ISSN:0975-9646

Performance Analysis in Ad-Hoc Network

Princy Tyagi

M.Tech Department Of Computer Science & Engineering
M.V.V..College Of Engg, Jagadhari (Yamuana Nagar)(Haryana)

Abstract -Ad hoc networking allows portable devices to establish communication independent of a central infrastructure. However, the fact that there is no central infrastructure and that the devices can move randomly gives rise to various kind of problems, such as routing and security. In this paper the problem of routing is considered. There are several ad hoc routing protocols, such as AODV1 , DSR2 , OLSR3 and ZRP4 , that propose solutions for routing within a mobile ad hoc network. However, since there is an interest in communication between not only mobile devices in an ad hoc network, but also between a mobile device in an ad hoc network and a fixed device in a fixed network (e.g. the Internet), the ad hoc routing protocols need to be modified. In this thesis the ad hoc routing protocol AODV is used and modified to examine the interconnection between a mobile ad hoc network and the Internet. For this purpose Network Simulator 2, NS 2, has been used. Moreover, three proposed approaches for gateway discovery are implemented and investigated.

Keywords : ***Ad Hoc, Mobile Networks, Performance Evaluation, Routing Protocol, Destination-Sequenced Distance- Vector (DSDV), Ad-hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR),***

I.INTRODUCTION

Wireless communication1 between mobile users is becoming more popular than ever before. There are two distinct approaches for enabling wireless communication betweentwo hosts. The first approach is to let the existing cellular network infrastructure carry data as well as voice. The major problems include the problem of handoff, which tries to handle the situation when a connection should be smoothly handed over from one base station to another base station without noticeable delay or packet loss. Another problem is that networks based on the cellular infrastructure are limited to places where there exists such a cellular network infrastructure. The second approach is to form an ad-hoc network among all users wanting to communicate with each other. This means that all users participating in the ad-hoc network must be willing to forward data packets to make sure that the packets are delivered from source to destination successfully. This form of networking is limited in range by the individual node transmission range and is typically smaller compared to the range of cellular systems. This does not mean that the cellular approach is better than the ad-hoc approach. Ad-hoc networks have several advantages compared to traditional cellular systems. These advantages include on demand setup, Fault tolerance, and unconstrained connectivity.

Ad-hoc networks do not rely on any pre-established infrastructure and can therefore be deployed in places with no infrastructure. This is useful in disaster recovery situations and places with non-existing or damaged communication infrastructure where rapid deployment of a communication network is needed. Because nodes are forwarding packets for each other, some sort of routing protocol is necessary to make the routing decisions. Currently, there does not exist any standard for a routing protocol for ad-hoc networks, instead this is in progress. Many problems remain to be solved before any standard can be achieved.

The DSDV algorithm is selected as the representative of the Table-Driven protocols because it maintains a loop-free, fewest-hop path to every destination in the network. DSDV prevents loops because of the sequence number, which gives the ability to the network to distinguish stale routes from new ones. Hence, this protocol achieves low routing overhead and low packet delay. Routing information is exchanged when significant new information is available, for instance, when the neighborhood of a node changes. The AODV algorithm is considered as the representative of the On-Demand protocols, because on the contrary to other On-Demand protocols, it supports unicast and multicast packet transmissions. None of the other On-Demand algorithms incorporate multicast communication. It also appears to achieve the lowest Routing Overhead from all other protocols in its category in accordance with other papers. This paper emphasizes at some of these problems and tries to evaluate performance of DSDV2, AODV3, DSR4

II.PROBLEM FORMULATION

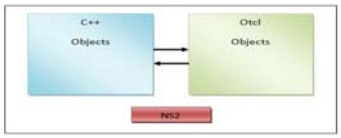
In Mobile Ad hoc Networks (MANET) much of the research has been done focusing on the efficiency of the network. There are quite a number of routing protocols that are excellent in terms of efficiency. But the security requirements of these protocols changed the situation and a more detailed research is currently underway to develop secure ad hoc routing protocols.

MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secured. To address these concerns, several secure routing protocols have been proposed: Secure Efficient Distance Vector Routing (SEAD), Ariadne, Authenticated Routing for Ad hoc Networks (ARAN), Secure Ad hoc On-Demand Distance Vector Routing (SAODV), Secure Routing Protocol (SRP), Security-Aware Routing Protocol (SAR). Although researchers have proposed several secure routing protocols, their resistance

towards various types of security attacks and efficiency are primary point of concern in implementing these protocols. Hence, there is a need for evaluation.

III.NETWORK SIMULATOR NS2

NS2 is an event driven network simulator used for network related research [15]. It was developed at UC Berkeley. It implements network protocols such as TCP and UPD, traffic source behaviour such as FTP, Telnet, and CBR etc. NS began as a variant of the REAL in 1989 and has evolved substantially over the past few years. In 1995 NS development was supported by DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. The wireless code from the UCB Daedelus and CMU Monarch projects and Sun Microsystems, have added the wireless capabilities to NS2. NS2 is the widely used simulation tool by researchers for ad hoc network simulations. So in this research, NS2 is used as a simulation tool to evaluate the performance of ad hoc secure routing protocols. NS is Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries. To simulate a network, a user should write an OTcl script that initiates an event scheduler, sets up the network topology using the network objects. In this thesis work we are going to use NS2 as a simulation tool to evaluate the performance of secure routing protocols.



(NS2 framework)

Iv .Ad Hoc Secure Routing Protocols Evaluation

A.Case study against identified attack patterns

In ad hoc networks, attacks can be classified into active and passive attacks. In passive attacks, attackers don't disrupt the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. An active attacker injects packets into the network, eavesdrops and also tries to compromise the network with denial of service. In the active attacks, the malicious nodes introduce false information to confuse the network topology. They can either attract traffic to them and then drop or compromise the packets. They can also send false information and lead packets to the wrong node and cause congestion in one area. The attacks can either target at the routing procedure or try to flood the networks.

SEAD was developed based on DSDV and incorporates One-Way Hash function to authenticate in the routing update mechanism in order to enhance the routing security. Securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. Distance vector protocols encapsulate the route information into a hop count value and a next hop. An attacker cannot create a valid route with a larger sequence number that it received due to the properties of hash function. As SEAD incorporates neighbour authentication through Hash functions, an attacker can not compromise any node. SEAD is prone through warmhole attack. Even if authentication is provided using hash functions, a warmhole attack is possible through tunnelling the packets from one location and retransmitting them from other location into the network. All packets in the wormhole attack flow in a circle around instead of reaching the destination.

B.Ariadne:

Ariadne was developed based on an on demand protocol, Destination Source Routing (DSR). Ariadne uses MAC s and shared keys between nodes to authenticate between nodes and use time stamps for packet lifetime. Warmhole attacks are possible in Aridane through two compromised nodes. Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps.

C.SRP:

Secure routing protocol (SRP) was developed based on Destination Source Routing (DSR). The intermediate nodes participating in the route discovery measure the frequency of queries received from their neighbours and maintain a priority ranking inversely proportional to the query rate. So the malicious compromised nodes participating in the network are given least priority to deal with. The security analysis is similar to Ariadne as it is based on DSR protocol.

D.ARAN:

Aran uses public key cryptography and a central certification authority server for node authentication and neighbour node authentication in route discovery. Denial-of-service attacks are possible with compromised nodes. Malicious nodes cannot initiate an attack due to the neighbour node authentication through certificates. Participating nodes broadcast unnecessary route requests across the network. An attacker can cause congestion in the network, there by compromising the functionality of the network.

Spoofing attacks are prevented by ARAN through node level signatures. Each packet in the network is signed by its private key before broadcasted to the next level and checked for the authentication. So spoofing the identity of node is hampered by ARAN. Due to the strong cryptographic features of ARAN, malicious nodes cannot participate in any type of attack patterns. Only compromised nodes can participate in any attack pattern.

E.SAODV

It is a widely implemented protocol in industry due to its strong security features. SADOV uses a central key management in its routing topology. Digital signatures are used to authenticate at node level and hash chain is used to prevent the altering of node counts. Tunnelling attacks are possible through two compromised nodes. Warmhole attacks are always possible with compromised nodes in any ad hoc network topology. The use of sequence numbers could prevent most of the possible reply attacks.

F.SAR:

SAR was developed using a trust-based framework. Each node in the network is assigned with a trust level. So the attacks on this framework can be analyzed based on trust level and message integrity. As show below the author [Seung, Prasad, Robin] evaluated the security of SAR in terms of trust level and message integrity.

Trust Level: SAR routing mechanism is based on the behaviour associated with the trust level of a user. It is a binding between the identity of the user and the associated trust level. To follow the trust-based hierarchy, cryptographic techniques like: encryption, public key certificates, shared secrets, etc. are employed.

Ad hoc security protocols ▶ / Attack patterns ▼	SEAD	Ariadne	SRP	ARAN	SAODV	SAR
DOS	Y	Y	Y	Y	Y	Y
Tunneling	Y	Y	Y	Y	Y	Y
Spoofing	Y	N	N	N	N	N
Blackhole	Y	N	N	N	N	N
Warmhole	Y	Y	Y	Y	Y	Y
Routing tables overflow attacks:	Y	N	N	N	N	N

Table 3.1

Y = Attack Possible N = Attack not possible

v..EVALUATION WITH SIMULATION

Due to the time limitations only two protocols SEAD and ARIADNE are evaluated using NS2 Simulator, which is available as an open source distribution. All the experiments are done with fixed pause times of 25, 50, 100, 200, 400 and 800 seconds. For generating the mobility scenarios for different pause times, which is based on a two-ray ground reflection model, the *setdest* tool given in NS2 is used. The radio model corresponds to the 802.11 operating at a maximum air-link rate of 2 Mbps. CBR traffic pattern is used. The traffic pattern was generated using "cbrgen.tcl" script, which is provided along with the standard NS2 distribution.

- Simulation environment and parameters:

No. of nodes used for simulation	20
Maximum No. of connection	20
Network Density dimensions	1000 x 1000 meters
Mobility pattern	Uniform
Link Bandwidth	2 mbps
Traffic pattern	CBR
Simulation time	800 seconds
Maximum node Speed	20meters/sec

TABLE1.1

vi.METRICS

The following metrics are used in the evaluation of SEAD and Ariadnce performance

*A.Packet Delivery Fraction (PDF)***:**

This is the ratio of total number of packets successfully received by the destination nodes to the number of packets sent by the source nodes.

$$PDF = \frac{No\ of\ Packets\ Received\ by\ destination}{No\ of\ Packets\ Sent\ by\ Source}$$

This estimate gives us an idea of how successful the protocol is in delivering packets to the application layer. A high value of PDF indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance.

B.Byte Overhead (BO):

The total number of routing bytes transmitted during the simulation. For packets sent over multiple hops, each transmission of the byte at each hop counts as one transmission.

C.Packets Overhead(PO):

The total number of routing packets transmitted during the simulation. For packets (512 kbps) sent over multiple hops, each transmission of the packet at each hop counts as one transmission.

*D.Median Latency(ML)***:**

The time taken by the route discovery packet to reach from the source to destination is known and Median latency. The less time to discover the route to the destination indicates the high performance of the protocol.

E.Average end-to-end delay (AED):

This is the average delay between, sending the data packet by the CBR source and its receipt at the corresponding CBR receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, and retransmission delays at the MAC layer.

$$AED = \frac{\sum_{i=0}^{n} Time\ Packet\ Received_i - Time\ packet\ sent_i}{Total\ Numbe\ of\ Packets\ Received}$$

Where 'n' is the total number of packets. A higher value of end-to-end delay means that the network is congested and hence the routing protocol doesn't perform well

vii.RESULTS

The simulation results from NS2 with respect to the following performance metrics are shown in the following figures. In the next chapter the obtained results will be discussed with respect to the performance appraisals.

Packet Delivery Fraction (PDF)

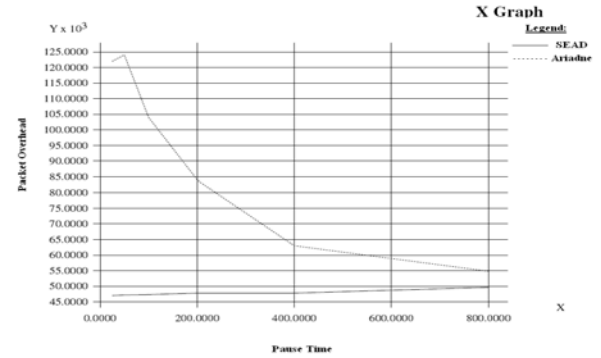


FIG 1

SEAD	Packet Delivery Fraction	Pause Time
	920.0000	25.0000
	930.0000	50.0000
	922.5000	100.0000
	935.5000	200.0000
	955.0000	400.0000
	970.0000	800.0000
Ariadne	762.5000	25.0000
	755.0000	50.0000
	780.0000	100.0000

TABLE I

Byte Overhead:

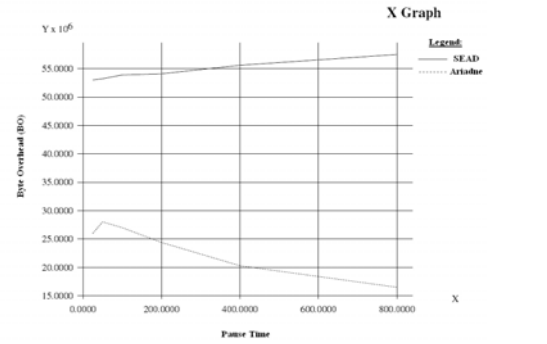


FIG 2

SEAD	Byte Overhead	Pause Time
	53.0000	25.0000
	53.5000	50.0000
	54.0000	100.0000
	54.5000	200.0000
	57.0000	400.0000
	58.0000	800.0000
Ariadne	26.0000	25.0000
	27.5000	50.0000
	25.5000	100.0000
	24.0000	200.0000
	20.0000	400.0000
	17.5000	800.0000

TABLE II

Packets Overhead:

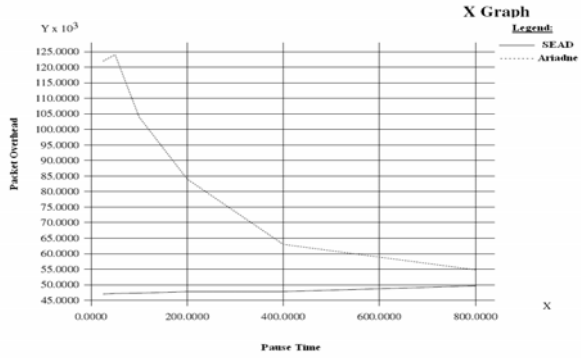


FIG 3

SEAD	Packets Overhead:	Pause Time
	46.5000	25.0000
	47.0000	50.0000
	47.5000	100.0000
	48.0000	200.0000
	49.0000	400.0000
	50.0000	800.0000
Ariadne	122.0000	25.0000
	124.5000	50.0000
	104.0000	100.0000
	85.0000	200.0000
	63.0000	400.0000
	55.0000	800.0000

TableIII

Median Latency:

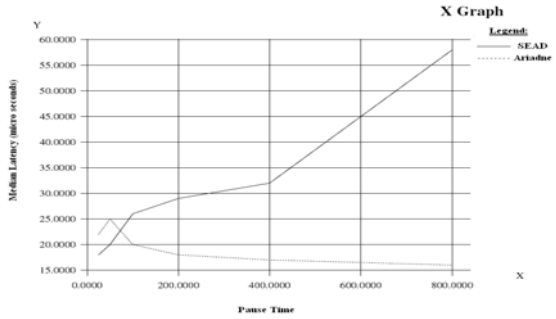


FIG 4

SEAD	Median Latency	Pause Time
	18.0000	25.0000
	20.0000	50.0000
	26.0000	100.0000
	29.0000	200.0000
	32.0000	400.0000
	57.5000	800.0000
Ariadne	22.0000	25.0000
	25.0000	50.0000
	20.0000	100.0000
	18.0000	200.0000
	17.0000	400.0000
	16.0000	800.0000

Table IV

Average end-to-end delay (AED):

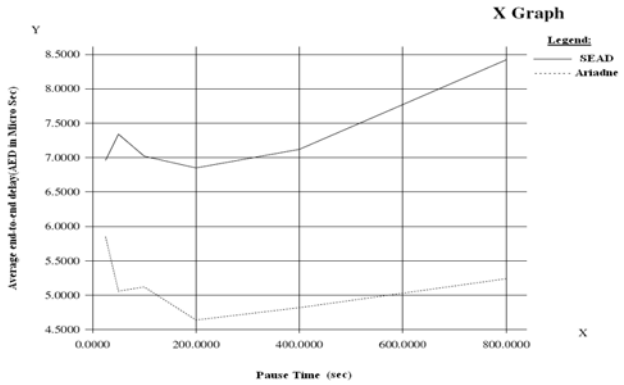


FIG 5

	Average end-to-end delay	Pause Time
SEAD	7.0000	25.0000
	7.3000	50.0000
	7.0000	100.0000
	6.8000	200.0000
	7.2000	400.0000
	8.2500	800.0000
Ariadne	5.8000	25.0000
	5.1000	50.0000
	5.2000	100.0000
	4.7000	200.0000
	4.8000	400.0000
	5.3000	800.0000

Table V

VIII. SECURITY AND PERFORMANCE ANALYSIS

The results of case studies against ad hoc attack patterns and the results of simulations are discussed in this chapter. Simulation tests are done only for SEAD and Ariadne with selected performance metrics. The simulation results with respect to the performance metrics are shown in the figures 3.1, 3.2, 3.3, 3.4 and 3.5. In all these simulation results x-axis shows the pause times and y-axis shows the values of performance metric used. The protocols are evaluated with comparatively.

A.SEAD and Ariadne Security and Performance Analysis:

- Security Analysis:

The security analysis of SEAD and Ariadne are done in this thesis. SEAD is a table driven protocol, and securing a table driven protocol is harder than securing an on demand protocol due to the existence of predefined routes. From the table 3.1 we can see that all type of security attacks are possible in SEAD routing protocols with a compromised node. If no compromised malicious nodes exist in the network, SEAD is stable to all attack patterns through neighbour authentication. Routing loops can only be possible when there is more than one malicious node in the network. The confidentiality of the network topology with respect to participating nodes is maintained with neighbour authentication.

Ariadne uses MAC s and shared keys to authenticate between nodes and use time stamps for packet lifetime. Warmhole attacks are possible in Aridane through two compromised nodes. Ariadne prevents spoofing attacks with time stamps. The use of source routes prevents loops, since a packet passing through only legitimate nodes will not be forwarded into a loop due to time stamps.

IX..PERFORMANCE ANALYSIS:

A. Packet Deliv ery Fraction (PDF):

Figure 6.1 shows the results of the performance metric, *packet delivery fraction*. A higher value of PDF indicates that most of the packets are being delivered to the higher layers and is a good indicator of the protocol performance. SEAD consistently outperforms Ariadne in terms of packet delivery fraction at lower pause times in the simulation. This shows that the route discovery is faster in SEAD than in Ariadne and the number of routing advertisements sent by SEAD are more than Ariadne. So at lower pause time SEAD contains more up to date routing information than Ariadne. At higher pause times the PDF graph for Ariadne increases gradually. As Ariadne uses TESLA broadcast authentication with shared keys between nodes, at the lower pause times it takes more time for route discovery and once secure routes are discovered the PDF graph increases gradually because of the secure route.

B. Byte Overhead (BO):

Figure 6.3 shows the results of the performance metric, *byte overhead.* SEAD graph shows increased byte overhead than Ariadne, this is due to the increased number of routing advertisements in SEAD than Ariadne. Ariadne graph shows a decrease in byte overhead with increased simulation time. The increased overhead in SEAD causes some congestion in the network. As the simulation time increases Ariadne outperforms SEAD with decreased byte overhead.

B. Packet Overhead (PO):

Figure 6.5 shows the simulation results of the performance metric, *packet overhead.* Packet overhead graph for SEAD is lower than in Ariadne. PDF graph for Ariadne decreases gradually and reaches SEAD as the simulation time increases. The increased packet overhead in Ariadne at the lower pause time is due to the route discovery packet flooding. After discovering the secure routes, the packet overhead decreases gradually.

D. Medial Latency (ML):

Figure 6.7shows the simulation results of the performance metric, *median latency*. The time taken by the route discovery packet to reach from the source to destination is known and median latency. The less time to discover the route to the destination indicates the higher performance of the protocol. Ariadne graph shows lower medial latency graph, which means it takes less time in the route discovery process when compared to SEAD, where as SEAD ML graph increases as the simulation time increases, indicating the congestion in the route discovery process as the simulation time increases.

E. Average end-to-end delay (AED):

Figure 6.9 shows the simulation results of the performance metric, *average end-to-end delay.* A higher value of end-to-end delay means that the network is congested and hence the routing protocol doesn't perform well. SEAD graph for AED shows that at lower simulation time AED values are lesser and it increases with increase in simulation pause time. Ariadne graph for AED shows decreased values for lower pause times and increases slowly. Ariadne outperforms SEAD with lower AED values.

X..CONCLUSION

Securing ad hoc environments is a challenging task. The main purpose of this thesis work was to acquire in-depth knowledge of ad hoc routing protocols and secures routing protocols. Security evaluation of some of the secure routing protocols are done using case study with the most commonly identified attack patterns in ad hoc networks. Performance evaluation of ad hoc secure routing protocols SEAD and Ariadne was done with most commonly identified performance metrics.

In the secure routing protocols most of the security attacks are possible with a compromised node. From the case study results, it concludes that table driven protocols are more prone to security attacks than on demand driven protocols. Protocols based on DSR and AODV are more stable to security attacks due to the strong cryptographic implementation.

The performance evaluation of SEAD and Ariadne shows that, Ariadne out performs SEAD in all the performance metrics. But it is important to see that at lower simulation pause times SEAD out performs Ariadne. This is due to the routing mechanism involved in these protocols. SEAD encapsulates routing information in routing tables, so at lower pause time SEAD out performs Ariadne.

FUTURE WORK

Research in the area of ad hoc secure routing protocols is still actively done. Due to the time constraint and code limitations the current work was only focused on evaluating two secure routing protocols SEAD and Ariadne with some selected performance metrics. The evaluation of other ad hoc secure routing protocols discussed in this thesis work with some more performance metrics will be considered as future research work.

REFERENCES

[1] Xiang Chen, Hongqiang Zhai, Jianfeng Wang, and Yuguang Fang," TCP performance over mobile ad hoc networks", CAN. J. ELECT. COMPUT. ENG., VOL. 29, NO. 1/2, JANUARY/APRIL 2004.

[2] Stylianos Papanastasiou, Mohamed Ould-Khaoua, Lewis M. Mackenzie," On the evaluation of TCP in MANETs", Department of Computing Science University of Glasgow Glasgow, UK G128QQ.

[3] Yih-Chun Hu, David B. Johnson and Adrian Perrig. "Secure Efficient Ad hoc Distance vector routing" in the Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and applications (WMCSA'02) Panagiotis

[4] Basagni, S. Conti, M. Giordano, S. Stojmenovi & cacute (Edit). [2004]. Mobile Ad Hoc Networking: September 2004 Wiley-IEEE Press. (pp. 1-33, 275-300, 330-354)

[5] C. Siva Ram Murthy and B.S. Manoj. [2004]. Ad Hoc Wireless Networks, Architecture and Protocols: 2004 Pearson Education (pp. 321-386, 473-526)

[6] Adrian Perrig, Ran Canetti, Dawn Song, and J. D. Tygar. Efficient and Secure Source Authentication for Multicast. In Network and Distributed System Security Symposium, NDSS '01, pages 35–46, February 2001.

[7] David B. Johnson, David A. Maltz, and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop WirelessAd Hoc Networks", in Ad Hoc Networking, Editor: Charles E.Perkins, Chapter 5, pp. 139-172, Addison-Wesley, 2001.

[8] Panagiotis Papadimitratos and Zygmunt J. Haas In Proceedings of the SCS Communication Networks and Distributed Systems Modelling and Simulation Conference (CNDS 2002), San Antonio, TX, January 27-31, 2002.

[9] Kimaya Sanzgir, Bridget Dahilly, Brian Neil Levine, Clay Shields, Elizabeth M and Belding-Royer [2002]. "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02).

[10] M. Abolhasan, T. Wysocki and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks", Ad Hoc Networks 2 , 2004 , pp. 1–22

[11] N. H; Tony Larsson, " Routing Protocols in Wireless Ad Hoc Networks- A Simulation Study," Department Of Computer Science and Electrical Engineering, Luleå University of Technology, Stockholm, 1998. Pp 20-29.

[12] C. Perkins and E. Royer, "Ad-hoc on-demand Distance Vector Routing," Proc. 2nd IEEE Wksp. Mobile Comp. Sys. App., Feb. 1999, pp. 90–100.

[13] Manel Guerrero Zapata, N. Asokan" Secure Ad-ahoc on-demand distance vector" in Nokia research center and was submitted to WiSe'02, September 28, 2002, Atlanta, Georgia, USA. Pp 35-45.

[14] Seung Yi, Prasad Naldurg and Robin Kravets in the Dept. of Computer Science, University of Illinois at Urbana-Champaign