ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 3, March 2013

An Unobservable Secure Routing Protocol against Wormhole and Black hole Attacks in MANET.

Annie Jesus Suganthi Rani.A and R.Mathan

Abstract— **Mobile ad-hoc network (MANET) is a self-configuring infrastructure-less network of mobile devices. The sensitive information such as mobility behavior should be kept private from adversaries in wireless environments. Privacy-preserving routing is crucial for some ad-hoc networks that require stronger privacy protection say battle field. USOR is an Unobservable Secure On-demand Routing protocol for mobile ad hoc network that achieves unlinkability and unobservability by employing anonymous key establishment based on group signature. Each node only has to obtain a group signature signing key and an ID-based private key from an offline key server or by a key management scheme. Due to dynamic nature and lack of centralized control, the ad hoc networks are vulnerable to attacks. There is no security provision against the wormhole and black hole attacks in existing USOR protocol. In a wormhole attack, attackers tunnel the data from one end of the network to the other, leading distant network nodes to trust they are neighbours and making them communicate through the wormhole link. Black hole nodes are those malicious nodes that conform to forward packet to destination. But they do not forward packet intentionally to the destination node. AODV, USOR and modified USOR are implemented on ns2, and there performances are evaluated.**

Index Terms—**Anonymity, Privacy, Security, Unlinkability, Unobservability, USOR.**

I INTRODUCTION

A.WIRED VS WIRELESS NETWORK

In wired networks one cannot intercept signals down the wire; hence it has high security whereas in wireless networks signals can be intercepted therefore it has low security.

Manuscript received March 10, 2013.

Annie Jesus Suganthi Rani.A, *Computer Science and Engineering, Holycross Engineering College under Anna University, Tirunelveli, Tamil Nadu, India.*

R.Mathan, *Assistant Professor, Computer Science and Engineering, Holycross Engineering College under Anna University, Tuticorin, Tamil Nadu, India.*

The speed in wired network is immensely higher than wireless network. Wireless network is affected by other signals and radio waves and they have limited signal range. Wired networks uses long cables which are cheap. But cable can be damaged. In wireless environment less or no cables are used. More people can be connected to one access point, convenient, allows freedom of working anywhere.

B. PRIVACY PRESERVING PROPERTIES

Privacy-Preserving is known as maintaining the private information securely. **Anonymity** is the state of being not identifiable within a set of subjects, the anonymity set. **Unlinkability** of two or more IOI from an attacker's perspective means that the attacker cannot sufficiently distinguish whether the IOI's are related or not. **Unobservability** of IOI from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.

C. CLASSIFICATION OF ATTACKS

Possible attacks in each layer are as follows: Application layer attacks are malicious code and repudiation. Transport layer attacks are session hijacking and flooding. Network layer attacks are Sybil attack, flooding, black hole, grey hole, worm hole, link spoofing, link withholding, location disclosure, etc... Data Link layer attacks are malicious behavior, selfish behavior, active attack, passive attack. Physical layer attacks are interference, traffic jamming, eavesdropping.

A routing protocol is a set of rules or standard that determines how routers on a network communicate with each other and exchange information enabling them to select best routes to a remote network.

The next section comprises of related work that detail about the existing anonymous routing protocol in ad hoc network. Section III describes about the unobservable secure routing protocol which detects the wormhole and black hole attacks. Mechanism to defend against the attacks is described in Section IV. Finally we summarize and conclude the paper.

II RELATED WORK

USOR[1] is an unobservable secure routing scheme that offers complete unlinkability and content unobservability for all types of packets. USOR uses a novel combination of group signature and ID-based encryption for route discovery. It solves the elliptic curve discrete log problem (ECDLP) and the bilinear Diffie-Hellman problem (BDH) on the two groups is hard. Both the group signature scheme and the ID-based scheme are based on pairing of elliptic curve groups of order of a large prime.

ANODR[2], an anonymous on-demand routing protocol for mobile ad hoc networks addresses route anonymity and location privacy. For **route anonymity**, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination. For **location privacy**, ANODR ensures that adversaries cannot discover the real identities of local transmitters. The design of ANODR is based on "broadcast with trapdoor information", which includes features of two existing network and security mechanisms, namely "broadcast" and "trapdoor information".

In ASR[3] Anonymous Secure Routing protocol that can provide additional properties on anonymity, i.e. Identity Anonymity and Strong Location Privacy and at the same time ensure the security of discovered routes against various passive and active attacks has been proposed.

ARM [4], Anonymous on demand routing scheme for MANET is an efficient solution that provides anonymity in a stronger adversary model. The adversaries are an external global passive adversary who can observe all possible communications between all nodes in the network at all time and a cooperating node inside the network, potential adversary. It prevents global passive adversary from learning the destination of the messages and which nodes are parts of the path from the source to the destination. It prevents a cooperating node from not being able to determine whether another node in the network is the sender or the destination of a particular message and from not being able to determine whether another node is part of a path between two nodes.

AnonDSR[5] stands for Efficient Anonymous Dynamic Source Routing for mobile ad-hoc networks which provides three levels of security protection namely user security, node identity and anonymity. It uses onion encryption. Unobservability is not provided in AnonDSR. An anonymous routing protocol with multiple routes called ARMR[6], make use of one-time public/private key pairs to achieve anonymity and unlinkability. ARMR uses one-time public keys and bloom filter to establish multiple routes for MANETs.

III USOR PROTOCOL

A. KEY GENERATION

Group signature scheme is a method for allowing a member of a group to anonymously sign a message on behalf of the group. Key server generates a group public key PU_{gp} which is publicly known by everyone. It generates a private group signature key PR_x for each node X. ID-based encryption is a type of public-key encryption in which the public key of a user is some unique information about the identity of the user, which allowed users to verify digital signatures using only public information such as the user's identifier.

B. ANONYMOUS KEY ESTABLISHMENT

Every node in the ad hoc network communicates with its direct neighbours within its radio range for communication. Source node 'S' with a private signing key PR_S and a private ID-based key K_S in the ad hoc network communicate with its direct neighbours.

(1) S generates a random number rS using random generator. It computes a signature of r_S using its private signing key PR_S to obtain $SIG_{PRs}(r_S)$. Anyone can verify this signature using the group public key PU_{gp}. S broadcast (r_S, $SIG_{PRs}(r_S)$) within its neighbourhood. (2) X neighbourhood of S receives (r_S, $SIG_{PRs}(r_S)$), verifies the signature on successful verification it computes $SIG_{PRx}(r_S|r_P)$ using its private signing key PR_X and r_X X's random number. X computes the session key $k_{SX} = H(r_S r_X)$, and replies to S with message (r_X, $SIG_{PRx}(r_S|r_P)$, $E_{Ksx}(k_x|r_S|r_X)$) where k_x is X's local broadcast key. (3) S verifies the signature inside the message from X. On valid signature 'S' proceeds to compute the session key with X as $k_{SX} = H(r_S r_X)$. S generates a local broadcast key k_S, and sends E_{Ksx} ($k_S|k_X|r_S|r_X$) to its neighbour X to inform X about the established local broadcast key. (4) X receives the message from S and computes the same session key as $k_{SX}=H(r_S r_X)$. It then decrypts the message to get the local broadcast key k_S.

C. ROUTE REQUEST

The route request messages flood throughout the whole network, while the route reply messages are sent backward to the source node only. S chooses a random number r_S, and uses the identity of node D to encrypt a trapdoor information that only can be opened with D's private ID based key, which yields $E_D(S,D, r_S)$. S selects a sequence number 'seq. no.' for this route request, and another random number N_S as the route pseudonym, which is used as the index to a specific route entry. To achieve unobservability, S chooses a nonce $Nonce_S$ and calculates a pseudonym as $Nym_S = k_{SX}(k_S|Nonce_S)$.

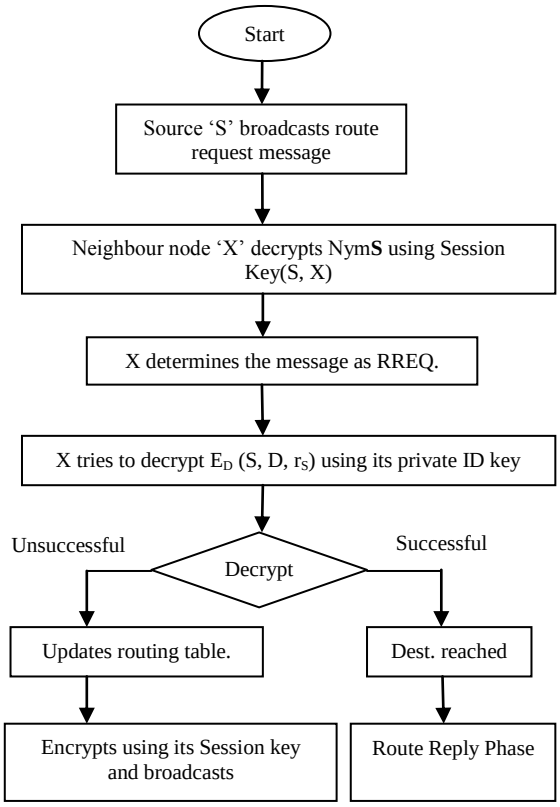

Fig. 1 ROUTE REQUEST - FLOW CHART

Each node maintains a temporary entry in his routing table (seqno, Prev RNym, Next RNym, Prev hop,Next hop) where seqno is the route request sequence number, Prev RNym denotes the route pseudonym of previous hop, Next RNym is the route pseudonym of next hop, Prev hop is the upstream node and Next hop is the downstream node along the route. As any node does not know the real identity of its upstream or downstream node.

S broadcasts the message: {$Nonce_S$, Nym_S, E_{Ks} (RREQ, N_S, E_D (S, D, r_S), seq. no.)}

Scr ID	Desn ID	Scr Loc X	Scr Loc Y	Scr Speed X
4	4	4	4	4
Scr Speed Y	TS	Nonce	Nym	E_{ks} (RREQ, N_s, E_d(S,D,r_{sP}), seqno)
4	8	32	32	32 bytes

Fig. 2 RREQ Packet format 128 bytes

D. ROUTE REPLY

After route request reaches the destination node D, it starts to prepare a reply message to the source node. Route reply messages are unicast instead of broadcast is used to save communication cost. D chooses a random number r_D and computes a ciphertext E_S(D, S, r_S, r_D) showing that it is the valid destination capable of opening the trapdoor information.

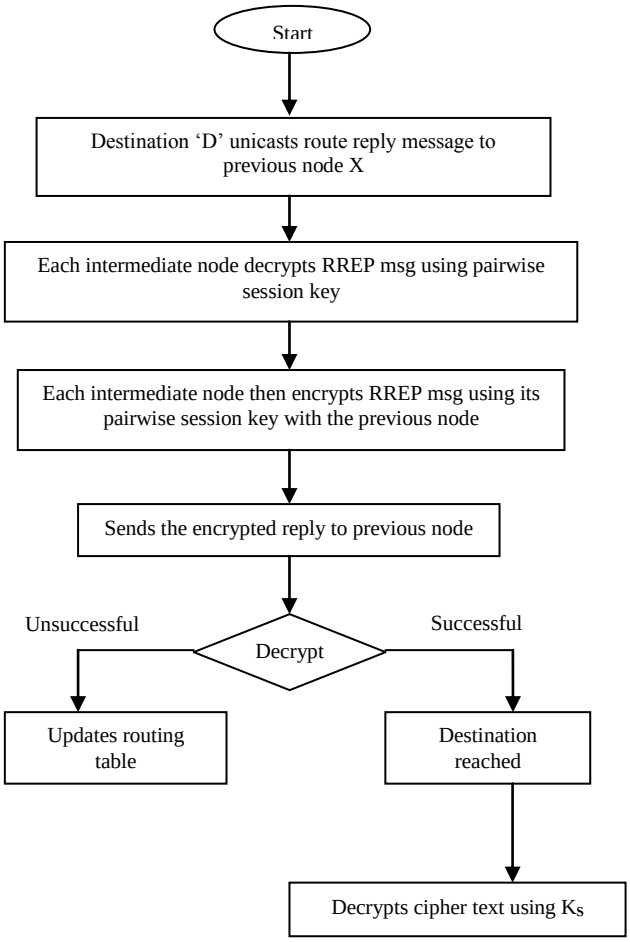

Fig. 3 ROUTE REPLY - FLOW CHART

A session key k_{SD} = H($r_S r_D$|S|D) is computed for data protection. Then it generates a new pairwise pseudonym Nym_{XD} = H(k_{XD}|$Nonce_D$) between X and him. At the end, using the pairwise session key k_{XD}, he computes and sends the following message to intermediate node X: {$Nonce_D$, Nym_{XD},E_{KXD}(RREP,N_X,E_S(D, S, r_S, r_D), seqno)}.

Scr ID	Desn ID	Scr Loc X	Scr Loc Y	Scr Speed X
4	4	4	4	4
Scr Speed Y	TS	Nonce	Nym	E_{ks} (RREP, Nc, E_s(D,S,r_{sP},r_{dP}), seqno)
4	8	32	32	32 bytes

Fig. 4 RREP Packet format 128 bytes

Other intermediate nodes perform the same operations as D does. Finally, the following route reply is sent back to the source node S by intermediate nodes say 'X' S decrypts the ciphertext using the right key k_{SX} and verifies that $E_S(D, S, r_S, r_D)$ is composed faultlessly. Now S is ensured that D has successfully opened the route request packet, and the route reply is really originated from the destination node D. X unicasts the message: $\{Nonce_D, Nym_{XD}, EK_{XD}(RREP, N_X, E_D(S, D, r_S, r_D), seq.\ no.)\}$

E. DATA TRANSFER

Source node S after successfully finding of a route to the destination node D, S starts unobservable data transmission under the protection of pseudonyms and keys.

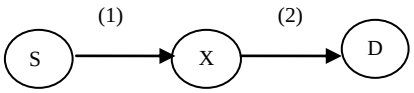

Fig. 5 DATA TRANSFER

As illustrated in Fig.5, data packets from S must traverse X to reach D.

Format of data packets sent by S:

$Nonce_S$, Nym_{SX}, E_{kSX} (DATA,N_S, seqno, E_{kSD}(payload)) (1)

X receives message from S. X knows that this message is for him according to the pseudonym Nym_{SX}. After decryption using the right key, X knows this message is a data packet and should be forward it to D according to route pseudonym N_S. X computes and forwards the data packet.

Format of data packets sent by X:

$Nonce_X$, Nym_{XD}, E_{kXD} (DATA,N_X, seqno, E_{kSD}(payload)) (2)

The data packet is further forwarded by other intermediate nodes until it reaches the destination node D. At the end, the data packet is received by D. By looking up in the route table, D knows himself as the destination of the packet. So he is able to decrypt the encrypted payload with the session key k_{SD}.

Table 1 Routing Table for S, X, D

Node	Sn	Prev_Nym	Next_RNym	Prev_Hop	Next_Hop
S	sn	-	N_S	-	K_X
X	sn	N_S	N_X	k_S	K_D
D	sn	N_X	-	k_X	-

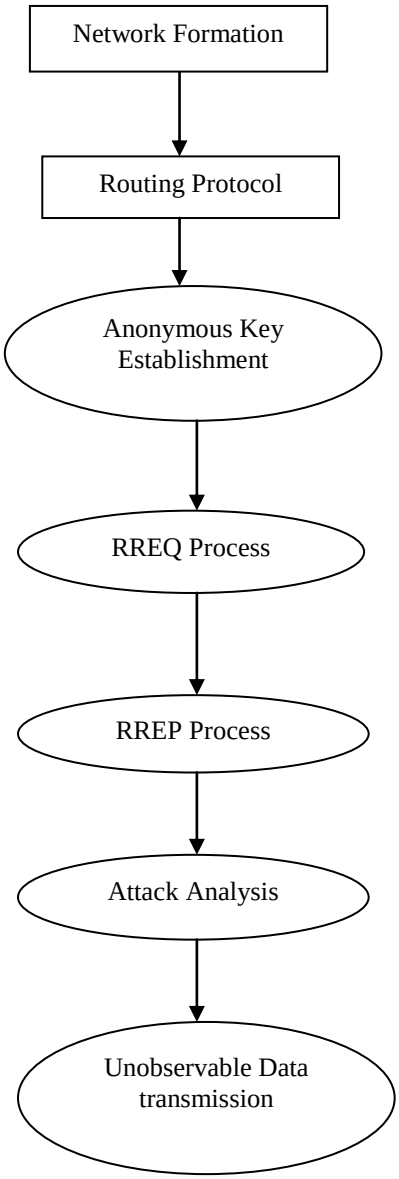

Fig. 6 OVERALL PROCESS

IV ATTACKS AND MECHANISM

Wormhole Attack: For launching a wormhole attack, an adversary connects two distant points in the network using a direct low-latency communication link called as the ***wormhole link***. The wormhole link can be established by a variety of means either by using an Ethernet cable, a long-range wireless transmission, or an optical link. Once the wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end. Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and this is the reason the attacks are serious. Activities of wormhole are they record the

wireless data they overhear. They forward it to each other. It replays the packets at the other end of the network. It replays valid network messages at improper places. It makes far apart nodes believe that they are immediate the neighbors.

An approach to detect the wormhole attack is based on the packet leashes [7]. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Leashes are designed to protect against wormholes over a single wireless transmission. When packets are sent over multiple hops, each transmission requires the use of a new leash. Leashes can be classified as geographical leashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash establishes an upper bound on a packet's lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed-of-light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet travelled further than the leash allows.

BlackHole Attack: A Black hole attack is an attack where all the packets in the network are redirected to a specific node the black hole node. When the packets reach this malicious node, they merely disappear into a black hole in universe. To carry out a black hole attack, the black hole node takes advantage of the ad hoc routing protocol, such as AODV or DSR, to advertise itself as having a valid route to the destination node, even though the route is spurious, with the intention to intercept packets. Or malicious node waits for neighbouring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere.

Malicious node falsely advertises good path to the destination node during the path finding process. The intension of the malicious nodes could be to hinder the path finding process or to interrupt all the data packets being sent to the concerned destination node. Fake RREQ packets [8] are used to catch the malicious nodes. The fake RREQ used to find the black hole nodes in the network is similar to the actual DSR RREQ packet, except that a fake destination address is used, which really doesn't exists.

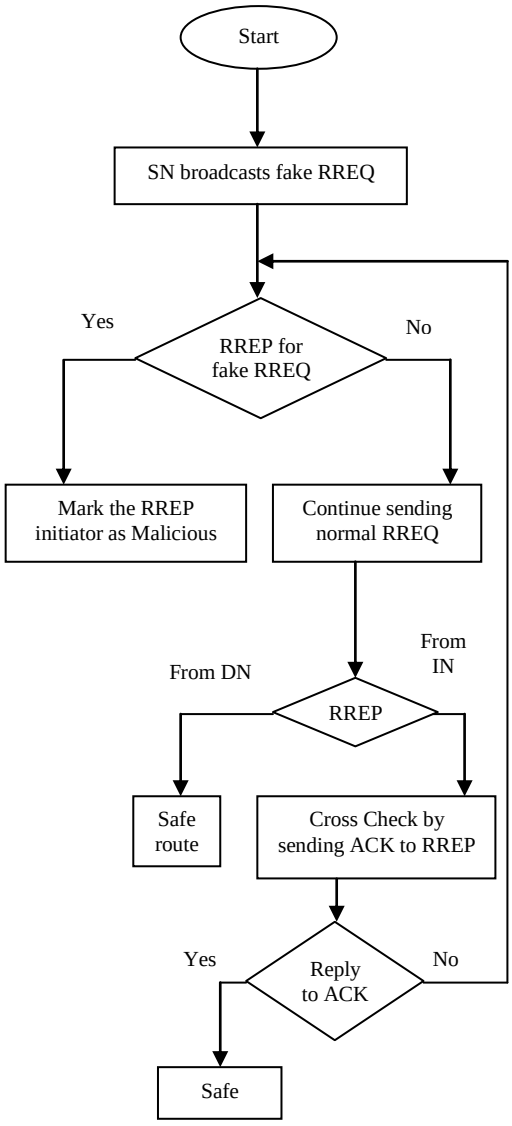

Fig. 7 BLACK HOLE ATTACK ANALYSIS - FLOW CHART

DESCRIBTION:

ACK : Acknowledgement
Dest : Destination
DN : Destination Node
E_K(Data) : Encrypted Data
IN : Intermediate Node
K : Key
Loc : Location
N_{once} : Number used once
N_S :Route Pseudonym
RREP : Route Reply
RREQ : Route Request
Scr : Source
Sn : Sequence Number
SN : Source Node
TS : Time Stamp

V PERFORMANCE ANALYSIS

TABLE 2 SIMULATION PARAMETERS

PARAMETERS	VALUE
Encryption	22ms
Decryption	17ms
Group-Signature-Generation	24ms
Group-Signature-Verification	26ms
Wireless-Radio-Range	250m
Average-Node-Speed	0-10m/s
Source-Destination-Pairs	25
Traffic-Type	512-byte
Traffic-Frequency	4
Wireless-Bandwidth	2Mbps
Node-Pause-Time	0s
Key-Update-Interval	40s
Average-Hops	2.90
Average-Neighbours	12.69

Packet Delivery Ratio

Fig. 8 Packet Delivery Ratio

The performance of AODV and USOR is analyzed. Packet delivery ratio is measured against the speed. And packet delivery delay is measured against speed.

Reasons for lower packer delivery ratio and greater delay of USOR, only trusted neighbours will forward route packets for each other, otherwise packets are simply dropped.

Packet Delivery Delay

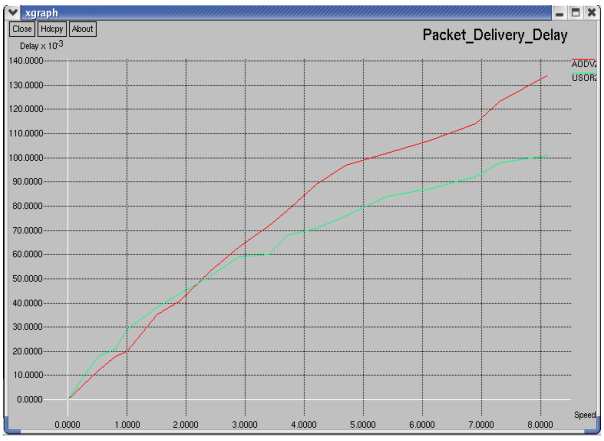

Fig. 9 Packet Delivery Delay

VI CONCLUSION

USOR is an Unobservable Secure On-demand Routing protocol for mobile ad hoc network that achieves unlinkability and unobservability by employing anonymous key establishment based on group signature. There is no security provision against the wormhole and black hole attacks in existing USOR protocol. In a wormhole attack, attackers tunnel the data from one end of the network to the other, leading distant network nodes to trust they are neighbours and making them communicate through the wormhole link. Black hole nodes are those malicious nodes that conform to forward packet to destination. But they do not forward packet intentionally to the destination node. AODV, USOR and modified USOR are implemented on ns2, and there performance is evaluated.

Future work is to study how to resistant USOR routing protocol against DoS attacks.

ACKNOWLEDGEMENTS

The authors would like to thank THE ALMIGHTY for showering his blessings throughout their life. They thank all the anonymous reviewers for their valuable feedback.

REFERENCES

[1] Zhiguo Wan, Kui Ren, and Ming Gu, “USOR: An Unobservable Secure On-Demand Routing Protocol for Mobile Ad Hoc Networks” IEEE Trans. on Wireless Communications, vol. 11, no. 5, pp. 1922-1932, May 2012.

[2] J. Kong and X. Hong, “ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad-Hoc Networks,” in Proc. ACM MOBIHOC’ 03, pp. 291–302.

[3] B. Zhu, Z. Wan, F. Bao, R. H. Deng, and M. KankanHalli,

"Anonymous Secure Routing In Mobile Ad-Hoc Networks," in Proc. 2004 IEEE Conference on Local Computer Networks, pp. 102–108.

[4] S. Seys and B. Preneel, "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks," in Proc. 2006 IEEE International Conference on Advanced Information Networking and Applications.

[5] L. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks," in Proc. 2005 ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 33– 42.

[6] Y. Dong, T. W. Chim, V. O. K. Li, S.-M. Yiu, and C. K. Hui, "ARMR: Anonymous Routing Protocol with Multiple Routes For Communications in Mobile Ad Hoc Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 15 2009.

[7] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.

[8] Issac Woungang, Sanjay Kumar Dhurandher, Rajendrar Dheeraj Peddi, Mohammed S. Obaidat, "Detecting Blackhole Attacks on DSR-based Mobile Ad hoc Network", International Conference on Computer, Information and Telecommunication Systems (CITS), May 2012.

Annie Jesus Suganthi Rani.A is a PG Scholar degree in computer science and engineering from Holycross Engineering College, Tuticorin, Tamil Nadu. She received her B.E. degree in computer science and engineering from Infant Jesus College of Engineering, Tuticorin, Tamil Nadu in 2011. Her area of interest is Mobile Ad Hoc Network and Security for Ad hoc networks.

R.Mathan is an Assistant Professor in Holycross Engineering College, Tuticorin. He received his B.E. degree in computer science and engineering from Tamil Nadu College of Engineering, Coimbatore, Tamil Nadu in 2006 and his M.E. degree in networking engineering from Kalasalingam University, Srivilliputtur, Tamil Nadu in 2011. He worked at Allsec Technologies Ltd as CS officer. His area of interest is Networking.