ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

LITERATURE SURVEY ON WORMHOLE ATTACK

Avinash S. Bundela
Computer Science & EngineeringMedicaps Institute of Technology and Management, Indore (M. P.), India

ABSTRACT
Security plays an important role in Mobile Ad Hoc Network when data transmission is performed within un-trusted wireless scenario. Various attacks like Black hole, Wormhole, Gray hole and many more have been identified & corresponding solutions have been proposed. These attacks are caused by the malicious node hence ad hoc wireless network is unprotected from the attacks of the malicious node. Between all these attacks the wormhole attack is harmful attack in which two or more malicious nodes create a virtual tunnel in the network. Two types of wormhole attacks have been recognized: Hidden attack and Exposed attack. Many detection techniques are proposed by the researchers for both types of wormhole attacks.

KEYWORDS: MANET, Routing, Security Attacks, wormhole.

INTRODUCTION
Wireless Mobile ad hoc network is an infrastructure less network & dynamic in nature. Infrastructure network does not have any fixed infrastructure for the communication. Nodes in such type of network can communicate directly with other nodes in the network & there is no requirement of any centralized network access point. A primary thing about these types of networks is that these networks do not have any routers but the wireless nodes work as a routers and a host. These types of networks don't have any fixed or static topology [1] [2].

A mobile ad hoc network consists of mobile nodes that use wireless transmission for communication. The nodes are movable and the motion of nodes may be random or periodical in mobile ad hoc network [3]. Due to node mobility, the nodes have limited battery power & limited bandwidth. The source & destination communicate through multiple hops in absence of centralized access point or administrator [2]. The MANET is also called a multi hop wireless network. An Ad-Hoc network is an autonomous collection of mobile nodes or users [4].

SECURITY ISSUES
Wireless Mobile Ad hoc networks are vulnerable to various attacks not only from outside attack but also from inside attacks (attacks within the network itself). Two different levels of attacks are discussed in Ad hoc network [5].
First level – based on the mechanisms of the ad hoc network called routing.
Second level – based on to damage the security mechanisms employed in the network [6].
The security attacks in MANETs are divided into two major types.

Passive attacks
The attacker does not have permission to alter the data when data transmitted within the network in passive attack, but attacker listen the network traffic. Passive attacker does not disrupt in the network but it attempts to find out important information from network traffic. It is very inconvenient to detect passive attack because passive attacker only listen the network traffic and it does not make any harm in the data. The real solution to control such type of attacks is that user can use encryption algorithms for data encryption [7].

Active Attacks
Active attacks are very harmful attacks on the network. An attacker makes unauthorized access on data as well as makes changes such as modification of packets, DoS, congestion etc. in the data when data transmitted in the network. There are two types of active attack:
Active external attacks: this type of attack is performed by outsider source which do not belong to network.
Active internal attacks: this type of attack is performed by malicious nodes which belong to network [7].

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

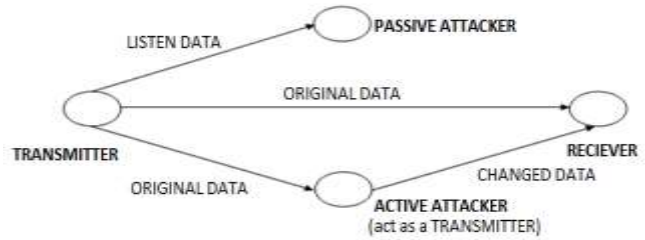

Figure 1: Active and Passive Attacks in MANET

Generally active attacks are classified into four major groups:

Dropping Attack

When source node has a packet for destination node then it selects one of the route for sending packet. The route has selfish node which silently drop all packets and do not forward packets towards destination node .Due to this dropping attacks can stop end-to-end communications.

Modification Attack

The malicious nodes modify the packet and due to this it disrupts the whole communication between nodes. The best example for modification attack is Sinkhole attack.

Fabrication Attack

The attacker node send fake message to all its neighbors' nodes without receiving any related message. When neighbors node requests for route to destination then the attacker node can also send fake route reply message to all its neighbors.

Timing Attack

The attackers attract other nodes by advertising itself as a node closer to the destination node.

BACKGROUND

Each node takes part in route decision to forward the packet in MANET, so it is very easy for malicious nodes to attack on MANET. The attackers inject itself in the active path from source to destination and also analyze the traffic flows between source nodes to destination node and harm the network operations in network layer attacks. There are several network layer attacks performed by malicious nodes. Some network layer attacks are discussed below:

Blackhole Attack

Blackhole attack, shown in Figure 2, is also called packet drop attack or it is a type of denial-of-service attack. Blackhole define as a place in the network where all incoming traffic is silently dropped by malicious node, without informing to the source node. This attack affects the packet delivery between nodes and also reduces the routing information available to the other nodes [8].

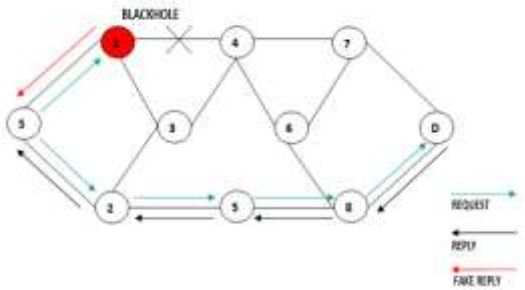

Figure 2: Blackhole Attack

Rushing Attack

This type of attack corrupts the route discovery process. When source node has data to transmit then it performs route discovery process from source to destination. The source node broadcasts RREQ packet which travels through many intermediate nodes to find optimal route and when RREQ packet received by malicious node, it increases the transmission speed of RREQ packet by which packet forwarded by malicious node reaches first to destination node

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

as compare to other nodes. At the same time malicious node store the copy of forwarded packet for future use and frequently forward copied packet to destination node by which destination node will be busy in receiving packet from malicious node. Figure 3 shows the rushing attack in the network in which S and D are source and destination nodes respectively, and node 4 is the attacker node called malicious node. Malicious node quickly broadcast the RREQ packet to ensure destination node that RREQ packet from itself arrive earlier as compare to other node [9].

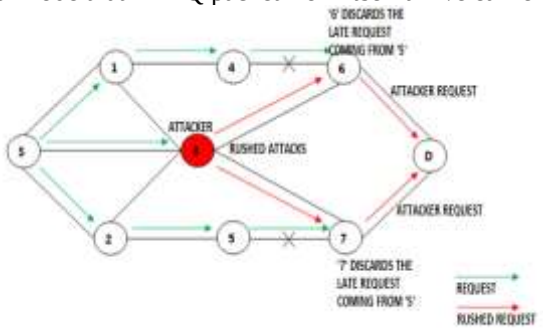

Figure 3: Rushing Attack

Wormhole Attack

Malicious node receive packet at one location in the network and tunnels them to another malicious node at another location in wormhole attack. The tunnel occurs between two malicious nodes is called wormhole. Attackers use wormholes in the MANET to make their nodes appear more attractive so that more traffic flow through their nodes. Figure 4 shows the wormhole attack in the network in which nodes 2 and 7 are malicious nodes respectively that form the tunnel in MANET. The source node S initiates the RREQ packet to find the route to destination node D. The source node S forwards the RREQ packet to their respective neighbors 1 and 2. The node 2 receives the RREQ packet and immediately shares it with node 7 and later node 7 initiate RREQ to its neighbor node D, through which the RREQ packet is delivered to the destination node D. The problem of high speed link forces the source node to select route <S-2-7-D> for destination. Node D ignores RREQ that arrives at a later time and therefore invalidates the legitimate route <S-1-4-6-D> [10][11][12][13].

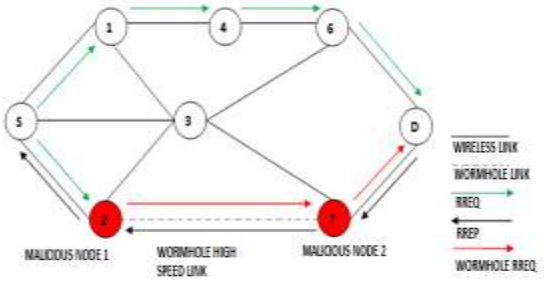

Figure 4: Wormhole Attack

Sinkhole Attack

A malicious node advertises wrong routing information to produce itself as a specific node and receives whole network traffic in sinkhole Attack. When malicious node receives entire network traffic then it modifies the secret information, such as changes made in data packets or discards data packets to make the network complicated. A malicious node tries to collect all secure data from all its neighbor nodes. The Sinkhole attack affects the performance of MANET protocols and the path presented through the malicious node appears to be the best available route for the nodes to communicate. Figure below shows the sinkhole attack [5].

Replay Attack

A malicious node records the control messages of other nodes in replay attack and resends them later when needed. A replay attack is a form of network attack in which a valid data transmission is maliciously repeated or delayed. This can be done by malicious nodes. These replay attacks are later misused to disturb the routing operation in a MANET [5].

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

Resource Consumption Attack
A malicious node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets in resource consumption attack. This type of attack is also called sleep deprivation attack.

WORMHOLE ATTACK IN MANET

Ad hoc networks are vulnerable to many attacks due to many reasons such as wireless links between nodes, deficiency in infrastructure, absence of centralized monitor or management, limited physical Protection, and the resource constraints. A particularly security attack which is called the wormhole attack, has been introduced in the ad-hoc networks [11] [12] [13]. A malicious node captures packets from one location in the network and tunnels the captured packets to another malicious node at another location as shown in the Figure 5, which replays them locally.

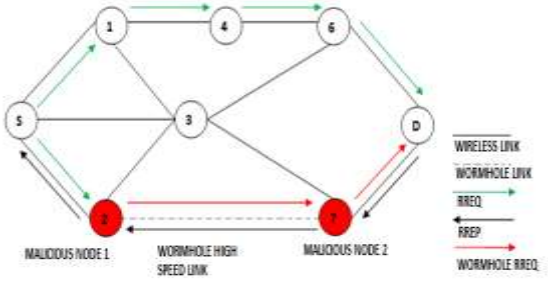

Figure 5: Wormhole Attack in Ad Hoc Network

Wormhole Attack Classification
Two attackers work together in a wormhole attack, one attacker receives the packets at one location in the network and tunnels the packets to its companion attacker at another location in the network. After that the companion attacker replays packets into the network. Two types of wormhole attacks have been identified. Malicious nodes, in the first type of attack called hidden attack, hide the fact that they forward a packet, meaning that, legitimate nodes do not know their participation in packet forwarding. Legitimate nodes, in the second type of attack called exposed attack, are aware of the fact that the malicious nodes are forwarding packets; just do not know they are malicious [11] [14] [15].

Hidden wormhole Attack
The attackers do not modify the content of the packet and the packet header, even the packet is an AODV advertisement packet, but they simply tunnel the packet from one point and reply it at another point. The sender treat the receiver as its immediate neighbour in this type of attack [15]. As shown in Figure 6 the packet from source node S is received by malicious node M1, M1 tunnels the packets to other malicious node M2 and replies them to receiver R, without modifying the packet header. As M1 and M2 do not include themselves in the header, than R can observe that the previous hop is S. The same observation can be done in the reverse path, and S finds R as its immediate neighbour, so the path found is {S, R}.This is undoubtedly not correct since S and R are Separated by node M1, node M2 and other node that are in the tunnel.

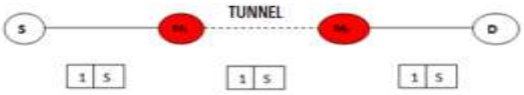

Figure 6: Hidden Wormhole Attack

Exposed Wormhole Attack
The attackers do not modify the content of the packet in this type of attack, but include themselves in the packet header following the route setup procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbours. Consider the situation where source node S wants to establish a route to receiver node R. As shown in Figure 7, malicious node M1 receives the packet from source node S, it modifies the pervious hop field to M1 and increases the hop count by 1. Then the RREQ packet is tunnelled to other malicious node M2 and M2 performs the same procedure and broadcasts the RREQ packet to receiver R. Receiver R finds its previous hop is M2 with hop count equals to 3. The same thing happens in the reverse path. When S receives the RREP packet, it finds its pervious hop is M1 with hop count equals to 3. And the route establishes as {S, Ml, M2, R} [15].

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

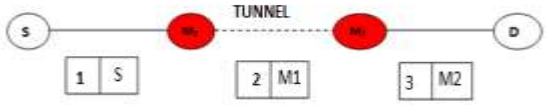

Figure 7: Exposed Wormhole Attack

Wormhole Attack Modes

There are four wormhole attacks mode in ad hoc network [11] [14].

Wormhole Using Encapsulation

A malicious (first Party) node hears the RREQ packet at one location in the network and tunnels it to another malicious (Second party) node at another location near the destination in this type of mode. The second party again rebroadcasts the RREQ packet. The neighbours of the second party receive the RREQ packet and drop any further legitimate requests that may arrive later on legitimate multi hop paths. Then the result is that the routes between the source and the destination go through the two malicious nodes that will be formed a wormhole between them. For example, consider Figure. 8, which shows Wormhole attack through Packet Encapsulation [13].

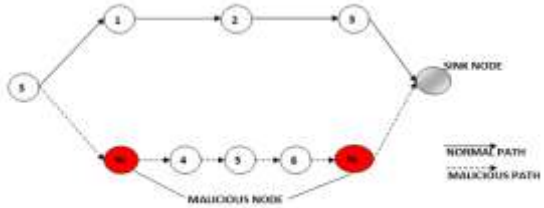

Figure 8: Wormhole Attack through Packet Encapsulation

Wormhole Using Out-of-Band Channel

Out of Band Channel can be achieved by using a long range directional wireless link or a direct wired link as shown in Figure 9. As compare to previous attack it is difficult to launch such mode of attack because it needs specialized hardware capability [13].

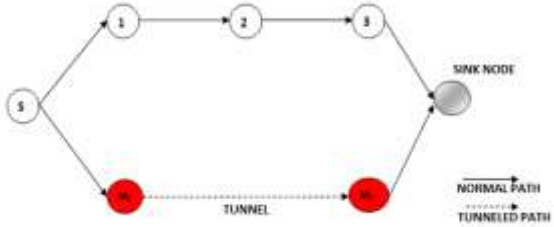

Figure 9: Wormhole Attack through Out-of-Band Channel

Wormhole With High Power Transmission

When a single malicious node gets a RREQ, malicious node broadcasts the RREQ at a high power level so the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a another malicious node as compare to another nodes because other node does not have such high power level as shown in the Figure 10.

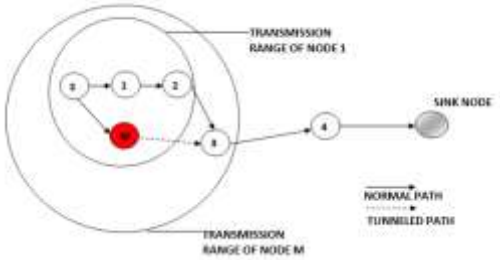

Figure 10: Wormhole Attack through High Power Transmission

Wormhole Using Packet Relay

Another mode of wormhole attack is packet relay in which two malicious nodes relay packet between two nodes

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

which are far apart from each other and convenience these nodes that they are neighbor.

RELATED WORK

A. Y. C. Hu, A. Perrig and D. B. Johnson [16] proposed a detection and prevention method in which there are basically two types of packet leashes:

1. Geographical Leashes
2. Temporal Leashes

Leash is nothing but the type of information that is added to a packet designed to restrict the packets maximum allowed transmission distance.

Geographical Leashes: The recipient of the packet is lie within a certain distance from the sender of the packet in Geographical Leashes. For construction of geographical leash, each and every node must know its own location and all nodes must have clocks which are loosely synchronized. The use of geographical leash is defined as, when a sending node send a packet, it include its own location (ps) and the time at which it send a packet (ts). When receiver node of the packet receives the packet it compares the values (ps and ts) to its own location (pr) and the time at which it received the packet (tr). If the clocks of sender and receiver are synchronized to within ± Δ, and ν is an upper bound on the velocity of any node, then at receiver end, the receiver can compute an upper bound on distance between sender and itself (receiver), dsr. Which is based on the timestamp ts (sending time of packet), tr (time at which packet is received), □ (maximum relative error in location information), ps (location of sender node) and pr (location of receiver node).

$dsr \leq \| ps - pr \| + 2\nu.(tr - ts + \Delta) + \square$

Any authentication technique like digital signature can be used to allow a receiver to authenticate the location and timestamp in the receiver packet.

Temporal Leash: The packet has an upper bound on its lifetime, by which a packet is restricted to travel maximum distance, since the packet can travel at most at the speed of light in temporal leash. For construction of temporal leash, all nodes must have clocks which are tightly synchronized. The maximum difference between any two nodes clocks is Δ. The value of the parameter Δ must be known by all nodes in the network. For temporal leashes the value of Δ must be on the order of few microseconds or even hundreds of nanoseconds. The level of time synchronization can be achieved by hardware such as LORAN-C, WWVB, GPS etc. Some other hardware such as cesium-beam clocks, rubidium clocks and hydrogen maser clocks are also be used for sufficiently accurate time synchronization for months. Use of temporal leash, when a sending node send a packet, it includes the time at which it send the packet, t_s. When receiver of packet receives the packet, the receiving node compares this value (t_s) to the time at which receiver node receives packet, t_r. At the receiver end the receiver is able to detect, if the packet traveled to far, based on clamed transmission time and the speed of light.

Advantage of geographical leashes over the temporal leashes is that the time synchronization is looser and another advantage is that geographical leashes uses the concept of digital signature scheme for successful secure delivery of packet at receiver end.

L. Hu and D. Evans [17] proposed a detection and prevention method in which Directional antenna system are used in ad hoc network for increasing the capacity and connectivity of ad hoc networks. Transmission of packet in particular direction gives a higher degree of spatial reuse of the shared medium. Directional antenna transmission system uses energy more efficiently. As compare to omnidirectional antenna, the transmission range of directional antennas is usually larger; which can reduce the number of hops in routing. Using directional antennas can increase spatial reuse and reduce packet collision and negative effect such as deafness. The directional antenna model assumes an antenna with N zones. Each and every zone has a conical shape or conical radiation pattern, spanning an angle of 2□/N radians. The model zones are fixed and non overlapping beam direction pattern; so that the N zones may collectively cover the whole plane.

When a node is idle, in this condition the node listens the carrier in omni mode. When idle node receives a message, it determine the zone on which the received signal power in maximal and the node uses that zone to communicate with sender. Directional antenna approach follows three steps: first step is Directional Neighbors Discovery, second is to Verified Neighbor Discovery and finally Strict Neighbor Discovery will be performed.

Wormhole attack is one of the serious attacks which form a serious threat in the wireless networks, mainly against many ad hoc wireless routing protocols and location- based wireless security systems. H. S. Chiu and K. S. Lui [15] proposed a detection method called Delay per Hop Indication (DelPHI). The sender is able to detect both kinds of wormhole attacks by observing the delays of different paths to the receiver. This method requires neither

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

synchronized clocks nor special hardware equipped mobile nodes. The performance of the DelPHI has been examined by simulations. The result of simulation shows that DelPHI has achieve higher than 95% in detecting normal path and 90% in detecting wormhole attack, in the absence of background traffic. Simulations has also shown that DelPHI can maintain above 85% detection rate for both normal and tunnelled paths given that there is background traffic. The message overhead of DelPHI has also been addressed in this paper.

T. V. Phuong, N. T. Canh, Y. K. Lee, S. Lee, and H. Lee [18] proposed a detection and prevention method called Transmission Time Mechanism (TTM) for MANET in which, source node establishes a route to another node called destination. This method checks whether there is a wormhole link in the route or not by calculating round trip time between two successive nodes along the route. Each and every node in the established route computes the Round Trip Time (RTT) between it and the destination and then sends these values back to the source node. The source node collects all these RTT values from different routes and calculates RTT's between two successive nodes of different routes and identify wormhole attack based on the fact that the RTT between two malicious or FAKE neighbors will be considerably higher than the two real neighbors.

A. S. Alshamrani [19] proposed a detection and prevention method called Packet Travel Time (PTT) algorithm for MANET. This mechanism initially uses the same process of calculating the RTT's which are used in transmission time mechanism (TTM) between two successive nodes. Furthermore it monitors all the transmitted packets in the network. After forwarding the RREQ packet, each node records the sending time (t_s) and save sending time (t_s) values in memory and the time when it overhears its neighbor rebroadcast the RREQ packet (t_h). Further each node calculate the PTT value ($PTT=t_h-t_s$) and each node save the PTT value until it receives the RREP and append PTT value in the special part which is created by the destination. When source node receives the RREP, it calculates the RTT between every two successive nodes by the same process that has been discussed in TTM and then these values has compared with the values of PTT's and find if there is any wormhole link in the route. Table I shows the sending and receiving time values of all nodes received by source node and the calculation done by the source node.

Table I

Sending And Receiving Time Values Of All Nodes

NODES	RREQ Sending Time	RREP Receiving Time	Calculation done by source node
S	0	32.5	32.5
A	1.5	31	29.5
W1	6.5	29.5	23
W2	12	24.5	12.5
B	13.5	19.5	6
C	15	18	3

RTT's between nodes are:

RTT's: 3 6.5 10.5 6.5 3

NODES: S-------A-------W1--------W2-------B-------C

Table II shows the values of PTT's will be received at source node. RTT's between nodes are:

RTT's: 3 6.5 10.5 6.5 3

NODES: S-------A-------W1--------W2-------B-------C

Table II shows the values of PTT's will be received at source node

Table II

Values Of Ptt's Received At Source Node

NODES	RREQ Sending Time	RREQ Overhearing Time	PTT's
S	0	1.5	1.5-0=1.5
A	1.5	6.5	6.5-1.5=5
W1	6.5	12	12-6.5=5.5
W2	12	13.5	13.5-12=1.5
B	13.5	15	15-13.5=1.5
C	15	-	-

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Journal Impact Factor: 2.114

CONCLUSION

Wormhole attacks can degrade network performance significantly and harms the network security in ad hoc network. Wormhole attack detection is quite complicated. This paper describes the types of security attacks and after that it describes some existing wormhole detection and prevention techniques including their advantages and disadvantages.

REFERENCES

1. H. Highly, "Topology Adaptable Ad Hoc Routing Protocol with Complementary Preemptive Link Breaking Avoidance and Path Shorting Mechanisms", Springer, 2010.
2. K. A. Shah and M. R. Gandhi, "Performance Evaluation of AODV Routing Protocol with Link Failures", IEEE, 2010.
3. N. Khemariya and A. Khuntetha, "An Efficient Algorithm for Detection of Black Hole Attack in AODV based MANETs", IJCA, March 2013.
4. B. J. Chang, Y. M. Lin and Y. H. Liang, "Distributed Wireless Links Repair for Maximizing Reliability and Utilization in Multicast MANET", IEEE, 2008.
5. P. Goyal, V. Parmar and R. Rishi, "Application MANET: Vulnerabilities, Challenges, Attack", International Journal of Computational Engineering & Management, vol. 11, January 2011.
6. A. Kaur and H. Singh, "A Study of Secure Routing Protocols", International Journal of Application or Innovation in Engineering & Management, vol. 2, no. 2, February 2013.
7. Gagandeep, Aashima and P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology, vol. 1, no. 5, June 2012.
8. P. Kansal, N. Prabhat and A. Rathee, "Black Hole Attack in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 3, March 2013.
9. A. L. Shahrani and A. Saad "Rushing Attack in Mobile Ad Hoc Networks", IEEE, 2011.
10. R. Maheshwari, J. Gao and S. R Das, "Detecting Wormhole Attacks in Wireless Networks", IEEE, 2006.
11. P. Sharma and A. Trivedi, "An Approach to Defend Against Wormhole Attacks in Ad Hoc Network using Digital Signature". IEEE, 2011.
12. R. Maulik and N. Chaki, "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications, vol. 3, pp. 271-279, 2011.
13. E. A. M. Anita and V. ThulasiBai, "Defending Against Wormhole Attacks in Multicast Roruting Protocols for Mobile Ad Hoc Networks", IEEE, 2011.
14. M. Azer, S. E. Kassas and M. E. Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks In wireless Ad Hoc Networks", International Journal of Computer Science and Information Security, vol. 1, no. 1, May 2009.
15. H. S. Chiu and K. S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", IEEE, 2006.
16. Y. C. Hu, A. Perrig and D. B. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks", IEEE, 2003.
17. L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", Network and Distributed System Security Symposium, San Diego, California, USA, February 2004.
18. T. V. Phuong, N. T. Canh, Y. K. Lee, S. Lee and H. Lee, "Transmission Time Based Mechanism to Detect Attacks", IEEE, 2007.
19. S. Alshamrani, "PTT: Packet Travel Time Algorithm in Mobile Ad Hoc Networks", IEEE, 2011.