attack

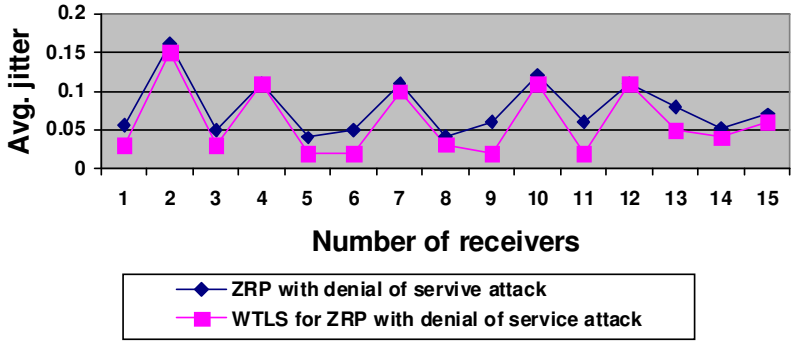

Figure 5: Comparison of Average Jitter of ZRP and ZRP for WTLS with Denial of Service attack

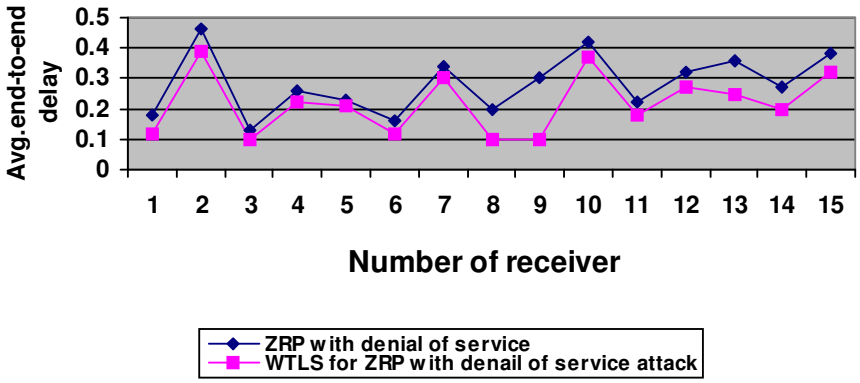

Figure 6: Comparison of End to End delay of ZRP and ZRP for WTLS with Denial of Service attack

From the simulation results it is observed that proposed model is robust against denial of service attacks and it also provides authentication, securing end-to-end communications through data encryption, handling delays, packet loss in routing and transport layer of MANET.

V. CONCLUSION

A mobile ad hoc network (MANET) is a self-organizing network consisting of mobile nodes that are connected through wireless media. A number of unique features, such as lack of infrastructural or central administrative supports, dynamic network topologies, open communication channels, and limited device capabilities and bandwidths, have made secure, reliable and efficient routing operations in MANET a challenging task. 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 this goal, the security solution need for whole protocol stack. The main focus of this work is to provide transport layer security for authentication, securing end-to-end communications through data encryption, packet loss and handling delays, The MANET transport layer protocols provides end-to-end connection, reliable packet delivery, flow control and congestion control. The proposed model combines hybrid routing protocol ZRP with WTLS to defend against Denial of Service(DoS) attack and it also provides authentication, privacy and integrity of packets in both routing and transport layers of MANET.

ACKNOWLEDGMENT

The authors would like to thank the University Grants Commission (UGC) for supporting this Major Research project (MRP).

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, pp. 64-75, June 2003.

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. Z. J. Haas, M. Perlman, "***The Performance of Query Control Schemes of Zonal Routing Protocol***", *IEEE Trans. on Networking*, vol. 9, no. 4, pp. 427-438(2001).

6. M.K. Denko, "***A Localized Architecture for Detecting Denial of Service (DoS) Attacks in Wireless Ad Hoc Networks",*** In Proc. IFIP INTELLCOMM'05, Montreal, Canada.

7. Aad, J.P, Hubaux, and E.W. Knightly, "***Denial of Service Resilience in Ad Hoc Networks"***, ACM MOBICOM 2004, Philadelphia, PA, USA.

8. V. Gupta, S. Krishnamurthy, and M. Faloutsos," ***Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks".*** In Proc. of MILCOM, 2002.

9. A. Habib, M. H. Hafeeda, and B. Bhargava, "***Detecting Service Violation and DoS Attacks"***, In Proc. of Network and Distributed System Security Symposium (NDSS), 2003.

10***. Zone Routing Protocol (ZRP) for Ad Hoc Networks***", *IETF* Internet Draft, Version 4, July 2002.

11. Prince Samar, Marc Pearlman and Zygmunt Haas, "***Independent Zone Routing: An Adaptive Hybrid Routing Framework for Wireless Networks***", *IEEE/ACM* Transactions on Networking, 12, No. 4, August 2004. pp: 599.

12. Murali Kodialam T. V. Lakshman, "***Detecting Network Intrusions via Sampling: A Game Theoretic Approach***", IEEE INFOCOM, 2003.

13. Dhaval Gada, Rajat Gogri, Punit Rathod, Zalak Dedhia and Nirali Mody Sugata Sanyal, Ajith Abraham, "***A Distributed Security Scheme for Ad Hoc Networks***", ACM Publications, Vol-11, Issue 1, 2004, pp. 5 – 5.

14.Zawtun and Aung Htein Maw, "***Wormhole attack detection in wireless sensor networks"***, World Academy of Science, Engineering and Technology, 46, 2008.

15.Ming Yu; Mengchu Zhou; Wei Su, ***"A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments"***, IEEE Transactions on Vehicular Technology Vol-58, Issue 1, Jan. 2009 , pp.449 – 460.

16. Nasser, N.; Yunfeng Chen, "***Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad Hoc Networks***", IEEE International Conference on Communications, ICC apos; Vol-07 , Issue 24-28 June 2007 , pp.1154 – 1159.

17. Oscar F. Gonzalez, God win Ansa, Michael Howarth, and George Pavlou, "***Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks",*** Journal of Internet Engineering, vol-2, 2008, pp.1.

Dr. Padmavathi Ganapathi is the Professor and Head of Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 23 years of teaching experience and one year Industrial experience. Her areas of interest include Network security and Cryptography and real time communication. She has more than 110 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA.

Dr. Subashini is the Associate professor in Department of Computer Science, Avinashilingam Deemed University for Women, Coimbatore. She has 18 years of teaching experience. Her areas of interest include Object oriented technology, Data mining, Image processing, Pattern recognition. She has 95 publications at national and International level**.**

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 is currently working as a Project Fellow in UGC project in Department of Computer Science in the same University and has three year of research experience. Her research interests are cryptography and Network Security. She has 12 publications at national and international level.