ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

Evaluating the performance of secure routing protocols in Mobile Ad-hoc Networks

Shawkat K. Guirguis[1], Ommelhana S .Saaid[2]

Professor of Computer Science & Informatics, Dept. of Information Technology,
Institute of Graduate Studies & Research, Alexandria University, Alexandria, Egypt[1]
Researcher in Dept. of Computer Science, Faculty of Science, Alexandria University, Alexandria , Egypt[2]

ABSTRACT: ***Mobile ad hoc network (MANET) is a special type of mobile wireless network where a collection of mobile devices form a temporary network without any aid of an established infrastructure. During data transmission between these devices there may be malicious threats, attacks, and penetrations which alters the performance of the system and insecure transmission. Multiple routing protocols especially for these conditions have been developed during the last years, to find optimized routes that free from attacks from a source to some destination. This paper presents comparison based on simulation of three secure routing protocol of MANET.***

Keywords: Mobile Ad hoc Networks, NS2, SEAD, SAODV, SZRP

I. Introduction

A mobile ad hoc network (MANET) is a distributed dynamic system of moving wireless devices (nodes). Mobile ad hoc networks are autonomous systems comprised of a number of mobile nodes that communicate using wireless transmission. They are self-organized, self-configured and self controlled infrastructure-less networks. This kind of network has the advantage of being able to be set up and deployed quickly because it has a simple infrastructure set-up and no central administration . the major examples of these networks are in the military or the emergency services.

In Mobile ad hoc networks the nodes are free to move, independent of each other, topology of such networks keep on changing dynamically which makes routing much difficult. Therefore routing is one of the most concerns areas in these networks. Normal routing protocol which works well in fixed networks does not show same performance in Mobile Ad Hoc Networks. In these networks routing protocols should be more dynamic so that they quickly respond to topological changes [1]. A robust and flexible routing approach is required to efficiently use the limited resources available, while at the same time being adaptable to the changing network conditions, such as network size (scalability), traffic density and mobility.

Many security schemes from different aspects of MANET have been proposed in order to protect the routing information or data packets during communications, such as secure routing protocols **,** In this paper we investigate the performance and efficiency of three representative protocols for Mobile Ad hoc Networks, we have chosen the secure protocols that fall under the most significant categories. Our simulation scenarios have been designed as to capture how different categories of MANET protocols cope with typical dynamic conditions and according to different scalability factors. We take into account variation of pause time (mobility), different packets rates and the malicious environment , considering their effects on routing efficiency (packet delivery ratio and normalized routing load), and network latency (end-to-end delay).

II. ROUTING IN MOBIE AD HOC NETWORKS

One of the most exciting and challenging aspects of ad hoc network is the routing issue. Most of the routing protocols are designed for wired and structured network. It is often very hard to adopt these protocols for ad hoc network. Broadly routing protocols can be classified into three groups: reactive, proactive and hybrid. This is summarized in the following figure:

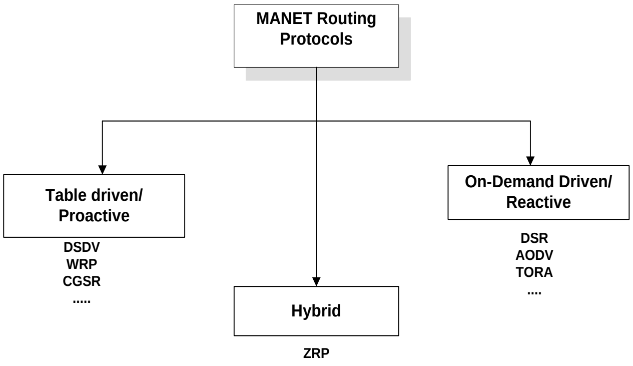

Fig 1. classification of routing protocols

A. ROACTIVE ROUTING PROTOCOLS

In table-driven or proactive protocols, the nodes maintain an active list of routes to every other node in the network in a routing table. The tables are periodically updated by broadcasting information to other nodes in the network such as the Destination Sequenced Distance Vector routing protocol(DSDV)[2].

B. REACTIVE ROUTING PROTOCOLS

In contrast to table driven routing protocols, on-demand routing protocols find route to a destination only when it is required. The on-demand protocols have two phases in common – route discovery and route maintenance. In the route discovery procedure, a node wishing to communicate with another node initiates a discovery mechanism if it doesn't have the route already in its cache. The destination node replies with a valid route. The route maintenance phase involves checking for broken links in the network and updating the routing tables. One of the most popular reactive protocol is Ad hoc On-demand Distance Vector routing protocol (AODV) [3].

C. HYBRID ROUTING PROTOCOLS

Hybrid routing protocols inherit the characteristics of both on-demand and table-driven routing protocols. Such protocols are designed to minimize the control overhead of both proactive and reactive routing protocols. The best example of hybrid routing protocols is the Zone Routing Protocol (ZRP)[4].

III. SECURITY GOALS

To secure the routing protocols in MANET, researchers have considered the following security services [5][6][7]:

Availability guarantees the survivability of the network services despite attacks. A Denial-of-Service (DoS) is a potential threat at any layer of an ad hoc network.

Confidentiality ensures that certain information be never disclosed to unauthorized entities. It is of paramount importance to strategic or tactical military communications.

Integrity ensures that a message that is on the way to the destination is never corrupted. A message could be corrupted because of channel noise or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node. Without authentication, an attacker could masquerade as a normal node, thus gaining access to sensitive information **.**

Non-repudiation ensures that the originator of a message cannot deny that it is the real originator. Non-repudiation is important for detection and isolation of compromised nodes.

IV. ISSUE IN SECURING THE ROUTING PROTOCOLS

Securing the routing protocols for ad hoc networks is a very challenging task due its unique characteristics [8]. A brief discussion on how the characteristics causes difficulty in providing security in ad hoc wireless network is given below.

Shared radio channel: Unlike the wired networks where a separate dedicated transmission line can be provided between a pair of end users, the radio channel used for communication in ad hoc networks is broadcast in nature and shared by all nodes in the network. Data transmitted by a node is received by all the nodes within its direct transmission range. So a malicious node can easily obtain data being transmitted in the network.

Insecure environment: The environment in which MANET are generally used may not be always secure, for example, a battle field. In such environment, nodes may move in and out of hostile and insecure enemy territory, where they would be highly vulnerable to security attacks.

Lack of central authority: In wired networks or infrastructure based wireless networks it would be possible to monitor the network traffic through routers or base stations and implement security mechanisms at those points. Since MANET don't have any such central points, these mechanisms can't be applicable to them.

Lack of association rules: In MANET, since nodes can leave or join the network at any point of time, if no proper authentication mechanism is used for associating nodes with the network intruders can easily join the network and carry out attacks.

Limited availability of resources: Resources such as bandwidth, battery power and computational power are scare in ad hoc networks. Hence, it is difficult to implement complex cryptography-based security mechanisms in such networks.

V. ATTACKS IN AD HOC NETWORKS

Two kinds of attacks can be launched against ad-hoc networks [8] , passive and active attacks

A. *PASSIVE ATTACKS*

A passive Attack is that attack in which an unauthorized party gains access to an asset and does not modify its content. The passive attacker does not send messages; it only eavesdrops on the network. The malicious entity in this type of attack only listens to the traffic, without modifying or disturbing it. The main threat by such an attack is that some confidential information is leaked to the attacker. Passive attacks can be either eavesdropping or traffic analysis.

1) Eavesdropping: The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a network topology between two workstations or tuning into transmissions between a wireless handset and a base station.

2) Traffic analysis : The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

B. *ACTIVE ATTACKS*

An active attack is that attack in which an unauthorized party makes modifications to a message, data stream, or file. In an active attack, the malignant node actively disturbs the normal operation of the network. This can be done by forging packets, disrupting normal routing or consuming network resources etc. Active attacks may take the form of one of four types masquerading, replay, message modification, and denial-of-service (DoS). These attacks are summarized as:

1) Masquerading : The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

2) *Replay* : The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

3) Message modification : The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

4) *Denial-of-service:* The attacker prevents or prohibits the normal use or management of communications facilities.

VI. SECURE ROUTING PROTOCOLS FOR AD HOC NETWORKS

We choosing three secure routing protocols , one based on proactive protocol and the other based on reactive protocol , the last one depend in the hybrid approach of the routing protocols.

A. *SAODV*

The Secure Ad-hoc On-Demand Distance Vector (SAODV) proposed by Zapata [9]is an extension of the AODV routing protocol. It can be used to protect the route discovery mechanism of AODV by providing security features like integrity, authentication and non-repudiation. The protocol operates mainly by using new extension messages with the AODV protocol. In these extension messages there is a signature produced by digesting the AODV packet using the private key of the original sender of the Routing message. The Secure-AODV scheme is based on the assumption that each node possesses certified public keys of all network nodes. Ownership of certified public keys enables intermediate nodes to authenticate all in-transit routing packets. The originator of a routing control packet appends its RSA signature and the last element of a hash chain to the routing packets. As the packets traverse the network, SAODV protocol gives two alternatives for ROUTE REQUEST and ROUTE REPLY messages. In the first case when a ROUTE REQUEST is sent, the sender creates a signature and appends it to the packet. Intermediate nodes authenticate the signature before creating or updating the reverse route to that host. The reverse route is stored only if the signature is verified. When this packet reaches the final destination, the node signs the ROUTE REPLY with its private key and sends it back. The intermediate and final nodes, again verify the signature before creating or updating a route to that host. The signature of the sender is also stored along with the route entry. The second case is also similar to the first one with the only disparity being that the ROUTE REQUEST message has another signature that is always stored along with the reverse route.

This second signature is used in the regular and gratuitous ROUTE REPLYs to future ROUTE REQUESTs that the node might reply to as an intermediate node.

B. *SEAD*

The *Secure and Efficient Ad hoc Distance vector routing protocol* (SEAD) [10] is based upon the *DSDV-SQ* routing protocol (which is a modified version of *DSDV* routing protocol). It uses efficient one-way hash functions to authenticate the lower bound of the distance metric and sequence number in the routing table. More specifically, for authenticating a particular sequence number and metric, the node generates a random initial value x Є $(0,1)^{\rho}$ where ρ is the length in bits of the output of the hash function, and computes the list of values $h_0,h_1,h_2,h_3,\ldots,h_n$, where $h_0=x$, and $h_i = H(h_i\text{-}1)$ for $0< i \le n$, for some *n*. As an example, given an authenticated *hi* value, a node can authenticate h_{i-3} by computing H (H (H (h_i-3))) and verifying that the resulting value equals $h_{i.}$ Each node uses one authentic element of the hash chain in each routing update it sends about itself with metric 0. This enables the authentication for the lower bound of the metric in other routing updates for that node. The use of a hash value corresponding to sequence number and metric in a routing update entry prevents any node from advertising a route greater than the destination's own current sequence number. The receiving node authenticates the route update by applying the hash function according to the prior authentic hash value obtained and compares it with the hash value in the routing update message. The update message is authentic if both values match. The source must be authenticated using some kind of broadcast authentication mechanism such as TESLA [11]. Apart from the hash functions used, SEAD doesn't use *average settling time* for sending triggered updates as in DSDV in order to prevent eavesdropping from neighbouring nodes.

C. *SZRP*

The Secure Zone Routing Protocol (SZRP) is based on the concept of Zone Routing Protocol (ZRP) [12,13]. It is a hybrid routing protocol that combines the best features of both proactive and reactive approaches and adds its own security mechanisms to perform secure routing. SZRP is designed to address all measure security concerns like end to end authentication, message/packet integrity and data confidentiality during both intra and inter-zone routing. For end to end authentication and message/packet integrity RSA digital signature mechanism is employed, where as data confidentiality is ensured by an integrated approach of both symmetric and asymmetric key encryption [14].

SZRP requires the presence of trusted certification servers called the certification authorities (CAs) in the network. The CAs are assumed to be safe, whose public keys are known to all valid CNs(common nodes). Keys are generated a priori and exchanged through an existing, perhaps out of band, relationship between CA and each CN. Before entering the ad hoc network, each node requests a certificate from it's nearest CA. Each node receives exactly one certificate after securely authenticating their identity to the CA. The methods for secure authentication to the certificate server are numerous and hence it is left to the developers; a significant list is provided by [15].

SZRP is a two phase protocol. The first phase is the preliminary certification process where each CN fetches their required keys from their nearest CA. The second routing by applying the process of digital signature and message encryption.

VII. SIMULATION EXPERIMENTS

We used standard simulator tool NS2 for simulation [16] Network simulator (NS2) is an event driven simulator tool and designed specifically to study the dynamic nature of wireless communication networks. A scenario is set up for simulation to evaluate the performance of three secure protocols SAODV, SEAD and SZRP . This scenario is run 7 times with different values of the pause time ranging from 0 to 600 seconds for each protocol (in total 84 run) . Other scenario is generated with different packet rate 2,4 and 6 ,with fixed pause time . And the last scenario with malicious environment is run 6 times with different numbers of malicious nodes from 2 to 12 nodes for each protocol (in total 72 run).

The data is collected according to three metrics – *Packet Delivery Fraction* , *Normalized Routing Load* and *End to end delay* .

A. *PARAMETER SETUP*

To get fair results between three secure routing protocol (SAODV, SEAD and SZRP) we fixed the scenario and parameters setup , in following table some details on settings used in experiments :

TABLE I
PARAMETER SETUP FOR SIMULATION

Parameter	**Value**
Operating System	Linux Ubuntu 10.04
Simulation	NS-2 (Version 2.34)
Area Size	1000 m * 1000 m
Maximum Speed	20 m/s
Maximum Connection	20
Packets Rate	2,4,6 Packets / Second
Traffic Type	CBR
Simulation Time	600 (sec)
Pause Time	0,100,200,300,400,500,600
Packet Size	512 bytes
Number of node	100
Malicious nodes	2,4,6,8,10,12

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 9, November 2012

B. *PERFORMANCE METRICS*

The performance metrics that have been used in this simulation is :

1) Packets Delivery Fractions (in percentage):

The ratio of the data packets delivered to the destinations to those generated by the Constant Bit Rate (CBR) sources. PDF shows how successful a protocol performs delivering packets from source to destination.

*Packet Delivery Fraction (pdf %) = (received packets/ sent packets) * 100*

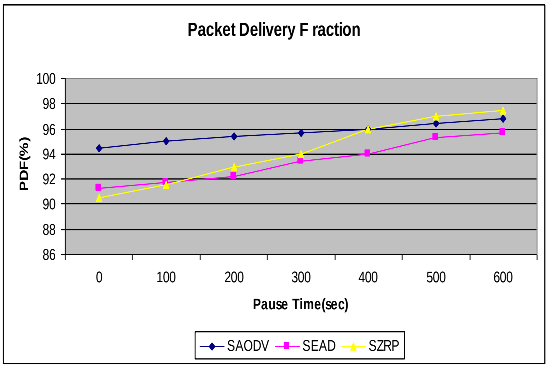

Fig. 1 Packet Delivery Fraction (%) vs Pause Time

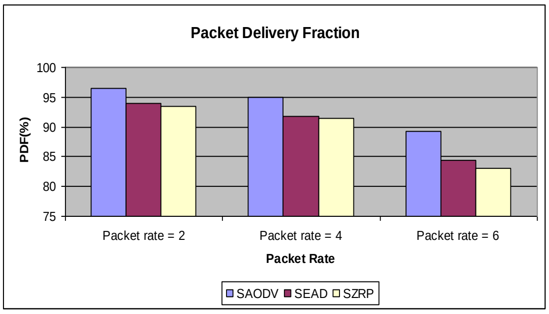

Fig. 2 Packet Delivery Fraction (%) vs Packets rate

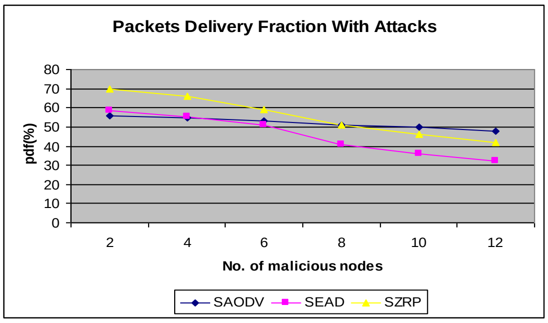

Fig. 3 Packet Delivery Fraction (%) vs malicious nodes

From the Figure 1, the results shows that SAODV outperform both SEAD and SZRP in PDF percentage. It means that SAODV produced more throughputs compared to SEAD and SZRP in total runtime of the simulations. At low pause time, SAODV gives higher PDF reading, But, when the pause time increased SZRP perform better than SAODV and SEAD .

In overall, PDFs percentage readings are increased from lower pause time to larger pause time because all nodes involved will be more steady, stable and accessible to all active nodes.

In figure 2 , on the same pause time with increasing packets rate also SAODV outperform both SEAD and SZRP . from the results we observe The PDF percentage decrease with increasing the packets rate

2) Average End to End Delay :

The delay experienced by packet from the time it was sent by a source till the time it reached the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC and propagation and transfer times. *For each packet sent, calculate the send time and receive time, then average it.*

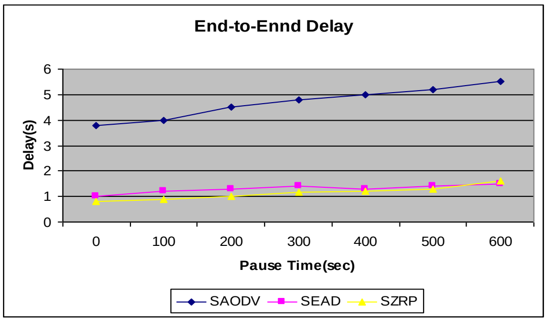

Fig. 4 End to End Delay vs Pause time

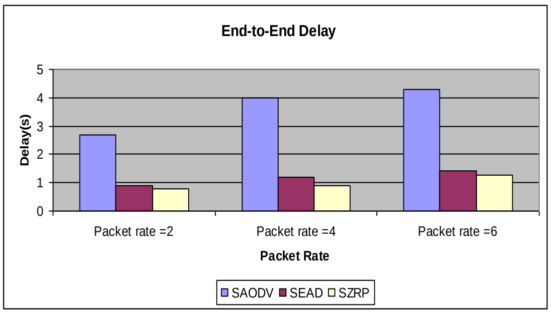

Fig. 5 End to End Delay vs Packets rate

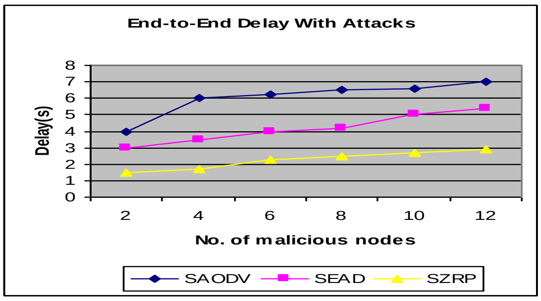

Fig. 6 End to End Delay vs malicious nodes

From the result, showing in figure 4 we can see that SAODV had higher delay , the delay in SZRP slightly less than SEAD and become equal in large pause time.

From figure 5 with increasing packets rates the delay increase , and the SAODV still have larger delay in compare with SZRP and SEAD.

In figure 6, The delay increase with increasing the number of malicious node. SAODV has larger delay in because it uses asymmetric key cryptography so it requires significant processing time to compute or verify signatures and hashes at each node.

3) Normalized Routing Load :

The number of routing packets transmitted for every data packet sent. Each hop of the routing packet is treated as a packet. *Normalized routing load* are use as the ratio of routing packets to the data packets.

As for the calculation, *Normalized Routing Load = routing packets sent / packet received*

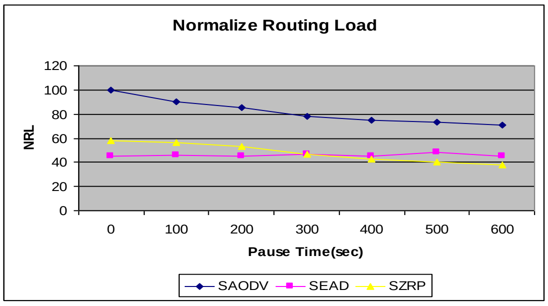

Fig. 7 Normalize Routing Load vs Pause time

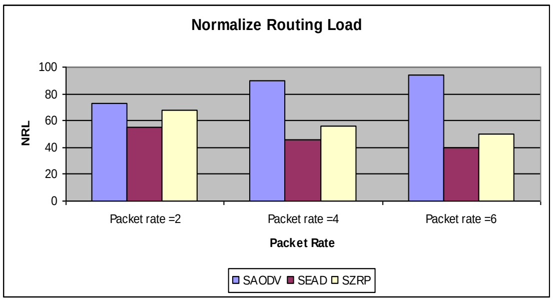

Fig. 8 Normalize Routing Load vs Packets rate

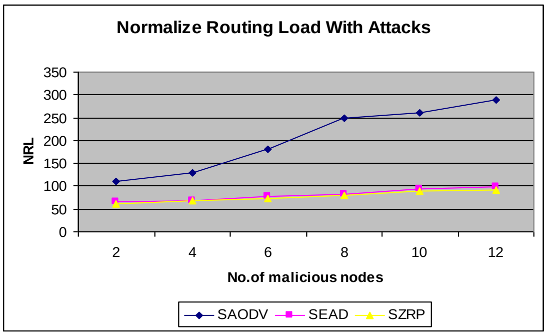

Fig. 9 Normalize Routing Load vs malicious nodes

The results from Figure 7, show that the routing load decreased when reaching towards the end of the simulation. SZRP and SEAD out perform SAODV , we also can see in lower pause time SEAD perform better than SZRP , but in larger pause time (Starting from 300 seconds) SZRP gives reading better than SEAD.

In the figure 8 , in three protocols the routing load increase with increasing packets rates, SAODV gives highest load and then come SZRP and the lowest load give by SEAD. On other hand in lowest pause time the routing load decrease because the high mobility of the nodes.

Form the results showing in figure 9, The NRL also increase with more number of malicious node. SAODV score high load value so, SEAD and SZRP perform better and less load than SAODV.

VIII. CONCLUSION

The two most important issues in mobile ad hoc networks are the performance and security. Each mobile node in a MANET acts as a router by forwarding the packets in the network. Hence, one of the challenges in the design of routing protocols is that it must be tailored to suit the dynamic nature of the nodes. In this paper we investigate the performance and security of three secure MANET routing protocols. SEAD provides low computational overhead, and is relatively simple, making it suitable for use in environments where there is low mobility. but It need to take a collaborative security approach to be to more robust . and other secure protocols SAODV in the most situation more secure than SEAD but it high over load due to asymmetric cryptography , the last one SZRP gives a better solution towards achieving the security goals like message integrity, data confidentiality and authentication, by taking an integrated approach of digital signature and both the symmetric and asymmetric key encryption technique.

REFERENCES

[1] Nitin H. Vaidya,"Mobile Ad Hoc Networks: Routing, MAC and Transport Issues", University of Illinois at Urbana-Champaign, Tutorial presented at: INFOCOM 2004 (IEEE International Conference on Computer Communication).

[2] C. Perkins and P. Bhagwat, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In Proc. of the ACM SIGCOMM, October 1994.

[3] C.E. Perkins, E. Royer, and S.R. Das, "Ad hoc on demand distance vector (AODV) routing," Internet Draft, March 2000.

[4] Haas Z.J, " A new routing protocol for the reconfigurable wireless network". In Proceedings of the 1997 IEEE 6th International Conference on Universal Personal Communications, ICUPC '97, San Diego, CA, October 1997; pp. 562 -- 566.

[5] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad. "Chapter 30: Security in wireless ad-hoc networks, the handbook of Ad hoc wireless network". , CRC PRESS Publisher, 2003.

[6] A Study of Secure Routing in MANET: *various attacks and their Countermeasures* Abari Bhattacharya , Prof. Himadri Nath Saha , IEMCON , Jan 2011

[7] Security in Wireless Ad Hoc Networks , Eric Lee ,Science Academy Publisher, United Kingdom , Vol. 1, No. 1, March 2011

[8] C.Siva Ram Murthy and B. S. Manoj. "Ad hoc wireless networks: Architecture and Protocols". Prentice Hall Publishers, May 2004, ISBN 013147023X.

[9] M. Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," *Proceedings of the ACM Workshop on Wireless Security (WiSe),* ACM Press,2002, pp.1-10.

[10] Y. C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc Networks Journal, 1, 2003

[11] William Stallings. "Network Security essentials: Application and Standards", Pearson Education , Inc 2003, ISBN 0130351288.

[12] Haas Z. J., Pearlman M. R., and Samar P., "The Zone Routing Protocol (ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[13] Jan Schaumann, "Analysis of Zone Routing Protocol", Course CS765, Stevens Institute of Technology Hoboken, New Jersey, USA, 8th December 2002

[14] Behrouz A. Forouzan, "Cryptography and Network Security", Special Indian Edition, Tata McHill publication, 2007

[15] J. J. Tardo and K. Algappan, "SPX: Global authentication using public key certificates", In Proceedings of the 1991 IEEE Symposium on Security and Privacy, pages 232–244, Oakland, CA USA, May 1991. IEEE Computer Society Press.

[16] The Network Simulator NS-2 tutorial homepage, http://www.isi.edu/nsnam/ns/tutorial/index.html