A Novel Defense IPS Scheme against Wormhole Attack in MANET

Mohini Gupta, M.Tech
Medicaps Institute of Technology & Management
Indore (MP) India

Amit Kanungo
Medicaps Institute of Science & Technology
Indore (MP) India

ABSTRACT
The security is one of the major issue in Mobile Ad hoc Network (MANET). Each node in the Ad hoc network has work as router to take part in route establishment and data delivery in between sender and destination, thus highly cooperative nodes are required to ensure that the initiated data transmission process does not fail. Worm hole attack is a type of attack that are work as to established path in between sender and receiver but if the sender has start data transmission then in that case the worm hole attacker has create a direct link, referred to as a wormhole tunnel between them, it means more of the number of trusted nodes it means higher successful data communication process rates may well expected. In this paper we proposed Intrusion detection as well as prevention technique (IPS) against wormhole attack, for detection we use routing entry base detection technique and get attacker node information like node number, number of attack packet, attack time etc. after that we prevent wormhole attack using neighbor trust worthy base technique and secure the mobile ad-hoc network communication, through our proposal we provide secure as well as reliable communication and simulate through network simulator-2 and analyze the network behavior in attack and prevention case. After that we measure the performance of network on the bases of network parameter like throughput, packet delivery ratio, overall analysis, routing load etc.

General Terms
Security, Algorithm

Keywords
MANET, routing, wormhole, IPS, ns-2

1. INTRODUCTION
Mobile Ad Hoc Network (MANET) provides quick communication among nodes (like mobile or a laptop) to transfer the packets from one node to other. An example of an ad hoc network , where nodes are communicating directly with each other. All the links between nodes are wireless. Bluetooth [1] is a typical example of such networks. These networks are independent of any fixed infrastructure or central entity like cellular networks [2] which requires fixed infrastructure to operate.

The nodes in MANET may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes. Due to this absence of authority, conventional techniques of network management and security are scarcely necessary for MANET. Any attacker or malicious node in the network can disturb the whole process or can even stop it. Several attacks like, wormhole, rushing etc [3] have been come into the picture under which a genuine node behaves in a malicious manner. It is quite difficult to define and detect such behavior of a node.

Therefore, it becomes mandatory to define the normal and malicious behavior of a node. Whenever a node exhibits a malicious behavior under any attack, it assures the breach of security principles like availability, integrity, confidentiality etc [4]. An intruder takes advantage of the vulnerabilities (which is discussed in next section) presents in the ad hoc network and attacks the node which breaches the security principles.

MANET also uses routing protocols to route the packets to its destination. Ad hoc networks routing protocols are divided into two categories: Proactive, Reactive and Hybrid [1, 3].

Proactive routing protocols are also known as “table driven” routing .In this, all the nodes store the routing information about other node present in the networks and routing updates are propagated in the network whenever network topology changes.

The advantage of proactive routing protocol is that node experiences minimal delay when route is needed and unexpired route is available in the routing table but the disadvantage of proactive routing is that these are not scalable and maintenance of routing table requires substantial network resources.

The hybrid routing protocol are the combination of both the protocols.

In the case of reactive routing protocol, route between the nodes is searched only when node wants to communicate with other node. To discover the routes they use route discovery procedure which in turns uses the flooding method. In this, initiator forwards the RREQ packet to its entire neighbor’s. If neighbor has the route for destination they reply otherwise forward the RREQ to the next node. In this way RREQ packet reaches to the destination which sends the reply to RREQ. But the method which is used to facilitate route discovery are used by the wormhole or the malicious node to consume the network resources which may lead to routing misbehavior attack.

In this paper, we propose a novel Intrusion detection as well as prevention technique (IPS) against wormhole attack which uses the AODV on demand routing protocol to reduce the effect of attack in the networks with high node mobility.

This paper is organized as follows: Section 2 covers the related work Section 3 defines research issue in field of wormhole attack behavior and their proposed solution are defined in Section 4. The simulation environment details are mentioned in section 5 and Conclusion and future work is given in Section 6.

2. RELATED WORK

Routing security in ad hoc networks is often equated with strong and feasible node authentication and lightweight cryptography. Unfortunately, the wormhole attack can hardly be defeated by crypto graphical measures, as wormhole attackers do not create separate packets. They simply replay packets already existing on the network, which pass the cryptographic checks. Existing works on wormhole detection have often focused on detection using specialized hardware, such as directional antennas, etc. In this research [5], we present a cluster based counter-measure for the wormhole attack, that alleviates these drawbacks and efficiently mitigates the wormhole attack in MANET. Simulation results on MATLab exhibit the effectiveness of the proposed algorithm in detecting wormhole attack.

In [6], wormholes are detected by considering the fact that wormhole attacks consists of relatively longer packet latency than the normal wireless propagation latency on a single hop. Since the route through wormhole seems to be shorter, many other multi-hop routes are also channeled to the wormhole leading to longer queuing delays in wormhole. The links with delays are considered to be suspicious links, since the delay may also occur due to congestion and intra-nodal processing. The OLSR protocol has been followed as the basis for routing. The approach [5] aims to detect the suspicious link and verify them in a two step process described below.

In [7], the wormhole attack is detected on multipath routing. When a source needs a new route, it will flood the network with RREQ and wait for responses. The intermediate node will forward the first RREQ packet only. The destination will wait for some time to collect all the obtained routes after receiving the first RREQ. A new scheme called Statistical Analysis of Multi-path (SAM) is proposed in [20]. SAM uses Pmax and Ø, which will be higher in the presence of wormhole attack. Here, Pmax is the maximum probability of relative frequency of a link to occur in the set of all obtained routes from one route discovery. Ø is the difference between the most frequently appeared link and the second most frequently appeared links in the set of all obtained routes from one route discovery. A probability mass function (PMF) is used to find that the highest relative frequency is more for a system under wormhole attack as compared to a normal system.

In [8] has proposed technique based on propagation speeds of requests and statistical profiling. For on demand route discovery schemes that use flooding, requests should be transmitted at a higher priority than all other packets. This implicitly increases the time to exchange information among malicious nodes. A distributed and adaptive statistical profiling technique to filter RREQs (each destination node filters RREQs that are targeted to it and have excessively large delays) or RREPs (each source node monitors the RREPs it receives and filters those that have excessively large delays) is suggested. Since different RREQs/RREPs take varying number of hops, the upper bound on the per hop time of RREQ/RREP packets is so calculated that most normal packets are retained and most falsified packets are filtered. The main advantages of this approach are that no network wide synchronized clocks are required, no additional control packet overhead is imposed and only simple computations by the sources or destinations of connections is required.

In [9] has proposed an approach that uses the anomaly in the MANET traffic behavior, particularly the behavioral anomalies in the protocol related packets for detection of worm holes. The HELLO message interval was set to 0.3 seconds, with a simple jitter function - randomly adding 0.03 seconds of delay overlaid upon it. The traffic is parsed, the HELLO messages arriving at a particular node are indexed, and the difference between arrival times of HELLO messages sent by its neighbors is calculated. The HELLO Message Timing Interval HMTI profile so obtained is used for detection of attacker nodes, as the frequency profile of HMTI is at a set frequency, a violation of OLSR protocol specifications. The interval between the packets is repeatedly much larger than it should be for a genuine node.

In [10] has proposed a set of generic mechanisms that together defend against the rushing attack: Secure neighbor detection, Secure route delegation, and Randomized ROUTE REQUEST forwarding. Secure neighbor detection allows each neighbor to verify that the other is within a given maximum transmission range. Once a node A determines that node B is a neighbor it signs a Route Delegation message, allowing node B to forward the ROUTE REQUEST. When node B determines that node A is within the allowable range, it signs an Accept Delegation message. The Randomized selection of ROUTE REQUEST message is to be forwarded, which replaces traditional duplicate suppression in on demand route discovery ensures that paths that forward REQUEST with low latency are only slightly more likely to be selected than other paths.

In [11] has defined the snare attack, and proposed ASRPAKE (An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks) and Decoy node deployment to mitigate this attack. The proposed anonymous secure routing protocol consists of five phases: the key pre-distribution phase, the neighborhood discovery phase, the route discovery phase, the route reverse phase, and the data forwarding phase. The anonymity of the VIN can further be enhanced using n no. of decoy nodes which allow the communication to be routed to the VIN only after verifying the authenticity of the source node. The main features of this approach are achievable end-to end anonymity and security, and the integration of the authenticated key exchange operations into the routing algorithm.

In [12] has identified the role of Trust in MANETs. When a network entity establishes trust in other network entities, it can predict the future behaviors of others and diagnose their security properties. Trust helps in Assistance in decision making to improve security and robustness, Adaptation to risk leading to flexible security solutions, Misbehavior detection and Quantitative assessment of system-level security properties.

In [13],[14] has done extensive work on Trust based security solutions and have proposed Fellowship, TEAM (Trust Enhanced Security Architecture for Mobile Ad-hoc Networks) SMRITI (Secure MANET Routing with Trust Intrigue). In TEAM a trust model (SMRITI) is overlaid on other security models such as key management, secure routing and cooperation model (Fellowship) to enhance security. SMRITI assists the security models in making routing decisions, corresponding to the Trust evaluation of the involved nodes. The advantage of this approach is that no special/tamper proof hardware is required and there is no requirement of a central authority as well.

3. RESEARCH ISSUES IN THE AREA

The absolute security in the mobile ad hoc network is very hard to achieve because of its fundamental characteristics, such as dynamic topology, open medium, limited range and functional resources. The main issue that occurs from attack is it consumes and modified the actual behavior of packets and due to the absence of centralized absence it is very difficult to find which node or nodes in the network creating a abnormal behavior. Each node will using the trust based routing scheme takes into account the behavior of the next node before forwarding a packet and so the total number of tunneled packets drops appreciably. It can

also be observed that at varying speeds, there are still some packets which are routed through the wormhole.

4. PROPOSED SOLUTION

Here we define algorithm for how the wormhole attack infection control to spread onto the network basically according to definition number of different way wormhole attack spread into the network name as packet encapsulation, out of band, high power transmissions and packet relay, in this algorithm we define wormhole attack on the bases of high power transmissions as well as packet relay method and define through algorithm bases very first we set normal ad-hoc network parameter and set criteria of wormhole attack scheme and spread attack onto the network and after applying IPS scheme to block the misbehaviour of attacker nodes.

Here we describe prevention scheme against wormhole attack and protect data capturing through mis-activity, in this scheme we apply entry base detection and route trust base prevention technique, for securing data communication. very first we generate normal activity entry and compare with new generated entry if not match that means our new arrival data is unsecure data and we get particular attacker node and if we found attaccaker node than we apply route trust mechanism and block the attacker node and prevent the our network communication against wormhole attack.

```
While ( S send RREQ_B)
{ rtable -> insert(rtable->rt_nexthop);
Add extra filed to rtable (next_hop , Through)  //both value 1 , 0 formate
If (new_entry == base_entry)
{
No any attack
}
ElseIf((next_hop=true)&&(through==true)&&(send_D_pkt==true) && (new_entry == base_entry))
{
True route ;
}
Else if  ((next_hop = false)&&(through == false) && (new_entry != base_entry))
{
In previous No data and route through that hop;
Insert into ->rtable; // for route to destination if shortest path
Create new Entry;
}
Elseif((next_hop = true)&&(through == false) &&(send_D_pkt==true))
{
In previous No data through that hop;
But exist in rtable entry ;

//Check reliability
if next hop(new_entry != base_entry);
{
Block that Hop ;
}
else { Send RREQ_B till the Destination }

}
Else {
Send_RREQ_B to next other hop ;
Search destination D;
}
```

The benefits of this scheme are :

The IPS scheme check the entry table of nodes that has participated in routing or effected from attacker.

IPS found that the destination node is not a neighbor of the source node then the link between them comes under misbehavior. After that detecting the misbehavior node/s.

IPS identify the unexpected increases in the path lengths that can be used as a possible the wormhole attack.

IPS obtain the routing entry information the available advertised path information, if the end-to-end path delay for a path cannot be explained by that the, existence of wormhole can be suspected.

Some of the paths may not follow the advertised false link, yet they may use some nodes involved in the wormhole attack. This will lead to an increase in hop delay due to wormhole traffic and subsequently an increase in end-to-end delay on the path. IPS find the secure path that is frre from attack

5. FURTHER FOR ATTACK SIMULATION ENVIRONMENT

The entire simulations were carried out using ns 2.31[15] network simulator which is a discrete event driven simulator developed at UC Berkeley as a part of the VINT project. The goal of NS2 is to support research and education in networking. NS2 is built using object oriented language C++ and OTcl (object oriented variant of Tool Command Language). NS2 interprets the simulation scripts written in OTcl. The user writes his simulation as an OTcl script. Some parts of NS2 are written in C++ for efficiency reasons.

A. Simulation Parameters

The simulation of normal AODV, Wormhole attack and IPS scheme are done the basis of following simulation parameters that has shown in table 5.1. These simulation parameters are decided on the basis of dynamic topology. In case of normal routing all the consider all 30 nodes but in case of wormhole attack consider 2 nodes as a attacker and remaining 28 are normal nodes and in case of IPS one node is IPS node, 2 nodes are attacker and rest of them are normal.

Table 1 Simulation parameters will uses for simulation

Simulator Used	NS-2.31
Number of nodes	50
IPS node	3
Wormhole Attacker	3
Dimension of simulated area (meters)	800 × 600
Routing Protocol	AODV
Simulation time	100 sec.
Traffic type (TCP & UDP)	FTP & CBR
Packet size	512 bytes
Number of traffic connections	5 TCP, 2 UDP
Node movement at maximum Speed	random & 20 m/s
Transmission range	250m

B. Simulation Results

Simulation results are evaluated on the basis of performance parameters like overhead, throughput etc. The simulation results are measured in case of normal AODV routing, in case of wormhole attack and after applying protection IPS scheme. Also measure the performance of TCP and UDP protocols.

1) NAM Visualization

The NAM (Network Animator) represents the number of nodes and the communication among them. 21, 22 and 4 are attacker node and 0, 28 and 48 are the IPS node. This NAM scenario is represents the number of nodes position in a simulation time is about 2.5 seconds in network. Also represents the numbers of nodes are deliver the data in network. The blue circle are represents the sensing of nodes after the data delivery is started.

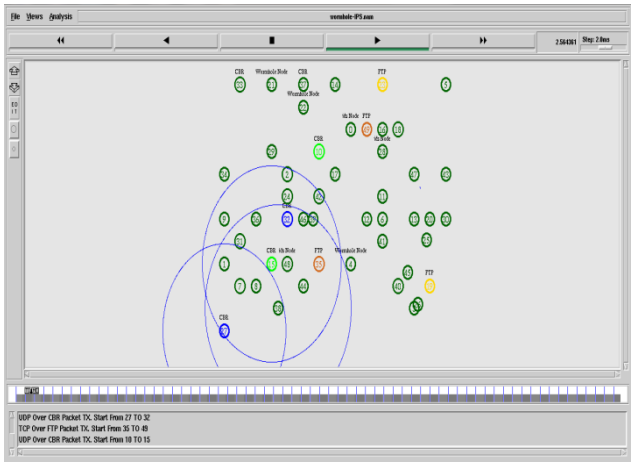

Fig. 1 Nam Scenario of nodes

2) Routing Packets Analysis in case of AODV, Wormhole attack and IPS

The routing load analysis is required to find the number of routing packets is delivering in network to established connection in between sender and receiver. The routing packets are important to know the information about the receiver. In this graph the routing load or number of routing packets in case of IPS are high almost about 4500 routing packets are deliver in network then next in case of normal routing about 7500 routing packets are deliver in network but at last the routing load in case of wormhole attack are minimum about only 1900 packets are deliver in network. The important point of normal routing is the minimum value of routing packets are show the better performance in network and this performance is determine in case of attack and the important point is that in minimum routing packets the actual data packets are deliver in network are negligible as compare to normal and IPS routing. In case IPS the routing packets are more deliver because of identifying the secure path for communication.

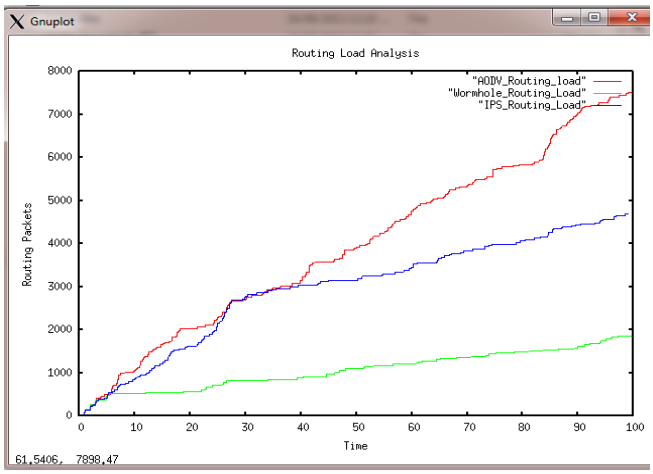

Fig.2 Routing Packets Analysis

3) PDR Analysis in case of AODV, Wormhole attack and IPS

This graph represents the Packet Delivery Ratio (PDR) analysis in case of normal AODV routing, in case of wormhole attack and in case of Intrusion Prevention System (IPS) scheme. Here the case of normal routing is only considered to match the network performance after applying protection scheme. Here we clearly visualized the effect of wormhole attack in network by that only about 10% packet delivery is possible in network at initial stage of simulation and after that the network performance are nearly zero and after about 90 second no PDF value is measure in network. But in case of after applying protection scheme i.e. IPS, the performance of network almost equal to normal means about 89% PDR are improves after applying security scheme against attack.

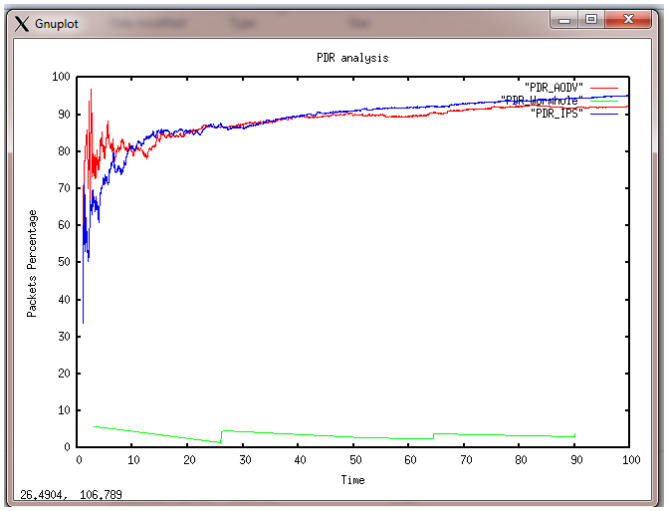

Fig. 3 PDR Analysis

4) Throughput Analysis in case of AODV, Wormhole attack and IPS

Throughput is depend on the total number of packets is send in network in per unit of time. In this graph the throughput analysis in case of normal AODV, wormhole and IPS scheme are presents. Here we notice that the in case of normal routing the throughput is about maximum 1700 packets per second in network. But in case of wormhole the throughput is negligible in network, means up to end of simulation it is about only 10 packets/ sec. but after applying IPS scheme the throughput value is increases up to 1200 packets/ sec. It means the proposed IPS scheme are definitely improves the network performance and proving the secure environment for communication.

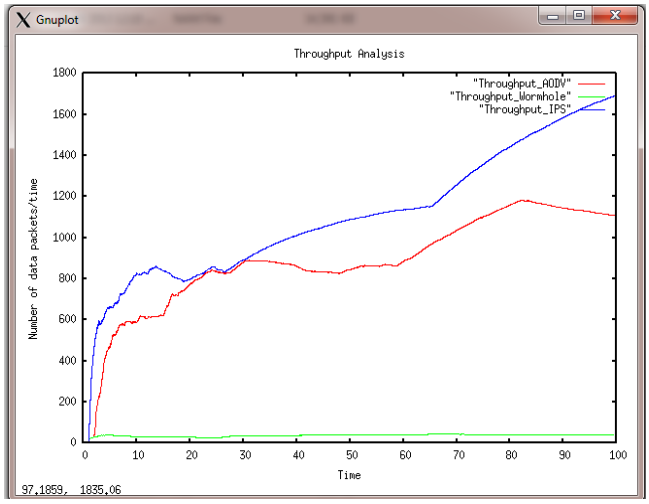

Fig.3 Throughput Analysis

5) Infection in case of Wormhole Attack

Infection percentage represents the infection percentage w.r.t time. Infection percentage in case of worm attack are continuously increases reach up to 50% and up to end of simulation the infection percentage are continuously degrades and reach to 22% infection %. At time about after 4 sec. the infection are in maximum percentage value but at the time of IPS the infection percentage is zero and not a single packet is affected by wormhole attack.IPS will block the whole activity of wormhole attack and remove the infection from network.

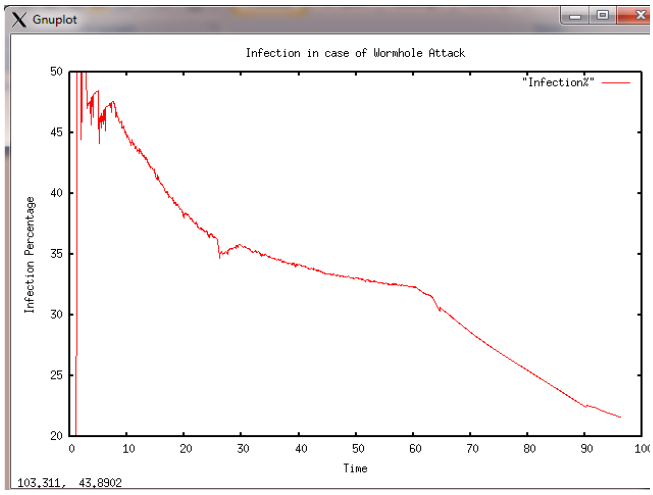

Fig. 4 Infection Analysis

6. CONCLUSION AND FUTURE WORK

In this paper, an complete simulation for MANET is done using AODV routing protocols and the effect of the presence of wormhole and IPS is also simulated. Significant performance parameters such as throughput, delay, packet delivery ratio, routing load have been considered. The study focuses on how performance is affected under wormhole attack in a network. The research here establishes the foundation for work to design IPS mechanism to identify the nodes and the links which are actively involved in the wormhole attack.

Attacker Node analysis

The attacker node analyses are measure the numbers of packets are infected by attacker node 4, 21 and 22 in network. This analysis are represents the information of attacker nodes.

Table 2 Infected Node Analysis

Infected Node	Total Infected Packets
4	122
21	210
22	29

The table 5.2 presents the summery of or actually represents the performance of normal routing, wormhole attack and IPS scheme are presented here in the foam of performance parameters.

Table 3 Overall Analyses

Parameters	AODV	Wormhole Attack	IPS
SEND =	6596.0	863.00	7349.00
RECV =	6075.0	33.00	6991.00
ROUTINGPKTS =	7560.0	1870.00	4708.00
PDF =	92.10	3.82	95.13
NRL =	1.24	56.67	0.67
No. of dropped data (packets) =	525	830	351

7. ACKNOWLEDGEMENT

I, Mohini Gupta, author of this paper would like to thank my College, Medicaps Institute of Technology & Management (situated at Indore) India (M.P.) for providing me adequate resources to make this paper. Also I would like to thank my guide Mr. Amit Kanungo for her valuable suggestions.

8. REFERENCE

[1] C.Siva Ram Murthy and B S Manoj, 'Mobile Ad Hoc Networks-Architecture and Protocols", Pearson Education, ISBN 81-317-0688-5 ,2004.

[2] Theodore S. Rappaport, "Wireless Communication" Prentice Publisher, ISBN 0133755363, January 1994.

[3] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols, Springer, 2005.

[4] Jangra1,A. Goel,N. Priyanka and Bhati,K. - Security Aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering, pp. 189-196, 2010.

[5] Debdutta Barman Roy, Rituparna Chaki and Nabendu Chaki, "A New Cluster-Based Wormhole Intrusion Detection Algorithm For Mobile Ad-Hoc Networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.

[6] John S. Baras, Svetlana Radosavac, George The odorakopoulos. "Intrusion Detection System Resiliency to Byzantine Attacks: The Case Study of Wormholes in OLSR". In *IEEE* Military Communications Conference (MILCOM), pp. 1-7, 2007.

[7] 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.

[8] X.Su, R.V.Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks," IEEE International Conference on Communications, ICC '07, pp. 1136-1141, June 2007.

[9] M.A.Gorlatova, P.C.Mason, M.Wang, L.Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," Military Communications Conference, MILCOM 2006, pp. 1-7, October 2006.

[10] Y.C.Hu, A.Perrig and D.Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego, California, pp. 30-40, Septe.