CCMP-AES Model with DSR routing protocol to secure Link layer and Network layer in Mobile Adhoc Networks

Dr.G.Padmavathi, Dr.P.Subashini, and Ms.D.Devi Aruna

Professor and Head, Department of Computer Science,
Avinashiligam University for Women, Coimbatore – 641 043

Associate Professor, Department of Computer Science,
Avinashilingam University for Women, Coimbatore – 641 043

Project fellow, Department of Computer Science,
Avinashiligam University for Women, Coimbatore – 641 043

ABSTRACT

Mobile Adhoc network is a special kind of wireless networks. It is a collection of mobile nodes without having aid of established infrastructure. Mobile Adhoc network are vulnerable to attacks compared to wired networks due to limited physical security, volatile network topologies, power-constrained operations, intrinsic requirement of mutual trust among all nodes. During deployment, security emerges as a central requirement due to many attacks that affects the performance of the ad hoc networks. Particularly Black hole attack is one such severe attack against ad hoc routing protocols which is a challenging one to defend against. The proposed model combines the On demand routing protocol DSR with CCMP-AES mode to defend against black hole attack and it also provides confidentiality and authentication of packets in both routing and link layers of MANET. The primary focus of this work is to provide security mechanisms while transmitting data frames in a node to node manner. The security protocol CCMP-AES working in data link layer keeps data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination. The simulation is done for different number of mobile nodes using network simulator qualnet 5.0. The proposed model has shown better results in terms of Total bytes received, packet delivery ratio, throughput, End to End delay and Average jitter.

Keywords

MANET, CCMP-AES, DSR, Blackhole attack

1. INTRODUCTION

In recent years, Mobile Adhoc Network (MANET) has received marvelous attentions due to self-design, self-maintenance, and cooperative environments [4][5][6]. In MANET, all the nodes are mobile nodes and the topology will change rapidly. Here, the mobile devices such as PDAs and laptops are used to route the data packets. In MANET, all the nodes actively discover the topology and the message is transmitted to the destination over multiple hop. The important characteristics of MANETs are lack of infrastructure, dynamic topology, multi-hop communication and distributed coordination among all the nodes. The potential deployment of MANET exists in many scenarios, for example in situations where the infrastructure is not feasible such as disaster relief and cyclone, etc. The

MANET have potential of realizing a free, ubiquitous, and omni directional communication. The wireless channels can be accessible by both legitimate users and malicious users. In such environments, there is no guarantee that a route between the two nodes will be free for the malicious users, which will not comply with the employed protocol. The malicious users will attempt to harm the network operations. During deployment, security emerges as a central requirement due to many attacks that affect the performance of the ad hoc network. Particularly Black hole attack is one such severe attack against ad hoc routing protocols which is a challenging one to defend against. The proposed model combines the On demand routing protocol DSR with CCMP-AES model to defend against black hole attack and it provide confidentiality and authentication of packets in both routing and data link layers of MANETs. The primary focus of this work is to provide security mechanisms applied in transmitting data frames in a node-to node manner through the security protocol CCMP-AES working in data link layer. It keeps data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination.

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.

2. REVIEW OF LITERATURE

This chapter briefly describes black hole attack and some of the existing secure routing protocols for MANETS.

2.1DESCRIPTION OF BLACK HOLE ATTACK

MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count.

A basic attack that an adversary can execute is to stop forwarding the data packets. As a result, when the adversary is selected as a route, it denies the communication to take place. In black hole attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a black hole as it swallows all objects; data packets[2][5].

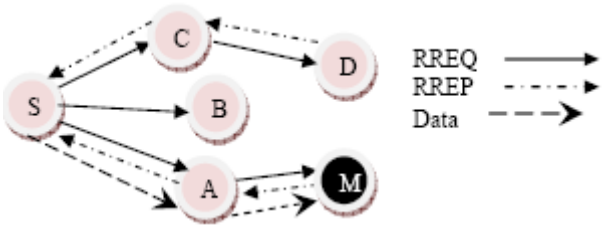

Figure1 Blackhole attacks in MANETs

In figure 1, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a black hole. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from M instead of D.

2.2 SOME OF THE EXISTING SECURE ROUTING PROTOCOLS FOR MANETS.

Jiang et al. [16] use digital signature based hop-by-hop authentication in the route discovery. As Route Request (RREQ) floods in the entire network, every node in the network gets involved in the signature generation and verification process, which consumes a lot of node's resources irrespective of whether the node is included in the

route or not. Moreover, public key cryptography results in long processing delay and computational overhead.

Kargl et al. [17] proposed Secure Dynamic Source Routing (SDSR) for standalone networks. According to the proposal, each node along the route appends its *Diffie-Hellman public key* and encrypted hash of calculated session key, to the Route Reply (RREP) packet, while it traverses from the destination to the source. It increases the RREP packet size enormously. A RREP packet larger than the maximum payload of 802.11 MAC frame is to be forwarded to the next hop in multiple frames. It increases delay at each node and degrades the efficiency of routing protocol. In addition to that, the online computation of session key from the *Diffie-Hellman public key* also adds delay to the route setup process.

Pirzada et al. [18] use promiscuous mode to detect the attacks such as black hole, gray hole, modification fabrication attacks, etc. However, techniques using promiscuous mode fail to work when an attacker uses unidirectional antennas and also fail to detect the collaborative attacks.

3. PROPOSED METHOD

This chapter briefly describes proposed method combines Dynamic Source Routing (DSR) and CCMP-AES MODEL.

Routing protocols can be classified into mainly two types proactive routing protocols and reactive 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. The widely used reactive protocol Dynamic Source Routing (DSR) 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 DSR routing protocol is given below.

3.1 DYNAMIC SOURCE ROUTING (DSR)

DSR is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks with mobile nodes. DSR allows the network to be completely self-organizing and self-configuring without the need for any existing network infrastructure or administration. The protocol is composed of two main mechanisms "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on demand, allowing the routing packet overhead of DSR to scale automatically to only what is needed to react to changes in the routes currently in use. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example, for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop free routing, operation in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes and is designed to work well even with very high rates of mobility. The main disadvantage of the DSR protocol is lack of security [7][8][9][10]. To enhance the security in DSR routing protocol the proposed model combines DSR with CCMP-AES. It defends against black hole attack and it provides confidentiality and authentication of packets in both routing and data link layers of MANETs [11][12][13][14].

3.2 CCMP-AES MODEL

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol [1][3][4]. The CCMP algorithm is based on the U.S. federal government's Advanced Encryption Standards (AES). CCMP offers enhanced security compared with

similar technologies such as Temporal Key Integrity Protocol (TKIP). CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes the vulnerability of black hole attack.CCMP is a Robust security network association (RSNA) data confidentiality and integrity protocol. CCMP is based on the Counter Mode with CBC-MAC(CCM) of the AES encryption algorithm. CCM is a generic authenticate-and-encrypt block cipher mode. A unique temporal key (for each session) and a unique nonce value (a value that's used only once for each frame) are required for protecting the Medium Access Control Protocol Data Unit (MPDU).Figure2 shows CCMP encapsulation block diagram. CCMP uses a 48-bit Packet Number (PN) to protect the MPDUs.CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting cipher text using the following algorithm. Table 1 shows CCMP encapsulation algorithm

Table 1: CCMP encapsulation algorithm

Increment the PN, so that each MPDU has a unique PN for the same temporal key
↓
Use the fields in the MPDU header to construct the additional authentication data (AAD) for CCM.
↓
Construct the CCM Nonce block from the PN, A2, and the Priority field of the MPDU where A2 is MPDU Address 2. The Priority field has a reserved value set to 0.
↓
Place the new PN and the key identifier into the 8-octet CCMP header.
↓
Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and MIC. This step is known as CCM originator processing

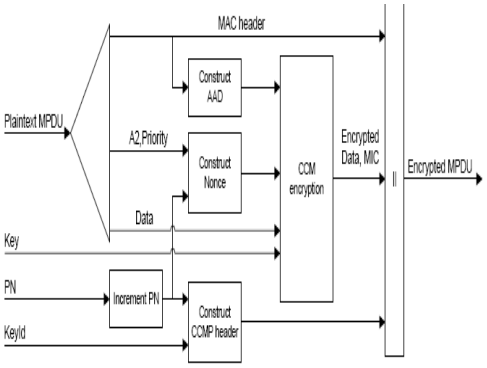

Figure 2: CCMP encapsulation Block Diagram

CCMP decrypts the payload of a cipher text MPDU and decapsulates plaintext MPDU using the following algorithm. Figure 3 show CCMP decapsulation Block Diagram. Table 2 shows CCMP decapsulation algorithm.

Table 2: CCMP decapsulation algorithm.

The encrypted MPDU is parsed to construct the AAD and nonce values.
↓
The AAD is formed from the MPDU header of the encrypted MPDU
↓
The nonce value is constructed from the A2, PN, and Priority Octet fields (reserved and set to 0).
↓
The MIC is extracted for use in the CCM integrity checking.
↓
The CCM recipient processing uses the temporal key, AAD, nonce, MIC, and MPDU cipher text data to recover the MPDU plaintext data and, to check the integrity of
↓
The received MPDU header and the MPDU plaintext data from the CCM recipient processing can be concatenated to form a plaintext MPDU
↓
The decryption processing prevents replay of MPDUs by validating that the PN in the MPDU is greater than the replay counter maintained for the session.

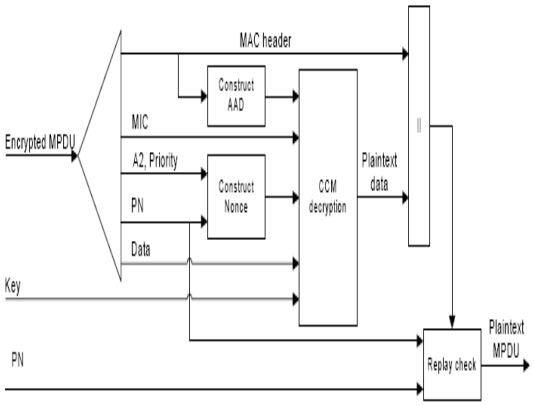

Figure 3: CCMP decapsulation Block Diagram

The decapsulation process succeeds when the calculated Message Integrity Code(MIC) matches the MIC value obtained from decrypting the received encrypted MPDU. The original MPDU header is concatenated with the plaintext data resulting from the successful CCM recipient processing to create the plaintext MPDU.

The proposed model combines the On demand routing protocol DSR with CCMP-AES model to provides confidentiality and authentication of packets in both routing and link layers of MANETs. The primary focus of this work is to provide security mechanisms applied in transmitting data frames in a node-to node manner, such as security protocol CCMP-AES working in data link layer and it keeps data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination.

4. 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. Each node independently repeats this behavior and mobility is varied by making each node stationary for a period of pause time. The simulation parameters are summarized in Table 3.

Table3: 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 analyze the performance of the network's 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
5) Total Bytes Received

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. The average packet delivery ratio is the average of the packet delivery ratios taken over all the receivers.

Average end-to-end delay: The end-to-end delay of a packet is defined as the time a packet takes 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. The average delay jitter is the average of the per-receiver delay jitters taken over all the receivers.

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.

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

Total Bytes Received:

The total amount of bytes received over all the received.

4.1 Performance comparison of routing protocol DSR and CCMP-AES Models for DSR routing protocol with black hole attack.

The different parameters are considered for evaluation. Average packet delivery ratio, Average throughput, Total Bytes Received should be higher and Average end-to-end delay, Average delay jitter must be lower.

Figure 4 shows that total byte received is higher in CCMP-AES with DSR with Blackhole attack compared to DSR.

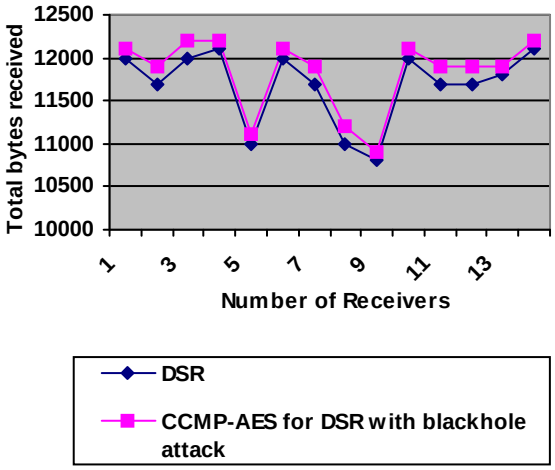

Figure 4: Comparison of Total bytes received of DSR and DSR for CCMP-AES with black hole attack

Figure 5 shows that total packet received is higher in CCMP-AES with DSR with Blackhole attack compared to DSR.

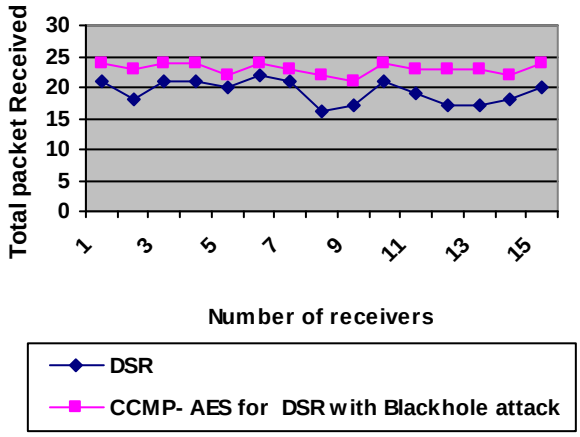

Figure 5: Comparison of Total packet received of DSR and DSR for CCMP-AES with black hole attack

Figure 6 shows that End to End Delay is lower in CCMP-AES with DSR with Blackhole attack compared to DSR.

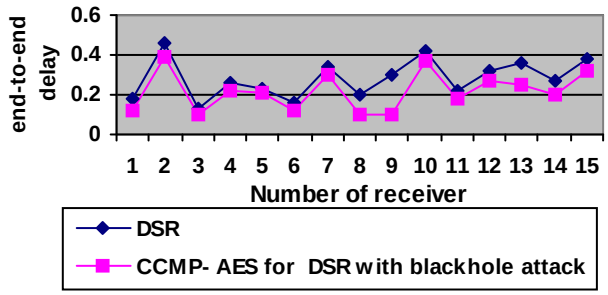

Figure 6: Comparison of End to End delay of DSR and DSR for CCMP-AES with black hole attack

Figure 7 shows that Throughput is higher in CCMP-AES with DSR with Blackhole attack compared to DSR.

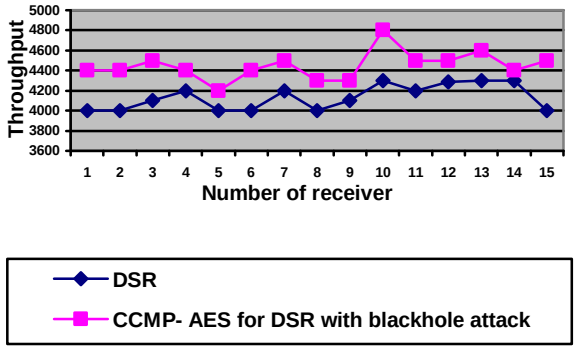

Figure 7: Comparison of Throughput DSR and DSR for CCMP-AES with black hole attack

Figure 8 shows that Average Jitter is lower in CCMP-AES with DSR with Blackhole attack compared to DSR.

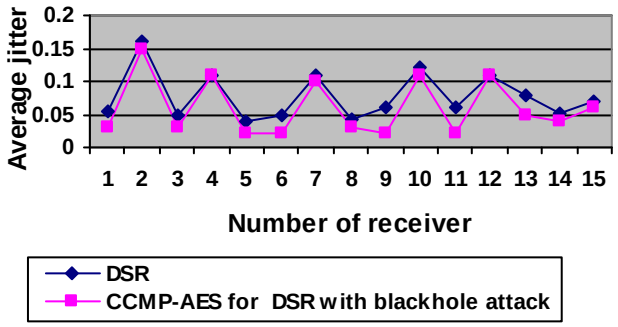

Figure 8: Comparison of a Average Jitter of DSR and DSR for CCMP-AES with black hole attack

From the simulation result it is observed that proposed model is robust against black hole attacks and it also provides confidentiality and authentication of packets in both routing and link layers of MANET.

5. CONCLUSION

Mobile Adhoc network is a special kind of wireless networks. It is a collection of mobile nodes without having aid to establish infrastructure. During deployment, security emerges as a central requirement due to many attacks that affects the performance of the ad hoc networks. Particularly Black hole attack is one such severe attack against ad hoc routing protocols which is a challenging one to defend against. The proposed model combines the On demand routing protocol DSR with CCMP-AES model to defend against black hole attack and it provides confidentiality and authentication of packets in both routing and link layers of MANETs. The primary focus of this work is to provides security mechanisms applied in transmitting data frames in a node-to node manner through the security protocol CCMP-AES working in data link layer and it keeps data frame from eavesdropping, interception, alteration, or dropping from unauthorized party along the route from the source to the destination. The proposed model has shown better results in terms of packet delivery ratio, throughput, End to End delay and jitter.

ACKNOWLEDGMENT

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

REFERENCE

[1] Changhua He and John C Mitchell, *"Security Analysis and Improvements for IEEE 802.11i"*, in the Proceedings of the 12th Annual Network and Distributed System Security Symposium (NDSS'05), 2005.

[2] H. Lan Nguyen and U, Trang Nguyen "*A study of different types of attacks on multicast in mobile ad hoc networks*", Ad Hoc Network, VoI.6, No. I,2007

[3] Specification for the Advanced Encryption Standard (AES), FIPS 197, U.S. National Institute of Standards and Technology. November 26, 2001. [Online] Available at: http://www.nist.gov/aes.

[4] D. Whiting, R. Housley, and N. Ferguson, "*AES Encryption & Authentication Using CTR Mode & CBC-MAC*", IEEE Doc. 802.11-02/144r2, Mar 2002.

[5] Latha Tamilselvan and V. Sankaranarayanan: "*Prevention of Black Hole Attack in MANET*", The 2nd international conference on wireless, Broadband and Ultra Wideband Communications January 2007

[6] M. Junaid , Dr Muid Mufti and M.Umar Ilyas, "*Vulnerabilities of IEEE 802.11i Wireless LAN CCMP Protocol*", *In the Proceedings Of World Academy Of Science, Engineering And Technology* Volume 11, February 2006.

[7] Mehdi Alilou and Mehdi Dehghan.t, "*Upgrading Performance of DSR Routing Protocol in Mobile Ad Hoc Networks*", World Academy of Science, Engineering and Technology 5 2005

[8] 8.Rajendra V. Boppana Anket and Mathur,**"***Analysis of the Dynamic Source Routing Protocol for Ad Hoc Networks*", Workshop on Next Generation Wireless Networks, December 2005

[9] Asad Amir Pirzada Chris McDonald and Amitava Datta: "*Performance Comparison of Trust-Based Reactive Routing Protocols*" IEEE Transactions on Mobile Computing, Vol. 5, Issue 6,June 2006, Pages: 695 – 710.

[10] P. Chenna Reddy and Dr. P. ChandraSekhar Reddy, "*Performance Analysis of Adhoc Network Routing Protocols"*, International Symposium on Ad Hoc and Ubiquitous Computing, 2006. ISAUHC '06. August 2007 Pages:186 - 187

[11] Y. Lu, W. Wang, Y. Song, and B. Bhargava, "*Study of distance vector routing protocols for mobile ad hoc networks*", in PERCOM '03". *Proceedings of the First IEEE International Conference on Pervasive Computing and Communications .IEEE Computer Society*, 2003

[12] Geetha Jayakumar and Gopinath Ganapathy ,"*Performance Comparison of Mobile Ad-hoc Network Routing Protocol*", *IJCSNS International Journal of Computer Science and Network Security*, VOL.7 No.11, November 2007

[13] N.Bhalaji and Dr.A.Shanmugam,"*association between nodes to combat blackhole attack in dsr based manet"*, International Conference on Wireless and Optical Communications Networks, WOCN '09, 2009 ,pages: 1 - 5

[14] Tanvir Ahmed, Syed Nuruzzaman ,Md. Nazimul Haque and Md Masum," *Modification of DSR and its implementation in Ad Hoc City*", international conference on Computer and information technology, 2007. Pages: 1 – 6

[15] Prof. M.Neelakantappa Dr.B.Satyanarayana and Dr. A.Damodharam ,"*Performance Improvement Techniques for Dynamic Source Routing Protocol in Mobile Ad Hoc Networks"*, International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009

[16] Tingyao Jiang, Qinghua Li, Youlin Ruan: "*Secure Dynamic Source Routing Protocol*" Proceedings of the Fourth International Conference on Computer and Information Technology (CIT'04) - Volume 00, (2004), Pages: 528 – 533.

[17] F. Kargl, A. Geiß, S. Schlott, M. Weber: "*Secure Dynamic Source Routing*", Hawaiian International Conference on System Sciences 38,Hawaii, USA, January 2005.

[18] Asad Amir Pirzada Chris McDonald, Amitava Datta: "*Performance Comparison of Trust-Based Reactive Routing Protocols*" IEEE Transactions on Mobile Computing, Vol. 5, Issue 6, June 2006 Pages: 695 – 710.

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 108 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 16 years of teaching experience. Her areas of interest include Object oriented technology, Data mining, Image processing, Pattern recognition. She has 55 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 one year of research experience. Her research interests are cryptography and Network Security. She has 6 publications at national and international level.