# Packet Travel Time based Mechanism for Detection and Mitigation against Wormhole Attack in AODV for MANETs

Ali Hassan, Syed Ahsan, Saleh Alshomrani, Adel Alshamrani

Faculty of Computing and Information Technology, King Abdulaziz University, North Jeddah Branch, KSA

**Abstract:** Wormhole Attack can significantly impede performance of any Mobile Ad hoc Network (MANET) by disrupting its normal routing operations. Such attack can be launched even if the network communication provides confidentiality and authenticity. Wormhole Attack usually involves two or more malicious nodes located at different physical locations which collude by disseminating incorrect routing information in order to attract data traffic to traverse through them. As result, malicious nodes have the option to drop the packets or deliver them. In this paper, an efficient algorithm has been presented for defending against wormhole attacks. The proposed mechanism is called Packet Travel Time (PTT), which enables nodes in the network to monitor how their neighbors behave and thus can detect and avoid forwarding their application traffic to go through suspected wormhole link. Simulation results have been presented to illustrate the effectiveness of the proposed algorithm. For evaluation purposes, AODV protocol has been considered as a routing protocol for MANETs.
[Ali Hassan, Syed Ahsan, Saleh Alshomrani, Adel Alshamrani. **Packet Travel Time based Mechanism for Detection and Mitigation against Wormhole Attack in AODV for MANETs.** *Life Sci J* 2014;11(10s):636-641]. (ISSN:1097-8135). http://www.lifesciencesite.com. 124

**Keywords**: Packet travel time, Wormhole attack, MANET, Ad hoc Networks

## 1. Introduction

Mobile Ad-hoc network (MANET) is formed by a collection of wireless nodes that communicate with each other without the existence of a central station to manage their communications. In MANET, there is no need for centralized base stations, access points, and servers; any participating device can route traffic in such network. MANETs have various types of applications such as military systems, natural disasters mitigation, health environmental control, emergency deployment, and video conferencing etc. [1][2][3]. For these types of application scenarios which are inherently decentralized, the ease of setting up a network, time efficient configuration and self-organization makes MANETs a suitable candidate for communication. However, decentralized nature of MANETs makes it more vulnerable to various security threats and breaches. Since both legitimate users and attackers can access wireless medium without any supervisory control, this further exacerbates security and privacy concerns.

Wormhole attack is classified as a critical security threat for MANETs. In wormhole attack, malicious nodes in the network establish a link between each other either by connecting through a high bandwidth wired link or using high powered omnidirectional antennas. Once, the wormhole link has been established, the adversary eavesdrop messages at one end, and then tunnel them to another different location in the network through the wormhole link. Packets can be tunneled by encapsulating them, using an out-of-bound high power link. During route discovery phase, they give an impression to the source that they are only one hop away from the destination and thus the path traversing through them (wormhole link) presents the most favorable route for data transmission. This result in more data traffic diverted towards this wormhole link, giving malicious nodes an option to simply drop packets [4][5].

## 2. Aodv Routing Protocol

Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol for MANETs which establishes a route from source to destination node only when required. In AODV, source initiates route discovery process by disseminating Route Request (RREQ) messages to its neighboring nodes for requesting a path to destination. Each node receiving RREQ packet first sets up a reverse route towards the source. In case it has a valid route towards destination, it replies back to the source otherwise it re-broadcasts this RREQ packet till it reaches destination [6][7]. Intermediate or destination node responds to RREQ messages by sending Route Reply (RREP) packet back to the source [8]. Therefore, on completion of route discovery phase, a single shortest path from source to destination can be found. Hello Messages are used for link maintenance and to determine neighbor connectivity. AODV routing protocol uses a destination sequence number to determine an up to date path to the destination. Each node updates its path to destination only if the destination sequence number of the received packet is greater than the last destination sequence number stored at the node [9]. In wormhole attack, malicious nodes use a high speed link, which results in RREQ packets traversing

through wormhole link reach destination faster than any other normal path. Subsequent RREQ packets arriving at the destination are simply dropped which makes AODV routing protocol vulnerable to wormhole attacks [10].

## 3. Wormwhole Attack

In the wormhole attack, two colluding nodes that are far away from each other, exchange packets via a tunnel. Each malicious node receives a RREQ packet from its neighboring nodes and sends it to its colluding malicious node at a different geographic location in the network. The second malicious node then rebroadcasts this RREQ packet to the surrounding nodes in the network [4]. When destination node receives such RREQ packet, it will believe that it has the best path available for data transmission and unintentionally realizes wormhole attack in the network [5]. In order to actuate wormhole attack, AODV control packets are tunneled by malicious nodes using one of the following methods:

**3.1. Using High Power Transmission:** In this type of attack, whenever malicious wormhole nodes receive any RREQ packet during route discovery phase, they broadcast it using maximum transmission power of their omnidirectional antennas. This increases the chance that RREQ packets going through malicious nodes reach destination nodes relatively quicker compared to alternative paths. By doing so, malicious nodes are more likely to be involved in forwarding of subsequent application packets between such source and destination [11][12].

**3.2. Using encapsulation:** In this method, malicious nodes encapsulate AODV RREQ packets and forward it towards their accomplices. One of the advantages of encapsulating the packet is that the number of hop count does not increase to include intermediate nodes. Therefore, it presents a shorter hop route compared to any others route and thus will be preferred for data transmission [11][12]. For example let's consider Fig. 1, where source node 'S' needs a shortest hop route to destination 'D' and therefore broadcasts a RREQ message. In this network there are two malicious nodes 'W1' and 'W2', which reside at different locations in the network. Node W1 captures this RREQ message received from node S and encapsulates it in a packet destined to W2 through (A, B, F, G, H). Node W2 upon receiving this RREQ packet de-capsulate it and rebroadcast it in its surrounding area.

**3.3. Using out-of-band channel:** In this method, attackers launch an attack by using long-range wired medium (an Ethernet cable or optical link), or using long – range wireless link. However, this type of attack needs special hardware capability [12] and is therefore not considered for simulation analysis in this paper.

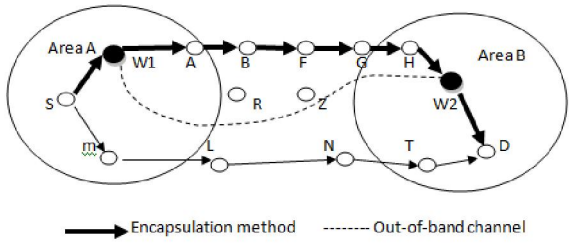


Fig. 1: wormhole through packet encapsulation and out-of-band channel.

## 4. Simulation Analysis Of Wormhole Attack In Aodv

In order to analyze the effects of wormhole attack, simulation has been carried out in OPNET™ Modeler. Each MANET station has been configured to run AODV routing protocol. In order to configure mobility profiles of mobile nodes, random waypoint model has been used. Traffic generation parameters for each MANET station have been configured to generate fixed sized IP traffic packets. For each data packet, destination nodes have been selected randomly. Standard AODV routing protocol has been modified to model the behavior of wormhole attack nodes. Table I provides the details of different network simulation parameters and table II summarizes parameters related to AODV routing protocol.

Table I: Network Simulation Parameters for Wormhole Attack

| Parameters | Values |
|---|---|
| MANET Routing Protocol | AODV |
| Simulation Time | 180 minutes |
| Geographic Space | 1000x1000 meters |
| Total Number of Nodes | 20 |
| Transmit Power (W) | 0.005 |
| Packet Inter-Arrival Time (sec) | Exponential (2.0) |
| Node Speed | 5 m/s |
| Packet Size (constant) | 1024 bits |
| MAC Protocol | IEEE 802.11 WLAN standard |
| Mobility Model | Random Waypoint |
| Wormhole attack nodes | 2 |

Table II: Parameters for AODV Routing Protocol

| Parameters | Values |
|---|---|
| Route Request Retries | 5 |
| Active Route Timeout | 3 sec. |
| Hello Interval | Uniform (1, 1.1) |
| Node Traversal Time | 0.04 sec. |
| TTL Threshold | 7 |
| Addressing Mode | IPv4 |
| Local Repair | Enabled |
| Packet Queue Size | Infinity (packets) |
| Gratuitous Route Reply Flag | Disabled |

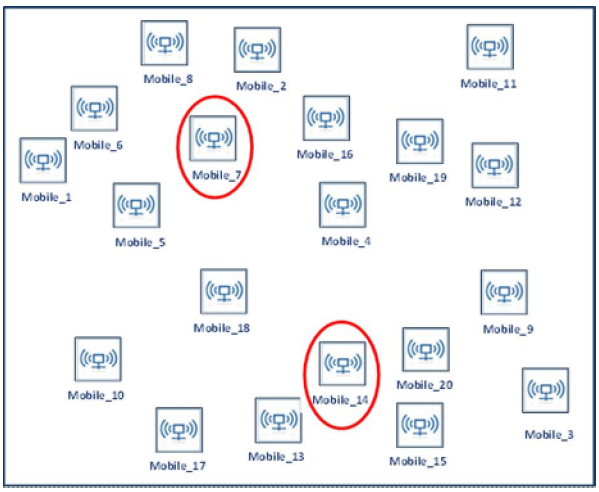


Fig. 2: Network topology of twenty nodes with two malicious nodes (Mobile_7 and Mobile_14)

Fig. 3 demonstrates how wormhole attack effects the operation of AODV routing protocol in terms of 'average number of hops per route' for all nodes in the network. In this case, during wormhole attack, malicious nodes presents preferable route for each source-destination route request by offering significantly shorter routes. All subsequent RREQ packets are discarded by the destination node as it has already chosen a better route traversing through the wormhole link. Fig. 4 augments this situation by showing that number of route replies i.e. RREP packets increase significantly when AODV is under wormhole attack. As a result, more and more data traffic will be attracted to pass through malicious wormhole attack nodes. Fig. 5 clearly shows that malicious nodes in the network (Node 7 & 14) receive significantly large number of application packets compared to other nodes in the network. This gives them a choice to either simply drop the data packet or forward it normally. This situation can clearly pose serious security and privacy threats like Denial of Service (DoS) attack.

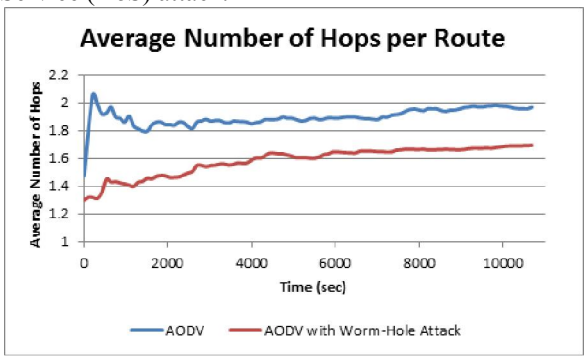


Fig. 3: Comparison between AODV routing protocol & AODV under Wormhole attack in terms of 'average number of hops per route' for all nodes in the network

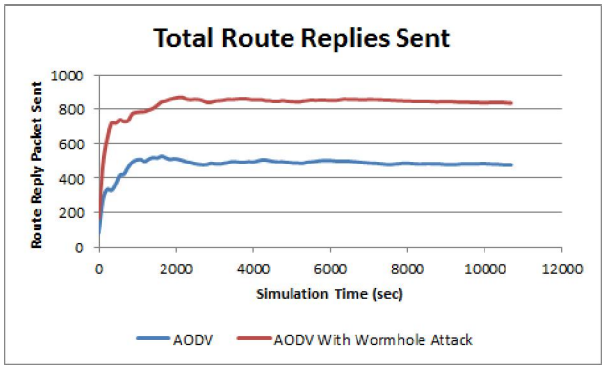


Fig. 4: Comparison between AODV & AODV under Wormhole attack in terms of 'total route replies' (RREP packets) sent by all nodes in the network

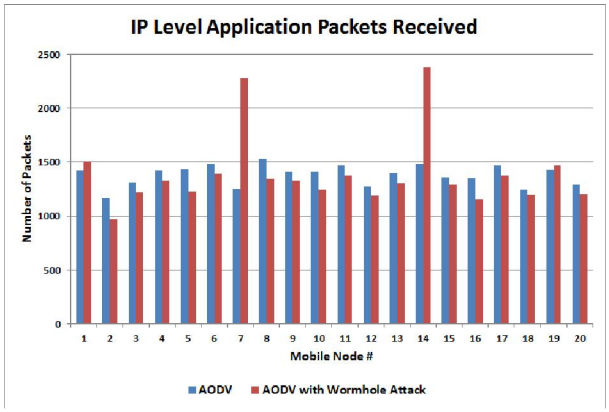


Fig. 5: Comparison between AODV & AODV under Wormhole attack in terms of 'number of application packets processed' by each node in the network

## 5. Packet-Travel-Time Wormhole Attack Mitigation Algorithm

### 5.1. The PTT Algorithm

The mechanism proposed in this paper is called Packet Travel Time (PTT) algorithm where nodes are assumed to have their network interfaces in the promiscuous reception mode, and network links operate bi-directionally. Each node sends a RREQ message to find a path to a destination, and each intermediate node either replies with RREP message or rebroadcast the received RREQ message to its neighbors. Once the RREQ reaches its destination, the destination sends the RREP message through the reverse route. Each node in the network broadcasting RREQ message, records RREQ sending time ($t_s$) and the time when it hears its neighbor rebroadcasting the packet ($t_h$). It then calculates the Packet Travel Time using equation 1 and save it till it receives corresponding RREP packet.

$$PTT = t_h - t_s \quad (1)$$

Once RREP packet is received for this particular source-destination path request, it appends this PTT value in a special field of RREP packet created by the

destination node. Each node also records the RREP receiving time ($t_r$), and send these two values back to the source. RTT between each two successive nodes is computed by the source using equation 2.

$$RTT = t_r - t_s \quad (2)$$

PTT and RTT values enable the source node to identify link with highest RTT value to be considered as a wormhole link. Each node in the network can now monitor its next successive neighbor and can evaluate its behavior while broadcasting the RREQ messages in the network.

In table III, we can note that the RREQ overhearing time ($t_h$) at any node (i) is equal to the RREQ sending time ($t_s$) at its next hop neighboring node (j). Thus, the equivalence of both results suggests that the recorded values are correct. Subsequently, the source can make a decision in case any node records a fake value. For example, as shown in Table III, the RREQ sending time at node A is 2 and the value of PTT at the same node (A) is 5.5. Using these values, node A can calculate value '$N_{ht}$' (equation 3), to determine whether its next node neighbor has recorded an incorrect RREQ sending time or not.

$$N_{ht} = PTT + t_s \quad (3)$$

'$N_{ht}$' here is the calculated RREQ sending time at the next neighboring node. Any malicious node now becomes incapable to record and send incorrect RREQ sending time values as they are being monitored by other nodes in the network.

Table III: Values of RREQ-sending-overhearing times, RREP-receiving time, RTT, and PTT of an example network shown in Fig. 1.

| | RREQ Sending Time ($t_s$) | RREP Receiving Time ($t_r$) | RREQ Overhearing Time ($t_h$) | PTT Packet Travel Time | RTT Round Trip Time | Note |
|---|---|---|---|---|---|---|
| Node S | 0 | 37 | 2 | 2 | 37 | PTT = RREQ hearing time – RREQ sending time ($t_h - t_s$). RTT = RREP receiving time – RREQ sending time ($t_r - t_s$). |
| Node A | 2 | 35 | 7.5 | 5.5 | 33 | |
| Node W1 | 7.5 | 33 | 13 | 5.5 | 25.5 | |
| Node W2 | 13 | 27 | 15 | 2 | 14 | |
| Node B | 15 | 22 | 17 | 2 | 7 | |
| Node C | 17 | 20 | *** | | 3 | |

### 5.2. Packet Forwarding Delay Attack and Proposed POD Mechanism

To improve effectiveness of the proposed mechanism, another serious threat i.e. the ability of malicious nodes to delay sending both the RREQ and the RREP messages, needs to be tackled. When malicious nodes use this delaying tactic, source node are unable to pinpoint the wormhole link as it could have more than one RTT values greater than average RTT values. For example consider the following RTT values between each two successive nodes:

$RTT_{S, A} = 32.5 - 29.5 = 4$

$RTT_{A, W1} = 29.5 - 23 = 7.5$

$RTT_{W1, W2} = 23 - 12.5 = 11.5$

$RTT_{W2, B} = 12.5 - 6 = 7$

$RTT_{B, C} = 6 - 3 = 4$

In this case, three links become incorrectly suspect of being wormhole links i.e. A→W1, W1→W2 and B→W2. Links between node A and W1 and between node B and node W2 are not wormhole links but the source would consider them as wormhole links. The cause of this confusion is the delaying tactic used by node W1 and W2 by delayed forwarding of RREQ and RREP respectively to their next hop neighbors.

The proposed scheme incorporates Prevention of Delay (POD) mechanism by using a special POD - Neighboring Node Table (referred from here onwards as $POD_{NNT}$). Since all nodes have their network interfaces in the promiscuous mode, any node sending/forwarding a RREQ packet records its RREQ sending time and starts up a timer count. If the RREQ overhearing time ($t_h$) of its next hop neighbor is within permissible time, it assigns a positive value in its $POD_{NNT}$ (table IV). However, if the next hop neighbor does not broadcast previously forwarded/sent RREQ packet within an allowed time for three consecutive occurrences, it is marked as a suspected malicious node employing delaying tactic. The current node records a negative value for this next hop neighboring node in $POD_{NNT}$ and informs other nodes in the network by broadcasting $POD_{NNT}$ to all other nodes in the network. In order to reduce control overhead, $POD_{NNT}$ is disseminated in the network only when a negative value is assigned for any node. Fig. 6 and 7 illustrate how a malicious wormhole attack node X delays forwarding RREQ packet and how node A notices this delaying tactic. In this case, node A must perform the following sequence of steps:

1. Resend RREQ packet to node X up to a maximum of three.
2. After three attempts, if X does not rebroadcast RREQ packet, assign a negative value for X in its $POD_{NNT}$.
3. Broadcast PODNNT neighboring node table to other nodes in the network.

Public-private key encryption has been employed to secure transmission and delivery of information contained in $POD_{NNT}$ and to avoid an alteration by any malicious node [13][14].

Table IV: POD - Neighboring Node Table ($POD_{NNT}$)

| RREQ sequence number | Neighbour ID | Count value |
|---|---|---|
| | | +ve/-ve Integer |

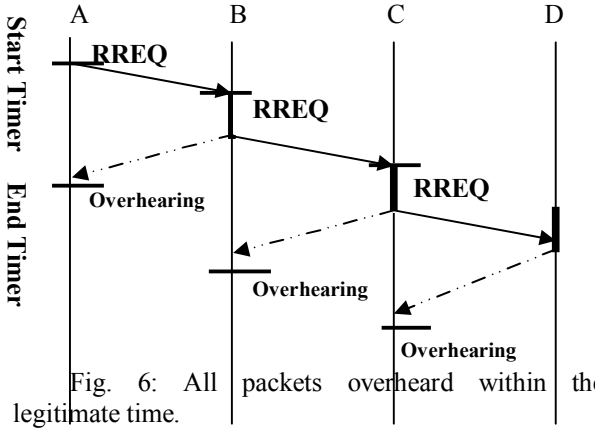


Fig. 6: All packets overheard within the legitimate time.

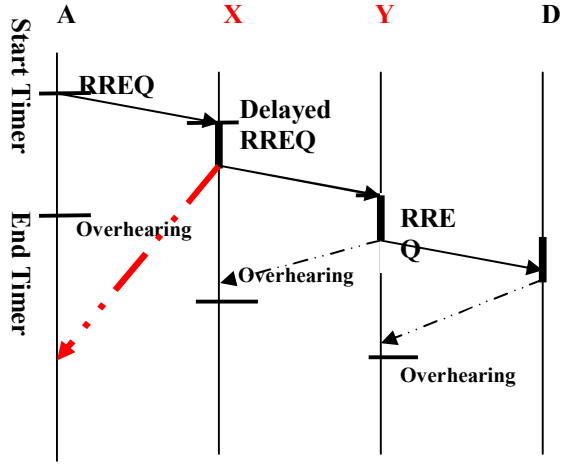


Fig. 7: An intended delay of the RREQ done by node X which is a wormhole malicious node.

### 5.3. Performance Evaluation

Performance evaluation of PTT algorithm for the network topology presented in Fig. 2 has been carried out in OPNET™ Modeler. Mobile station number 7 and 14 has been configured to launch wormhole attack in the network. Same network simulation and AODV routing protocol parameters have been considered as presented in section IV.

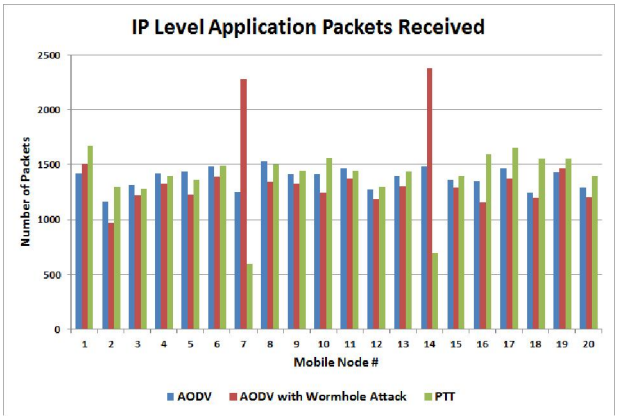


Fig. 8: Performance comparison between AODV, AODV under Wormhole attack and PTT algorithm, in terms of 'number of application packets processed' by each node in the network

RREP packet format in AODV process model has been modified to create a special field to store PTT values. A new packet format has been defined in OPNET"s packet editor to carry encrypted information contained in PODNNT. IP level application packet size has been kept constant at 1024 bits. Each node is configured to use random waypoint mobility model having a speed of 5 m/sec. MANET mobile stations use IEEE 802.11 WLAN standard for MAC protocol. Destination nodes for the packets are chosen randomly using uniform distribution.

Performance comparison of PTT algorithm in terms of number of application packets processed by each node in the network has been presented in Fig. 8. In this experiment, malicious node has been configured to generate its own IP level application traffic. This figure evidently shows that malicious nodes launching wormhole attack in the network (Node 7 & 14) receive significantly large number of application packets compared to other nodes when standard AODV routing protocol is employed. This situation can clearly pose serious security and privacy threats like Denial of Service (DoS) attack. However, when PTT algorithm is employed, normal nodes in the network are able to detect such malicious nodes and avoid using them for forwarding packets towards the destination. This reduces the capacity of malicious nodes to drop application packets of other nodes.

## 6. Conclusion

In this paper PTT algorithm has been proposed as a potential solution to mitigate wormhole attack. Simulation analysis of wormhole attack has been carried out by modifying standard AODV routing

protocol in OPNET™ Modeler. In the proposed PTT algorithm, network nodes observe behavior of their neighboring nodes by overhearing their broadcast of RREQ packets. Prevention of Delay (POD) mechanism has been incorporated to identify malicious nodes using delaying tactics of postponing forwarding of RREQ and RREP packets. Public key encryption has been used to secure contents of PODNNT before dissemination throughout the network. The proposed scheme reduces the chances of malicious nodes to drop data packets destined for other nodes in the network and adversely effecting average throughput in the network. Simulation results are encouraging and show that PTT algorithm significantly reduces the number of application packets traversing through wormhole attack nodes.

**References**


1. J. Sun, “Mobile ad hoc networking: an essential technology for pervasive computing”, in Proc. Int. Conf on Info-tech & Info-net, Beijing, China, 2011, pp. 316-321.
2. Norman A. Benjamin, Suresh Sankaranarayan. “Performance of Wireless Body Sensor based Mesh Network for Health Application”, International Journal of Computer Information Systems and Industrial Management Applications, 2, pp. 20-28, 2010.
3. Masayuki Nakamura, Atsushi Sakurai, Jiro Nakamura. “Autonomic Wireless Sensor/Actuator Networks for Tracking Environment Control Behaviors”, international Journal of Computer Information Systems and Industrial Management Applications, 1, pp. 125-132, 2009.
4. Hon Sun Chiu King-Shan Lui, DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks, International Symposium on Wireless Pervasive Computing ISWPC, 2006.
5. Alshamrani, “PTT: Packet travel time algorithm in mobile ad hoc networks,” in Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference, March 2011, pp. 561 – 568.
6. D.B.Johnson and D.A. Maltz, “Dynamic Source Routing in Adhoc wireless networking”, Mobile computing, kluwer Academic publishers, vol. 353, pp. 153-181, 1996.
7. Z.J.Haas “The Routing Algorithm for the Reconfigurable Wireless Networks”, Proceedings of ICUPC 1997, vol. 2, pp 56/- 566, October 1997.
8. Mohammed Saeed Alkatheiri, Jianwei Liu and Abdur Rashid Sangi, "AODV Routing Protocol Under Several Routing Attacks in MANETs" IEEE 978-1-61284-307-0/11/2011.
9. Asma Tuteja, Sunil Thalia, Rajneesh Gujral, “Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2” in ACE 2010, 21- 22 June 2010, pp. 330-333.
10. 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.
11. V. Mahajan, M. Natu, A. Sethi. “Analysis of wormhole intrusion attacks in MANETS”. In IEEE Military Communications Conference (MILCOM), pp. 1-7, 2008.
12. Marianne Azer et al., ”A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in wireless Ad Hoc Networks”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 1, No.1, May 2009.
13. Shamir, "How to share a secret," Communication of the ACM, vol. 22, pp. 612–613, 1979.
14. L. Zhou and Z.J. Haas. "Securing Ad Hoc Networks." IEEE Network Magazine, vol. 13, no.6, Nov./Dec. 1999.


10/15/2014