Volume 2, No. 4, July-August 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Enhanced Authenticated Routing for Ad Hoc Networks (EARAN)

Ajay Jangra and Shalini Singroha*
CSE Department, UIET
Kurukshetra, INDIA.
er_jangra@yahoo.co.in
shalinisingroha@gmail.com

Abstract: The area of Mobile ad hoc networks is developing very fastly day by day. But in spite of this ad hoc network faces many security challenges that require being faced. This paper proposed EARAN (Extended authenticated Routing for Ad Hoc networks) protocol that is an extension of ARAN protocol. EARAN protocol contains all identified attacks using public-key cryptographic mechanisms and give end-to-end authentication. This paper also gives detail phases of EARAN protocol, and explains how this makes the protocol environment secure. It provides better end-to-end delay and throughput than existing ARAN protocol.

Keywords: Mobile Ad Hoc Network (MANET), Selfish node, RDP, RREP, DAck, ARAN

I. INTRODUCTION

MANET is a collection of nodes which organize itself without any central coordinator and nodes move freely in the network. They may enter or leave the network without any restrictions. Therefore, wireless ad hoc network's topologies are dynamic and it is costly to maintain. So, wireless channels make message transmission and routing more challenging [1]. Nodes of Ad hoc networks can function as routers that discover and keep routes to other nodes as well as end-users. Nodes in wireless ad hoc networks have limited resources i.e. bandwidth, battery power and CPU power. Because of this limited resources, no security consideration have made in many routing protocols like AODV, DSR etc. So afterwards to secure the network many secure routing protocols are established [2]. From the point of security every routing protocol must fulfil the following criteria that are Certain Discovery, Isolation, Lightweight Computations, Location Privacy, Self-stabilization and Byzantine robustness [3]. Security also shows identification of attacks, threats and vulnerability of a certain system. The attacks on network can be divided in to two types: Active and Passive. A passive attack does not affect the operation of the protocol, instead of its tries to discover valuable information by listening to traffic. On the other hand, Active attacks are tried to disrupt the topology of the network by breaking existing paths between network nodes. Therefore from the viewpoint of active attacks integrity and authentication are more dangerous [3]. Some ordinary types of active attacks are as follows:-

A. Attacks Using Modification:

This is the very easy way for a malicious node to affect the operation of an ad hoc network. Here the malicious node needs to do only one job that is to announce finer routes than the ones presently existing. This type of attack is settled on the modification of the metric value for a route or by changing control message fields. Three ways from which it can be achieved are Redirection by Modifying the Route Sequence Number, Redirection by Modifying the Hop Count and Denial of Service by modifying Routing information [4].

B. Attacks Using Impersonation:

Spoofing appears when a node represents fake identity in the network, such as modifying its IP or MAC address in outgoing packets. It is promptly attached with other attacks those based on modifications [4].

C. Attacks Using Fabrication of Information

These attacks contains the generation of false routing messages. These types of attacks can be divided in to two types: Falsifying Route Error Messages and Routing Table Overflow [4].

II. PREVIOUS WORK

There are mainly two approaches that are used to provide solutions to the security issues in ad hoc networks are: "Prevention" and "Detection and Reaction" Techniques. Prevention mechanism can not provide guarantee to complete cooperation among nodes in the network. These mechanisms require encryption techniques to provide authentication, confidentiality, integrity and non-repudiation of routing information. However existing preventive approaches, few approaches some use symmetric algorithms, some use asymmetric algorithm; while the others use on-way hashing, individual having different trade-offs and goals. On the other side, Detection approaches specify solutions that try to identify clues of any unauthorized activity in the network and take appropriate action against such nodes [5].

Under the prevention using asymmetric algorithm the issue of secure routing in particular has obtained significant attention. Ariadne [6] a secure version of DSR is proposed by Hu et al. Ariadne relies on pre-deployed pair wise symmetric keys or pre-deployed asymmetric cryptography for authentication. A third choice for Ariadne is the TESLA authentication scheme. TESLA scheme is based on asymmetric encryption that requires a certification authority or pre deployed keys. It also need that the packets are

delayed by the longest RTT in the network before they are sent.

Chu et al. proposed a secure proactive routing protocol called SEAD [7] that is based on DSDV. It is also based on Public key that is signed with hash chains.

SAODV [8] is an extension of AODV routing protocol. SAODV functionality work under in security of the AODV protocol by authenticating the unchangeable field of the routing messages using digital signatures.

Then Papadimitratos et al. [9] developed the SRP (Secure Routing Protocol). This protocol is vulnerable to attacks such as fabricated Route error messages. The basic process of SRP is to set up a Security Association (SA) between the source and destination node.

Furthermore ARAN (Authenticated Routing for Ad Hoc networks) proposed by Sanzgiri, laflamme, dahill, Levins, Shlelds and Belding-Royer. It is an on-demand routing protocol which is based on type of query-reply dialog. This means that ARAN protocol does not try to continuously keep the up-to-date topology of the network, but when there is a requirement, it calls a function to detect a route to the destination. Authenticated Routing for Ad hoc Network protocol uses cryptographic certificates to provide routing security. This is a preliminary certification process that uses a route instantiation process that guarantees end-to-end authentication, so only authenticated nodes involves at every hop between source & destination. It detects and protects against malicious actions by third parties and also peers in ad-hoc infrastructure. This protocol introduces message integrity, authentication and non-repudiation to an ad-hoc environment [4].

III. ENHANCED AUTHENTICATED ROUTING FOR AD HOC NETWORKS (EARAN)

ARAN is a preliminary certification process that uses a route instantiation process that guarantees end-to-end authentication, so only authenticated nodes involves at every hop between source & destination. Limitation in ARAN is that it doesn't tell if any malicious or suspicious node is present in Data transfer phase then this protocol what action will take this. So to overcome this problem this paper presents EARAN protocol. EARAN is the extended version of ARAN protocol. EARAN includes two distinct stages to explain its functioning. In the first stage of EARAN protocol, it needs extra work from peers beyond traditional ad hoc protocols however this stage is very simple. On the other hand, nodes that have choice of second stage specify secure shortest route.

Stage 1 –>

A. Certification Process of Authorized Nodes:

EARAN protocol uses cryptographic certificates that come along with message- integrity, authentication and non-repudiation to the route discovery process. Here this protocol therefore requires the use of a trusted certificate server T, whose public key is known to all other valid nodes. Nodes require these certificates to authenticate themselves to other nodes during the exchange process of routing messages. The utilization of public keys and certificates is very rare in various secure ad hoc routing protocols, but most of assume that the presence of this information without any detail description of how it is transmitted. Here keys are pre-generated and exchanged through an existing out-of-band relationship between T and each node. Prior joining the ad hoc network, each node has to quest a certificate signed by T. Every node accepts exactly one certificate after securely authenticating its identity to T. So a node A receives a certificate from trusted certificate server T as follows:-

T - > S: Cert $_{S}$ = [IP_S, K_{S+}, t, e, G_{ID}, $U_{MAC\ ADDRS}$] K_{T-}

Where

IP_S - > IP Address of S

K_{S+} - > Public Key of S

t - > Time stamp when the certificate was created

e - > Duration of the Certificate

G_{ID} - > Multicast Group ID of a Network

$U_{MAC\ ADDRS}$ - > Unique MAC Address of particular node

K_{T-} - > Whole Certificate Signed by T

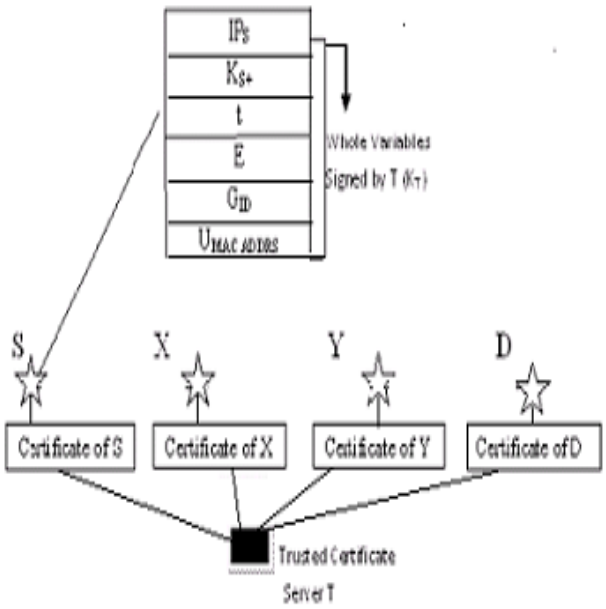

Figure 1. Certification Process of Authorized Nodes

These all variables discussed above concatenated and signed by Trusted Certificate Server (T). It is required that all nodes must hold fresh certificates with the trusted server T.

Stage 2 - >

B. Process of Authorized Route Discovery:

Nodes that have of second stage specify secure shortest route. For source the purpose of end-to-end authentication is to check that the intended destination was reached. Here the source trusts the destination to choose the return path. The route discovery process of EARAN protocol starts with a node broadcasting a RDP (Route Discovery Packet) to its neighbours.

S - > brdcast: [RDP, IP_D, N_S, G_{ID}, $U_{MAC\ ADDRS}$] K_{S-} , Cert $_{S}$

Route Discovery Packet (RDP) includes following variables:-

IP_D - > IP address of the Destination

N_S - > Nonce that uniquely identify an RDP coming from a source. Every time S performs Route Discovery then it monotonically increases the nonce.

G_{ID} - > Multicast Group ID

$U_{MAC\ ADDRS}$ - > Unique Mac Address of every particular node

K_{S-} - > All variables signed by its private key (K_{S-})

Cert $_{S}$ - > Certificate of S

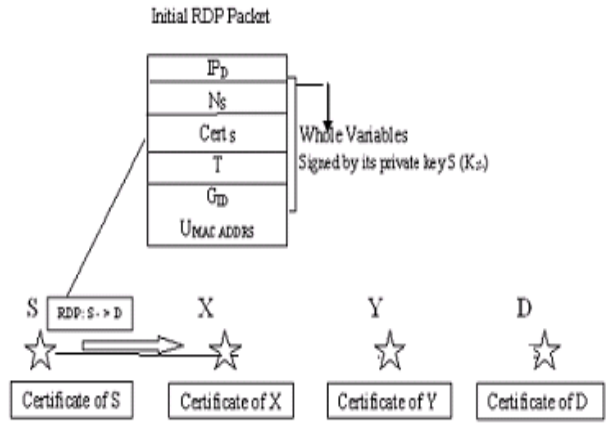

Figure 2. Route discovery Part 1

By adding the U $_{MAC\ ADDRS}$ in RDP Packet, the transmission of packet is more secure and it takes less time to reach its destination. When a node receives a Route Discovery Packet (RDP), a reverse path back to the source is set up by recording the neighbour from which it received the Route Discovery Packet. So it is ready upon accepting a reply message to send back to the source. In addition to, the receiving node consumes S's public key, which it take out from S's certificate to authorize the signature and examine that A's certificate has not terminated. The receiving node also verifying the (N_S , IP_S) tuple to examine that it has not already processed this Route Discovery Packet (RDP), because nodes do not send messages with already –seen tuples. Therefore, receiving node signs the content of the message then attaches its own certificate and send broadcasts the messages to each of its neighbours. The signature also protects from spoofing attacks that may change the route or from loops.

Let X is a neighbour that has acquired from S the RDP broadcast, which it afterwards broadcast again.

X - > brdcast: [[RDP, IP_D, N_S, G_{ID}, $U_{MAC\ ADDRS}$] K_{S-}], K_{X-} ,Cert $_{S,}$ Cert $_X$

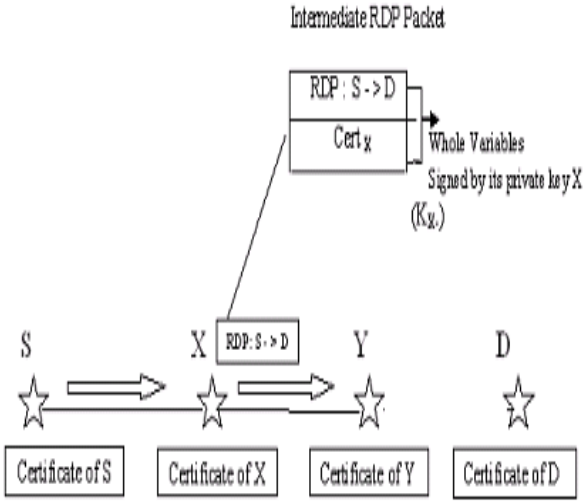

Figure 3. Route Discover Part 2

Afterwards, acquiring the Route Discovery Packet (RDP), X's neighbor Y authorizes i.e validate the signature for both S, the RDP initiator and X, the neighbor it gets RDP from using the certificate in the RDP. Y then delets X's certificate and signature, records X as its predecessor and then signs the contents of the message that is originally broadcast by S and attaches its own certificate. Y then broadcast again the RDP.

Y - > brdcast : [[RDP, IP_D , N_s ,$G_{ID,}U_{MAC\ ADDRS}$] K_{S-}] $K_{Y-,}$,Cert $_{S,}$ Cert $_Y$

Every intermediate node along the path repeats the same steps as Y.

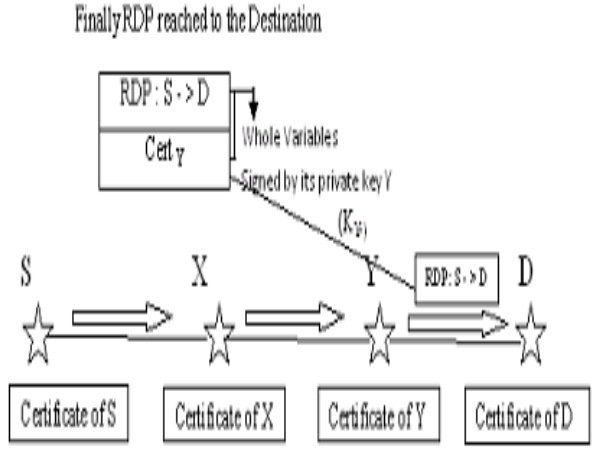

Figure 4. Route Discover Part 3

C. Process of Authenticated Route Setup:

When the message is received by the destination, who responds the first RDP that it acquires for a source and a given nonce. There is no compulsory that the first Route discovery Packet "(RDP) acquires travelled along the less no. Of hops that contains the shortest path of the source. Additionally RDP packet do not enclose a hop count or any specific recorded source route and as well as at each hop malicious nodes are signed, so malicious nodes have no scheme to redirect the traffic. Therefore after receiving the RDP, the destination unicasts a RREP (Route Reply Packet) back along the reverse path to the source.

Let the first node that acquires the Route Reply Packet sent by D to be node Y:

D - > Y: [RREP, $IP_{S,}$ $N_{S,}$ G_{ID}, $U_{MAC\ ADDRS}$] K_{D-}, Cert $_D$

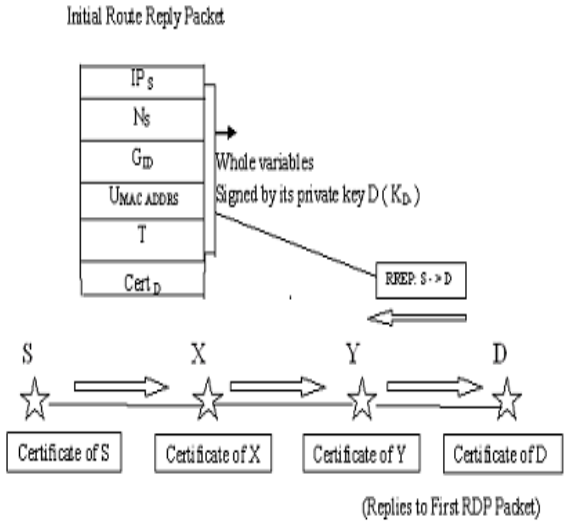

Figure 5. Route Setup Part 1

The Route reply encloses a packet type identifier ("RREP") , the IP address of S (IP_S), the certificate belonging to D (Cert $_D$) and the nonce sent by S. Nodes that acquires the RREP send the packet back to the predecessor

from which they acquired the original Route Discovery Packet. Every node along the reverse path back to the source signs the route Reply packet and attaches its own certificate before sending the Route Reply Packet to the next hop.

So, Now Let Y's upcoming hop to the source is node X. Then

Y : - > [[RREP, IP $_S$, N $_{S,}$ $G_{ID,}$ $U_{MAC\ ADDRS}$] K_{D-}] K $_{Y-}$, Cert $_D$, Cert $_Y$

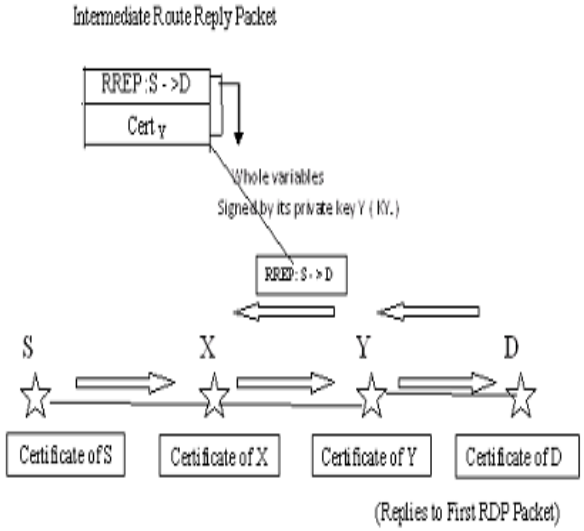

Figure 6. Route Setup Part 2

Now X validates Y's signature on the received message, delets the signature and certificate and then signs the contents of the message and attaches its own certificate before unicasting the Route Reply Packet to S:

X - > S : [[RREP , IP $_S$, N $_{S,}$ $G_{ID,}$ $U_{MAC\ ADDRS}$] K_{D-}] K_{X-} , Cert $_D$, Cert $_X$

Now every node verifies the nonce and signature of the previous hop as the Route Reply Packet is returned back to the source. This prevents from attacks where malicious nodes Originate routes by impersonation and then replay's of D's message. Afterwards when the source receives the Route Reply Packet it checks the destination's signature and also the nonce returned back by the destination.

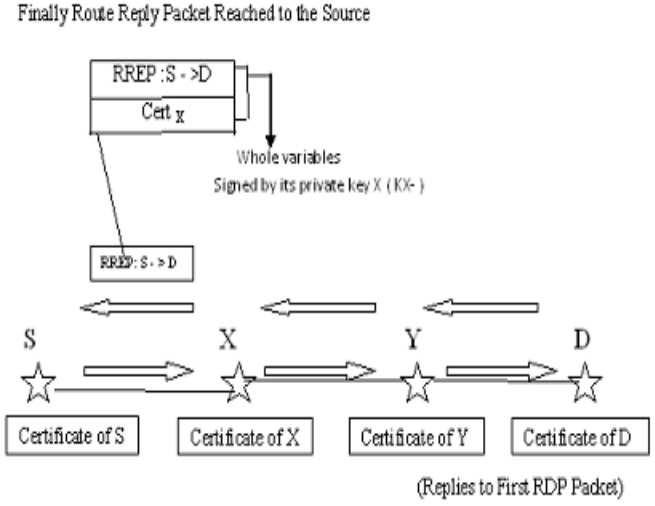

Figure 7. Route Setup Part 3

a. Here to verify the certificate we assume that when each certificate successfully reaches to the destination at least three time then we can say that certificate is legitimate and path followed by that certificate is verified.

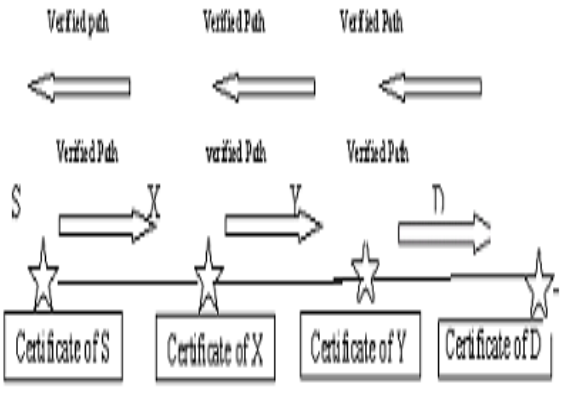

Figure 8. Route Setup Part 4

D. Process of Data Transfer:

In Data Transfer Phase of EARAN, for e.g. Source S communicates to the destination in three ways and in all the three data communication ways there is a node that misbehaves. So in this Situation it takes three cases. These are Warning, Suspend and Terminate. In Warning case if node misbehaves it sent the warning to the node that it improves it behavior. If that node still misbehaves then it takes Suspend Case. In this case it suspends the node for some time so that it improves its behavior. If still the node performance is not good and it misbehaves then it finally terminates the node from the network.

E. Process of Route Maintenance:

In the route maintenance process, when no traffic has originated on an existing route for that route's lifetime, so in routing table route is deactivated. When data received on an inactive route creates nodes to develop a RERR (Route Error) message. As well as, nodes utilizes route Error messages to report links in active routes that are broken down due to node movement. Here this is compulsory that all Route Error messages are signed.

For a route between source S and destination D, a node Y produce the Route Error message for its neighbour X as follows:-

Y - > X: [RERR, IP $_S$, IP $_D$,N $_{Y,}$ G_{ID} , $U_{MAC\ ADDRS}$] K_{Y-}, Cert $_Y$

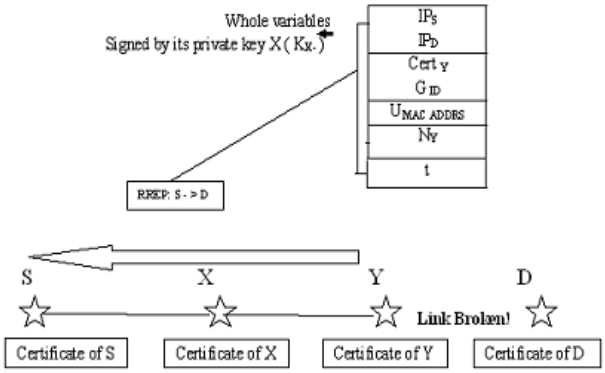

Figure 9. Route Maintenance in EARAN

This particular message is then sends along the path toward the source without any modification and a nonce insures that the Route error message is fresh. It is very hard to discover when Route Error messages are fabricated for links that are truly active and it is not broken. However the signature on the message protects impersonation and also enables non-repudiation.

A node that transfers a large no. of Route Error message whether the route error messages are valid on either fabricated, they should be keep off.

F. Process of Key Revocation:

In the process that a certificate requires to be revoked, the Trusted Certificate server T forwards a broadcast message to the ad hoc group that announcing the revoked node. For calling the revoked certificate Cert $_D$, the transmission shown as follows:-

T - > brdcast: [revoke, Cert $_T$] K_T-

Any node acquiring this message broadcast again it to its neighbours. It is require that revocation notices should to be stored until the revoked certificate run out i.e. expired normally. Any neighbour of the node that consists with the revoked certificate requires being reform routing as required to prevent transmission through the untrustworthy node.

However this method is not failsafe. In some particular cases, the untrustworthy node that keeps its certificate revoke may be the sole-connection between two regions of the ad hoc network. In this case, the untrustworthy node may not send the notice of revocation for its certificate that result in a separation of the network that lasts until the untrustworthy node is no longer the sole-connection between the two separation ports.

At the time that the revoked certificate must have expired, the untrustworthy node is not able to renew the certificate again and also routing across the node ceases.

IV. CONCLUSION

Current ad hoc routing protocols are subject to many attacks such as modification or fabrication of routing messages or impersonation of other nodes. These can also permit attackers to act upon a victim's selection of routes and enable denial-of-service attacks. In this paper, EARAN gives authentication and non-repudiation services by using cryptographic certificates that ensures end-to-end authentication. Furthermore, EARAN is on demand distance vector routing, it get benefit of low cost and high performance because of its reactive nature. It performs well than ARAN in terms of packet transmission and provide more security to the network.

V. REFERENCES

[1] E.Venkat Reddy, " Trustworthy Robust Routing Protocol for Mobile Ad hoc Network", Amina Institute of Technology, Hyderabad, Andhra Pradesh-India, Published in E. Venkat reddy/ International Journal Of Engineering Science and Technology Vol.2 (2), 2010,77-86.

[2] [2] K.Seshadri Ramana, Dr. A.A.Chari, Prof. N.Kasiviswanth, "Trust Based Security Routing in Mobile Ad hoc Networks", Kurnool-518007, A.P., India. Published in K.Seshadri Ramana et.al./ (IJCSE) International Journal on Computer Science and engineering, Vol. 02, No. 02, 2010, 259-263.

[3] Seema Mehla, Bhawna Gupta, Preeti Naagrath , " Analyzing security of Authentiated Routing Protocol (ARAN)" , Published in International Journal on Computer Science and Engineering, Vol. 02, No. 3,2010, 664- 668.

[4] Kimaya Sanzgiri, Daniel laFlamme , Bridget Dahill, "Authentiacted Routing for Ad hoc Networks", Department of Computer Scince, University of California,Santa Barbara,, Published in IEEE INCP 2002.

[5] C.Sreedhar,, Dr.S.Madhusudhana Verma, Prof.N.Kasiviswanath, " A Survey on Security Issues in Wireless Ad hoc network Routing Protocols", Kurnool, Andhra Pradesh, India, Published in C.Sreedhar et.al. (IJCSE) International Jounal on Computer Science and Engineering, Vl. 02, No. 02,2010,224-232.

[6] Yih-Chun HU, Adrian Perrig, David B.Johnson, " ARIADNE: A Secure On-Demand Routing Protocol for Ad Hoc networks, MobiCOm 2002, September 23-28, 2002, Atlanta, Georgia, USA.

[7] Yih-Chun Hu, David B. Johnson and Adrian Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications, pp. 3-13, IEEE, Calicoon, NY, June2002.

[8] Manel Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector (SAODV) Routing INTERNET-DRAFT draft-guerreo-manet-sadodv-00.txt, August 2002. Published in the IETF MANET Mailing list October 8th 2001.

[9] P.Papadimitratos and Z.Haas, "Secure Routing for Mobile Ad Hoc Networks", in Proc. SCS CNDS, Jan. 2002.