ISSN:0975-9646

LERP: A Secure Location Based Efficient Routing Protocol

Rajan Gandhi [#1], Prof Prasanna Joeg *[2]

[#] *PG Research Scholar, Department of Computer Science Engineering*
Vishwakarma Institute of Technology, Pune

[*]*Professor at Department of Computer Science of Engineering*
Vishwakarma Institute of Technology, Pune

***Abstract*— In wireless communication and mobile Ad hoc network mainly concern with security. In MANETs use anonymous routing protocol which should be provide anonymity for route, source, and destination. So this protocol hides the route of source to destination from outside observer and gives anonymity protection from attacker. There is many protocol available which does not provide full anonymity. So we developed secure location based efficient routing protocol which provides anonymity for source, destination and route. This protocol is randomized in nature. Existing anonymity protocol depends on Hop by Hop encryption and redundant traffic. So it generates high cost for communication. LERP dynamically partition a network into zone and choose random node in that zone which make anonymous route between source and destination. We also provide solution of wormhole attack. Experimental results exhibit consistency with the theoretical analysis, and show that LERP achieves better route anonymity protection and lower cost compared to ALERT anonymous routing protocol with wormhole attack.**

***Keywords*— Mobile ad hoc network, Anonymity, Hop by Hop encryption, redundant traffic, wormhole attack, AOMDV.**

INTRODUCTION

The development of mobile network and wireless communication have emerge in more form. It uses in many application and area like commerce, military, education and entertainment. MANETs has infrastructure less independent feature. So this feature makes ideal choice for communication. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyse data and traffic analysis by communication eavesdropping or attacking routing protocols. Anonymous routing is crucial in MANET for better communication by hiding node identities and prevent from the outside observer. Mostly in MANETs anonymity in terms of source, destination and route. Route anonymity considers as path between source and destination should be anonymous so attacker cannot find flow of packet. For source and destination anonymity hide the real identity and location of node from the other node. Some protocol depends on Hop by Hop encryption means this transfer the packet node to node. . In the sense protocol use some algorithm to transfer the packet. Shortest route path algorithm or GPSR. Some protocol depends on redundant traffic. Means if in network there is more traffic than first it wait for clear the traffic. So this protocol takes more time for communication.

Existing anonymity protocol depends on Hop by Hop encryption [1] and redundant traffic [2]. Most of the current approaches cannot provide all of the aforementioned anonymity protections. For example, ALARM [3] cannot protect the location anonymity of source and destination, SDDR [4] cannot provide route anonymity, and ZAP [5] only focuses on destination anonymity, ALERT [6] does not provide anonymity protection against wormhole attack. Many anonymity routing algorithms are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR) [7] that greedily forwards a packet to the node closest to the destination. However, the protocol's strict relay node selection makes it easy to reveal the source and destination and to analyse traffic. However, existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs.

In order to provide high anonymity for source, route and destination with low cost, propose secure location based routing algorithm (LERP). LERP first dynamically partition the network into zone and randomly choose a node into that zone. In each routing step, data sender or forwarder partition the network and separate itself with destination zone. Then it choose random node and use GPSR algorithm to send next relay node. So LERP is resilient to timing attacks. In summary, LERP provide following advantage.

1. *Anonymous routing:* LERP provide anonymity for source, destination and location anonymity.
2. *Low cost:* Rather than relying on hop by hop encryption or redundant traffic, LERP use randomized routing and provide anonymity protection.
3. *Resilience to timing attack:* LERP provide solution for timing attacks [8] because of non-fix routing path for a source destination pair.
4.

I. LERP: A SECURE LOCATION BASED EFFICIENT ROUTING PROTOCOL

A. Dynamic Pseudonym and Location Service

In one node communication, source node S send the request to destination node D and destination node D reply with some data. In LERP, in network each hop uses dynamic pseudonym as its node identifier rather than using its real mac address, which can be used to trace the node existence node in the network. For avoid pseudonym

collision, uses collision resistance function such as hash SHA-1 [9]. To prevent from attacker to re-computing, time stamp should be smaller value.

In previous algorithms, we show that location of destination and public key can be known by others. So we using secure location service [10] to provide information of each node location and public key. So location service enables source node who know about destination node, securely obtain public key and location of destination node. By location of destination determine next hop in geographic routing. The public key use for securely establish symmetric key for secure communication.

B. LERP routing algorithm

LERP is a randomized in nature. Its features dynamic and unpredictable routing path, which consist of number of intermediate relay node. As shown in Fig.1, given area called as zone. First we do partition of that zone as horizontal than vertical. Such zone partitioning continuously until we have smallest zone in an alternative manner like horizontal and vertical. This process can be known as hierarchical process.

Fig.1 shows an example of LERP routing. In that zone having K nodes where D reside destination zone denoted as Z_D. K is used to control the degree of anonymity for destination protection. In fig.2 darkest zone is the destination zone. So in LERP routing, first check whether source and destination in same zone. If so, then it divides the zone alternatively in the horizontal and vertical manner. Repeat the process until itself and Z_D is not in same zone. It then randomly chooses position of other zone called temporary destination (TD), and uses GPSR algorithm to send the data to the node closest to TD. This node is known as random forwarder (RF). So LERP achieved K anonymity [11] for destination by broadcast the data to the all node and whoever node has destination public key that node accept the data and other packet will be dropped.

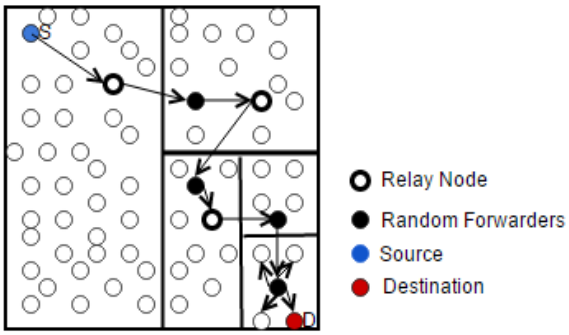

Fig.1. Routing among zone in LERP

Fig.1. shows that S trying to communicate with D. There are also many other possible path for communicating. S first horizontally divide the are into two equal zone for separating S and Z_D. Then S select first temporary destination (TD) where Z_D reside. Then S uses GPSR to send packet to TD. The packet is forwarded by several relays until reaching a node that cannot find a neighbour closer to TD. This node is considered to be the first random-forwarder RF. Once RF receive packet, it vertically divides into two regions so Z_D and itself separated in two different zones. Then RF selects next temporary destination and uses GPSR to send packet to next TD. The process repeated until packet receiver finding itself in to Z_D. In Z_D, K nodes will be available. Then node broadcast the packet to K nodes. A larger number of hierarchies generate more routing hopes. Which increase delay but also increase anonymity protection.

C. Packet Format of LERP:

For successfully communication between source and destination, most important thing is how you build your packet. So source and each packet embed following information with transmitted packet.

1) Zone position of Z_D. That will be H partitioned zone.
2) Random forwarders which is currently selected for routing.
3) Location of random forwarders.

With the N^{th} partition of network, attacker should need high computational power to launch the attacks like active attacks. Moreover N^{th} partitioned of zone makes even harder to locate the source. For hiding packet from adversary node, LERP employs cryptography. The work [19] is proved that public key cryptography is costs more overhead compare to symmetric key cryptography. LERP uses symmetric key for encryption. So S can get $D's$ public key from secure location service as we describe earlier. In communication, S first embed symmetric key K_s, encrypted with $D's$ public key. When S send its content then D decrypted using own public key. Therefore, the packet communicate between S and D can be securely protected using K_s.

RREP/RREQ		P_s	P_D	L_{Z_S}	L_{Z_S}	L_{RF}
h	H	K^S_{pub}	$TTL_{K_{pub}}$	K^{Data}_{pub}		Data

Fig.2. Packet format of LERP

Fig.2. shows the packet format of LERP, we are using RREQ/RREP/NAK. A node use NAK for loss of packet.

Letter on we are going to introduced wormhole attack. So for that NAK field will be use and RREQ/RREP is also using for wormhole attack. That will be explained later on. Here because of randomized in nature we omit the MAC header omitted. NAK field is usually using in geographic routing based approaches to reduce traffic cost. In the packet,

K^S_{pub} is used for source public key encryption; P_S is the pseudonym of the source; P_D is the pseudonym of the destination. H is the maximum allowed number of partition and h is number of division made so far. . L_{TD} is the currently location of temporary destination. K^S_{Pub} is the symmetric key of source. $TTL_{H_{pub}}$ is use for source anonymity. K^{Data}_{pub} is use for encryption of data. When

node A wants to know location and public key of node B, it will contact location server as describe in *A*.

D. Source Anonymity

In all communication protocol mainly problem concern about how maintain source and destination anonymity. LERP achieved source anonymity by no other node in network can see the source node except its neighbor's node and creating same starting and forward message. For further security, LERP take number of node and send same packet as source node and hide source node among other node.

LERP utilizes a TTL field in each packet to prevent the packets issued in the first phase from being forwarded in order to reduce excessive traffic. Only the packets of S are assigned a valid TTL, while another packets only have a TTL=0. After decides the next TD, it forwards the packet to the next relay node, which is its neighbour based on GPSR. Every node receive packet but cannot find valid TTL. So whichever node has valid TTL that node can decrypt it and other node will drop such a packet.

E. Destination Anonymity

Destination anonymity is related to how much number of partition we do of that network field. Means if doing more partition of network field then fewer nodes available for destination zone. So we should try that there should be minimum partition take place.

Let's in destination zone having M nodes where D resides denoted as Z_D. M is used to control the degree of anonymity protection for destination. In the sense when packet reaches to the destination zone packet send to the M node which is available to the destination zone Z_D, By this M anonymity protection can achieve for destination.

One problem is where the position of destination zone Z_D resides. Let H denote the maximum number of partition is allowed, using number of node in Z_D and node density ρ, H is calculated by

$$H = log_2(\frac{\rho * G}{k})$$

Where G is the size of the entire network area. Using H, the size of G and the position of D, the source can calculate the zone position of Z_D.

II. STRATEGY AGAINST WORMHOLE ATTACK

This section discusses the strategies to deal with wormhole attack [12]. Wormhole attack is a most active attack now a days and every protocol has problem against wormhole attack about how to deal with it. So in this section we provide solution of this attack with low cost and provide anonymity.

A. Wormhole Attack

Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbours but are actually distant from one another [13]. A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network. Consider Fig.3. in which node A sends RREQ to node B, and nodes X and Y are malicious nodes having an out-of-band channel between them. Node X "tunnels" the RREQ to Y, which is legitimate neighbor of B. B gets two RREQ – A-X-Y-B and A-C-D-E-F-B. The first route is shorter and faster than the second, and chosen by B. Since the transmission between two nodes has rely on relay nodes, many routing protocols have been proposed for ad hoc network. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes as shown in Fig.3. the resulting route through the wormhole may have lower hop count than normal routes. In with this, attackers using wormhole can easily manipulate the routing priority in MANET to perform eavesdropping, packet modification or perform a DOS attack. The entire routing system in MANET can even be brought down using the wormhole attack

There are several technique and algorithms available for detection and prevention. Technique like packet leash, Time of flight, Delphi, LiteWorp. Algorithms like DSDV (Destination sequenced distance vector) [14], OLSR (Optimized link state routing) [15], DSR (Dynamic source routing) [16], and AODV (Ad hoc on demand routing algorithm) [17]. But we are trying with AOMDV (Ad hoc on demand multipath distance vector routing algorithm) [18].

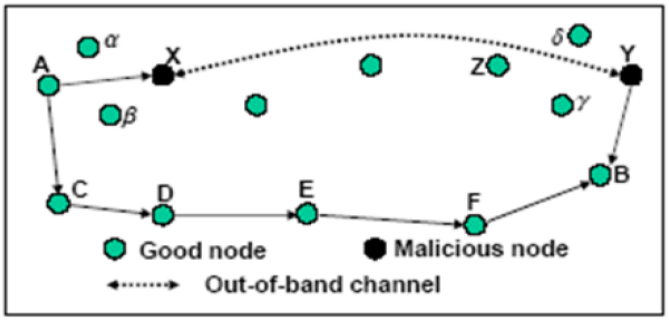

Fig.3 Wormhole Attack

AODV and AOMDV algorithms are pure on demand routing algorithms. AODV creates single path. While AOMDV creates multiple path. So we are using mechanism of AOMDV algorithm. When wormhole attack occurred, it will choose another random forwarder randomly. Then broadcast the RREQ message to random forwarder. Upon receiving RREQ message from source node, random forwarder send RREP message to source node with available reverse multiple path. If RREP message does not receive to the source in time, it means any error occur in that path and source discard that path. Upon detecting error in any link to a node, the neighbouring nodes forward route error message to all its neighbours using the link. These again initiate a route discovery process to replace the broken link. Here we only use AOMDV mechanism. In our algorithm, it checks one random forwarder at a time. If it has no error in that route then it will check another random forwarder. If any error occur between any two random forwarder then it will discard that route and find another path and randomly select the random forwarder.

III. Performance Evaluation

In this section, we provide result of LERP and also provide result with wormhole attacks. LERP provide anonymity with low cost because LERP not depend on hop-by-hop encryption and redundant traffic.

A. *The number of actual participating node:* These nodes include RFs and relay node which are taking part in communication.

B. *The number of random forwarder:* These nodes include RFs which are taking part in routing. RFs show routing anonymity.

C. *The number of remaining node in destination zone:* This is the number of nodes which is actually available in destination zone. More nodes in destination provide more anonymity for destination and prevent from wormhole attack.

D. *The number of hops per packet:* This is measure by hops count divided by, number of packet sent.

E. *Latency per packet:* This is the average between source to destination of packet routing. It includes time cost of routing.

A. The number of actual participating node:

Fig.4. demonstrates the actual participating nodes in LERP. We take 200 nodes for simulation. We see that LERP produce more actual participating nodes because its produce many route between source to destination. In LERP, more nodes in network produce more participating nodes because each routing involves more new random forwarders.

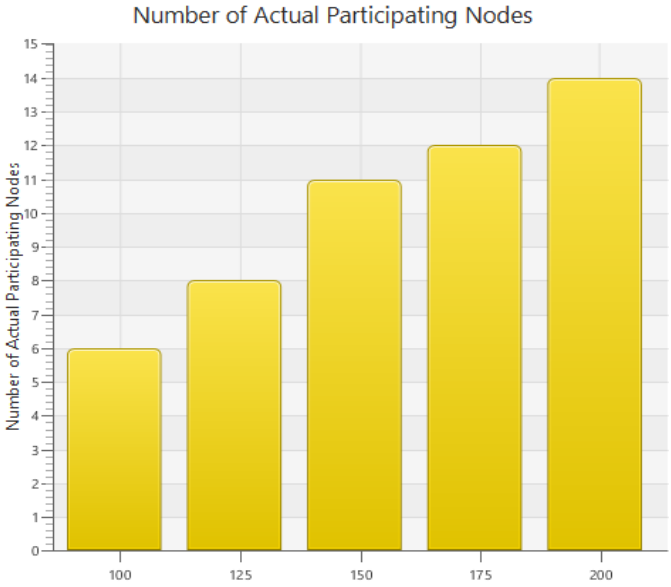

Fig.4. The number of actual participating node

B. The number of random forwarder:

Fig.5. demonstrates the number of random forwarder versus the number of partitions in LERP. It seem like higher number of partition lead to more number of random forwarders. So it will provide higher anonymity.

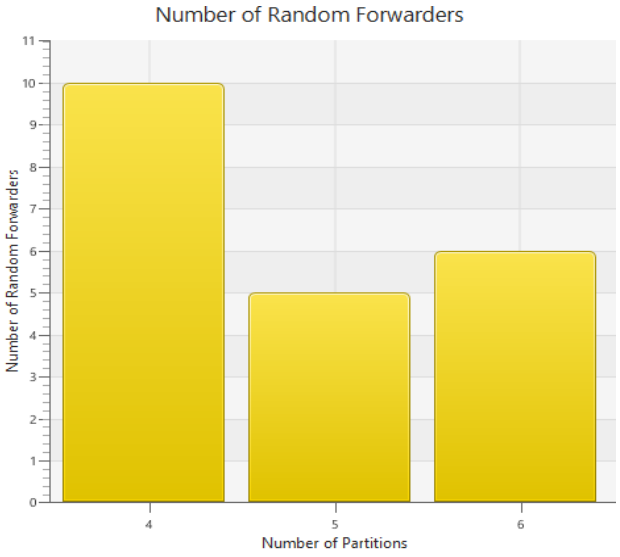

Fig.5. The Number of random forwarder

C. Destination anonymity protection:

Fig. 6 depicts the number of remaining nodes with five partitions and a 2 m/s node moving speed when the node density equals 100, 125, 150, 175 and 200, respectively. The

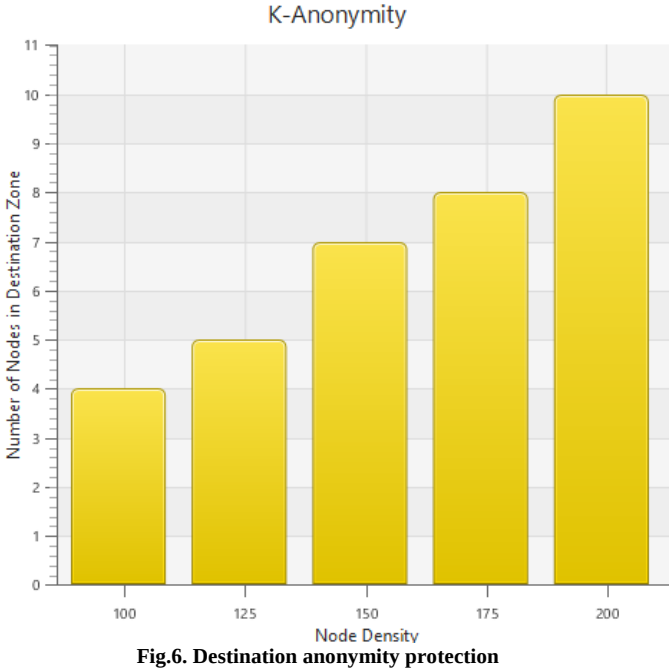

Fig.6. Destination anonymity protection

Fig.6 shows that the number of remaining nodes increases as node density grows while it decreases as time goes on. This is because higher node density leads to more nodes in the destination zone, and more nodes could remain in the destination zone after certain a time than with lower node density. Also, because of node mobility, the number of nodes that have moved out of the destination zone increases as time passes.

D. The number of hops per packet:

Fig.7. shows the average hops per packet when the moving speed of nodes is varied from 1 m/s. With wormhole attack we compare ALERT and LERP. So we got less number of hops in ALERT compare to LERP. LERP give consistent result with wormhole attacks. So LERP provide more anonymity. Here we see that ALERT has 3 or 4 hops when wormhole attack introduce while LERP has 5 hops constantly. So LERP give better result.

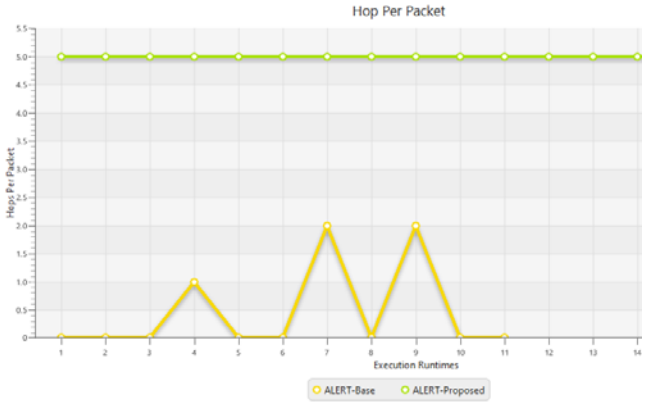

Fig.7. The number of hops per packet

If there is no location update then hops will be increase and it takes longer route. While if there is destination update, the packet will be routed to the destination following the shortest path regardless of the moving speed. LERP has slightly higher hops compare to ALERT.

F. Latency per packet:

Fig.8. present total time taken by packet to reach the source to destination by LERP and ALERT. Here we see that when wormhole attack introduce, ALERT take more time and LERP take less time. Recall that LERP is choose random forwarder for routing. ALERT uses public key encryption while LERP uses symmetric key encryption. so LERP takes shorter time than ALERT.

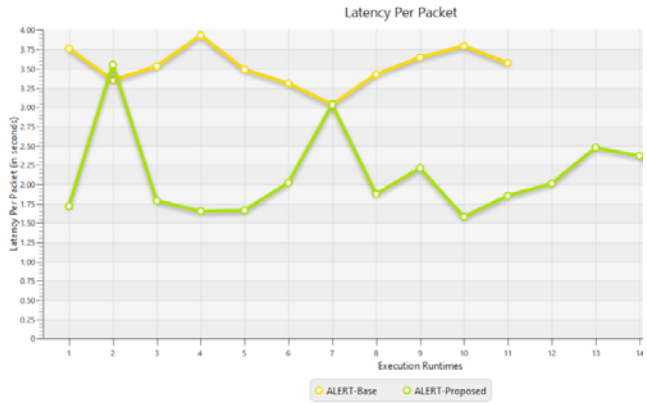

Fig.8. Latency per packet

IV. CONCLUSION

Anonymity becomes critical issue in MANETs. Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. LERP is distinguished by its low cost and anonymity protection for sources, destinations, and routes. LERP provide anonymity for source, route and destination with low cost. LERP has also ability to fight against timing attack. For making more efficient with some active attack, we introduce wormhole attack and give solution with using AOMDV algorithm technique.

ACKNOWLEDGMENT

We are thankful to our professor Prasanna Joeg, our friends who help us during our hard times when we need their assistance during thesis study and simulation.

REFERENCES

[1] Haiying Shen and Lianyu Zhao, "ALERT: An Anonymous Location Based Efficient Routing Protocol in MANETs " IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 1079-1093, June 2013.

[2] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location-Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.

[3] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware Services over VANET Using Geographical Secure Path Routing," Proc. IEEE Int'l Conf. Vehicular Electronics and safety (ICVES), 2008.

[4] X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.

[5] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf.Network Protocols (ICNP), 2008.

[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.

[7] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

[8] L. Sweeney, "k-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5, pp. Type equation here.557-570, 2002.

[9] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), pp. 10-29, 2001.

[10] Debian Administration, http://www.debian-administration.org/users/dkg/weblog/48, 2012.

[11] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proc. 32nd Int'l Conf. Very Large Databases (VLDB), 2006.

[12] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[13] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, Nov. 2008 "Analysis of wormhole Intrusion Attacks In MANETS",IEEE Military Communications Conference,MILCOM 2008.

[14] R.H. Khokhar, Md. A.Ngadi, S. Manda. "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", *International Journal of Computer Science and Security*, 2 (3), pp. 18-29, 2008.

[15] F. Natt-Abdesselam, B. Bensaou, T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Network", *IEEE Communications Magazine*, 46(4), pp. 127-133, 2008.

[16] Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks" , *In Proceedings of the International Journal of Computer Theory and Engineering, Vol. 2, No. 1* February, 2010, pp.78-86.

[17] N. Song, L. Qian, X. Li. "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach". In Proceedings of the 19th IEEE *International Parallel and Distributed Processing Symposium*, pp. 8-15, 2005.

[18] D.B. Roy, R. Chaki, N. Chaki. "A New Cluster-based Wormhole Intrusion Detection Algorithm for Mobile Ad-hoc Networks", *IJNSA*, 1 (1), pp. 44-52, 2009.