Wormhole attack in Mobile Ad Hoc Networks: A Review

Mr. Susheel Kumar[1]
Associate Professor & H.O.D.
Department of Computer Science and Engineering
Jind Institute of Engineering & technology.
Jind, Haryana, India.

Vishal Pahal[2] , **Sachin Garg**[3]
Department of Computer Science and Engineering
Jind Institute of Engineering & technology.
Jind, Haryana, India.

***Abstract*— Mobile Ad-Hoc Network (MANET) is a wireless network without infrastructure. Self configurability and easy deployment feature of the MANET resulted in numerous applications in this modern era. It generally works by broadcasting the information and used air as medium .It's broadcasting nature and transmission medium also help attacker, whose intention is to spy or disrupt the network. Many type of attack can be done on such Mobile Ad-hoc network. The emphasis of this paper to study wormhole attack, some detection methods and different techniques to prevent network from these attacks.**

***Keywords*- Wormhole attack, Mobile Ad hoc network security, intrusion detection.**

I. INTRODUCTION

Adhoc network are popular and useful because of infrastructure less nature. These are wireless networks, where nodes communicate with each other using multi-hop links. There is no stationary infrastructure or base station for communication. Such a network is helpful in creating communication between nodes that may not be in line-of-sight and outside wireless transmission range of each other. Similar wireless networks have important applications in a wide range of areas covering from health, environmental control to military systems. Each node itself acts as a router for forwarding and receiving packets to/from other nodes The original idea of MANET started out in the early1970s. [18] It generally work by broadcasting the information and use air as medium ,these help attacker ,whose intention is to spy or disrupt the network, so they face acute security problems compared to the wired medium. One of such critical problem is wormhole attack problem. Wormhole attack are one of that type of attack ,which is done by attacker ,can do lot of damage to the network. These attacks can be combined with selective forwarding or eavesdropping. Wormholes can either be used to analyze ,authenticity and non-repudiation are difficult to achieve in MANET, mainly because every node in the traffic through the network or to drop packets selectively or completely to affect the flow of information. There are different type of method available for detection of wormhole attack and it's prevention. The security mechanisms used for wired network such as authentication and encryption are futile under hidden mode wormhole attack, as the nodes only forward the packets and do not modify their headers. Attack in participating mode is more difficult, yet once it is launched, it is also hard to detect. It means all security mechanism available for hidden type wormhole attack is not applicable on exposed type wormhole attack.

MANET has several challenges. They include:-

a) ***Power awarenes:*** Since the nodes in an Ad-hoc network typically run on batteries and are deployed in hostile terrains, they have stringent power requirements. appear smaller, one significant attribute of cluster-based routing is that it can make a dynamic topology appear less dynamic. In order to implement a dynamic hybrid routing scheme, efficient clustering algorithms must be designed.
b) ***Dynamic topology:*** The nodes are mobile and hence the network is self-organizing. Because of this, the topology of the network keeps changing over time.
c) ***Quality of service (QoS)*** – Providing constant QoS for different multimedia services in frequently changing environment.
d) ***Multicast Routing*** – Designing of multicast routing protocol for a constantly changing MANET environment.
e) ***Security:*** Security in an Ad-hoc network is extremely important in scenarios such as a battlefield. The five goals of security – availability, confidentiality, integrity

the network participates equally in routing packets.

f) ***Distributed network:*** A MANET is a distributed wireless network without any fixed infrastructure.

II. IMPACT OF WORMHOLE

To show the impact of wormhole attacks, there is simulated randomly distributing nodes in a rectangular region and used the shortest path algorithm to find the best route between any node pairs. If a wormhole is formed, some node pairs may find "shorter" path through the wormhole and hence be controlled by the wormhole. In first experiment, the base station is at corner, one wormhole endpoint is near the base station and the other endpoint moves diagonally across the network. In the second experiment, the base station is at center, one wormhole endpoint is near the base station and another endpoint moves across the network. We are interested in how many routing paths are affected by a single wormhole?

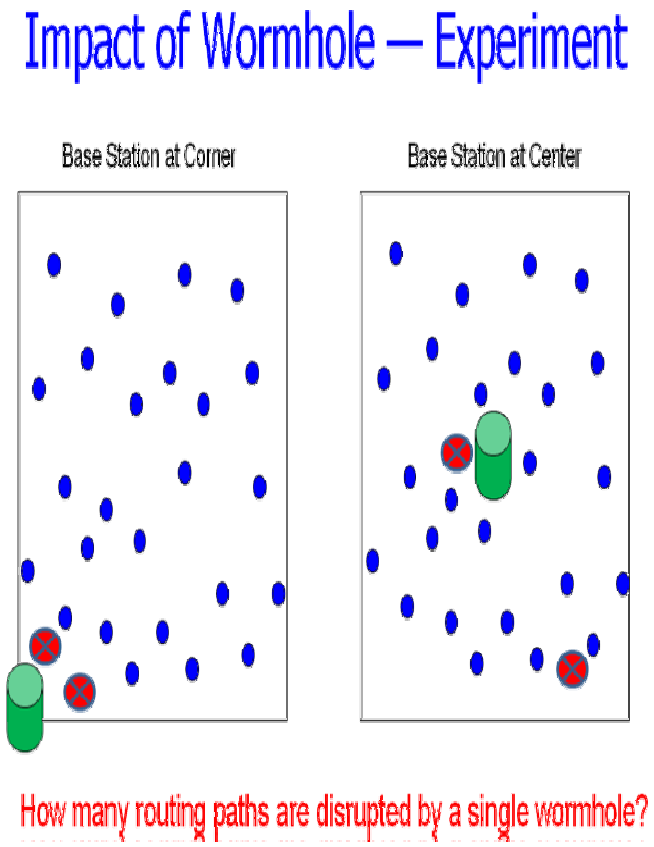

Figure1: Example of different position of base station

The fig.2 below shows the experimental result. If the base station is at center, a single wormhole will be able to attract 30% of the traffic. When the base station is at corner, a wormhole with one endpoint near the base station and the other endpoint one hop away will be able to attract nearly all traffic. This indicates that a single wormhole can greatly affect the performance of network.[3]

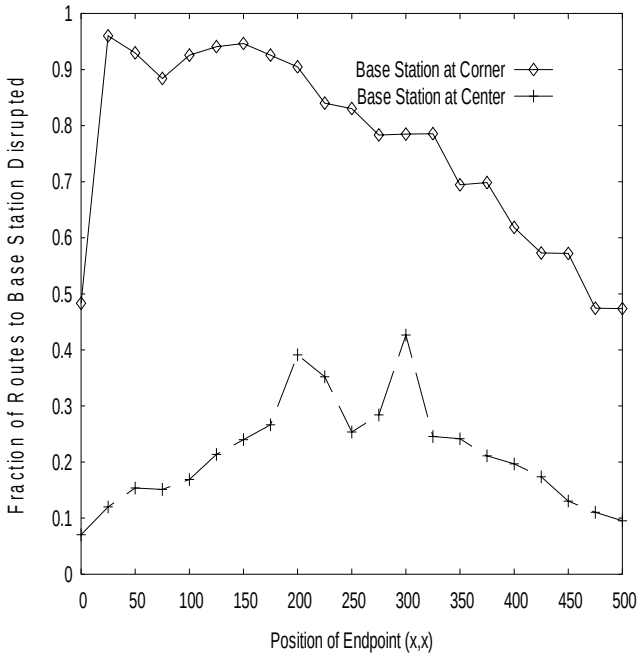

Figure.2: Experimental result [3]

III. PREVENTION OF WORMHOLE ATTACK

Each node will send RREQ messages to destination by using its table of neighbor **[12].** If the sending node does not receive back the RREP message within a fixed time, it detects the presence of wormhole and adds the route to its wormhole list. Each node maintains a neighbor node table which contains a RREQ sequence number, neighbor node ID, sending time and receiving time of the RREQ and count. Here the source node sets the Wormhole Prevention Timer (WPT) after sending RREQ packet and wait until it overhears its neighbor's retransmission. According to the author, the maximum amount of time required for a packet to travel one-hop distance is WPT/2. Therefore, the delay per hop value must not exceed estimated WPT. However, the proposed method does not fully support DSR as it is based on end-to-end signature authentication of routing packets.

There are some proposals to detect wormhole attacks like:
1) The abrupt decrease in the path lengths can be used as a possible symptom of the wormhole attack.
2) With the available advertised path information, if the end-to-end path delay for a path cannot be explained by the sum of hop delays of the hops present on its advertised path, existence of wormhole can be suspected.

3) 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. An abrupt increase in the end-to-end delay and the hop queuing delay values that cannot be explained by the traffic supposedly flowing through these nodes can lead us to suspect the presence of wormhole**.** [14]

IV. CLASSIFICATION OF WORMHOLE ATTACK

For example, in figure 3, the path from S to D via wormhole link (W1, W2) has the length of 5 when the normal path has the length of 11. Therefore, in most routing protocols,S prefers sending data to D along the path with wormhole link.[9]

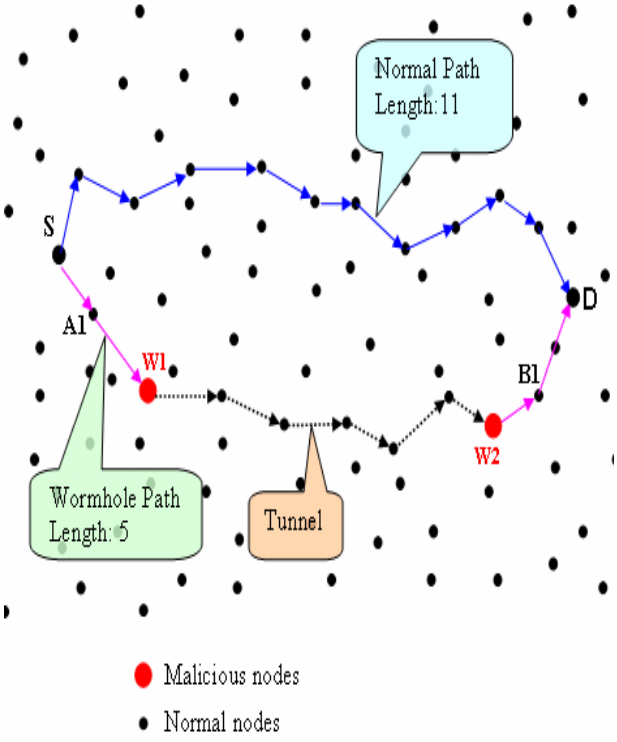

Figure. 3: Example of network showing wormhole attack

There are several ways to classify wormhole attacks. Here we divide wormhole attacks into 2 categories: hidden attacks & exposed attacks, depending on whether wormhole nodes put there identity into packets' headers when tunneling & replaying packets.

A. *Hidden Attacks*

Before a node forwards a packet, it must update the packet by putting their identity (MAC address) into the packet's header to allow receivers know where the packet directly comes from. However, in hidden attacks, wormhole nodes do not update packets' headers as they should so other nodes do not realize the existence of them. For example this kind of attack, a path from S to D via wormhole link W1, W2 will be(Fig. 3):

S _ A1 _ B1 _ D

In this way, B1 seems to get the packet directly from A1 so it considers A1 its neighbor although A1 is out of radio range from B1 (fake neighbors). General speaking, in hidden attacks nodes within W1's vicinity are "fake neighbors" of nodes within W2's vicinity and vice versa.

B. *Exposed Attacks*

In exposed attacks, wormhole nodes do not modify the content of packets but they include their identities in the packet header as legitimate nodes do (figure 3). Therefore, other nodes are aware of wormhole nodes' existence but they do not know wormhole nodes are malicious. In case of exposed attacks, the

path from S to D (figure 3) via wormhole will be:

S _ A1 _ W1 _ W2 _ B1 _ D

In hidden attacks, there are many fake neighbors created by wormhole link but there's no fake neighbor except (W1, W2) in this case. This difference leads to differences in detection mechanisms. Some mechanisms which can do well in detecting hidden attacks cannot detect exposed attacks and vice versa.

C. *Detection of wormhole attack*

If the wormhole is placed carefully by the attacker and is long enough, it is easy to see that this link can attract a lot of routes. Note that if the wormhole link is short, it may not attract much traffic, and hence will not be of much use to the adversary. A wormhole attack is considered dangerous as it is independent of MAC layer protocols and immune to cryptographic techniques. Strictly speaking, the attacker does not need to understand the MAC protocol or be able to decode encrypted packets to be able to replay them. In its most sophisticated form, the wormhole can be launched at the bit level or at the physical layer .In the former, the replay is done bit-by-bit even before the entire packet is received (similar to cut-through routing .In the latter, the actual physical layer signal is replayed (similar to a physical layer relay). These forms of wormholes are even harder to detect. This is because such replays can happen quite fast and thus they cannot be detected easily by timing analysis.

V. SIGNIFICANCE OF WORMHOLE ATTACK

While wormhole could be a useful networking service as this simply presents a long network link to the link layer and up, the attacker may use this link to its advantage, but depend upon intension attacker can do spy and damage.

VI. DETECTION AND AVOIDANCE OF WORMHOLE ATTACKS

Several approaches have been developed to defend against Wormhole attacks in mobile ad hoc networks. In [2] packet leashes are used to protect reactive routing protocols against wormhole attacks. A leash is defined as any information appended to a packet to restrict the maximum transmission distance of the packet. Two kinds of leashes have been proposed: *geographical leashes* and *temporal leashes*. In the geographical leash, the sender appends its location and sending time to a packet. Based on this information, the receiving node computes an upper bound on the distance to the sender. This solution requires in fact location information and coarse synchronization of all nodes in the network. In the temporal leash, the sender appends the sending time to the packet and the receiving node computes a traveling distance of that packet assuming propagation at the speed of light and using the difference between packet sending time and packet receiving time. This solution requires a fine-grained synchronization among all nodes.

The SECTOR protocol [1] presents a countermeasure against wormhole attacks by allowing nodes to prove their encounters with other nodes. However, several hypotheses are needed for this protocol to work correctly. Among these are, the necessity of coarse synchronization, the ability of nodes to measure their local timing with a nanosecond precision, the pre-establishment of security associations between each pair of nodes, and the presence of a central authority that controls the network membership. The so-called disjoint path based approaches have been adopted recently.

In [4] 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 . 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. The performance of on-demand multipath routing (MR) protocol and DSR are compared under wormhole attack.

In [7] detection of wormhole nodes is done on the basis of the Hello control messages. As a metric of compliance with the OLSR specifications, the author has used the percentage of HELLO Message Timing Intervals (HMTIs) that lie within a range bounded by the amount of jitter. A range $R = [T - \delta, T + \delta]$ has been defined. If an HMTI is in this range R, it is considered to be valid; otherwise it is out-of-protocol. A secondary check is done whenever the Hello Message Timing Interval packet behavior is suspicious. On the other hand, a poorly performing node would have associated with it a relatively large number of retry packets, which would not be the case with an attacking node. This way, the problem of false positive alarms is negotiated.

In [10] 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 [10] aims to detect the suspicious link and verify them in a two step process described below.
In the first step, Hello packets are sent to all the nodes within its transmission range. When the receiver receives a Hello (request), it records the sender's address and the time delay Δ left until it is scheduled to send its next Hello message. For piggybacked reply, the node attaches the recorded address of the sender and their respective values of Δ. When a node receives a Hello (reply), it checks whether it contains information related to any of its outstanding requests. If no such information is present, then it treats it as any other control packet. Otherwise, the node checks the arrival time of Hello (reply) to see whether it arrived within its scheduled timeout interval taking into consideration the delay Δ that occurred at the receivers end. If it is within its timeout then the link between itself and node is considered to be safe, otherwise suspicious and communication to that node is suspended by the sender nodes until the verification procedure is over. In the second step, the sender will send a probing packet to all the suspected nodes detected in the previous step. If a proper acknowledgement is received from some node X within its scheduled timeout then node X is again considered to be safe. Otherwise the presence of wormhole is proved. Further the end-to-end authentication is also considered by using symmetric key cryptography.

Both in SaW [16] and DaW [13] similar propositions are made. Only difference is in the selection of routing protocols. In reference [16] AODV protocol was followed while in [13] DSR routing protocol was used. In both of these papers, trust based security models have been proposed and used to detect intrusion. Statistical methods have been used to detect the attacks. If any link is found to be suspicious, then available trust information is used to detect whether the link is a wormhole. In the trust model

used, nodes monitor neighbors based on their packet drop pattern and not on the measure of number of drops. Karl Pearson's formula for correlation coefficient is used in identifying the pattern of the drops. In [13] another algorithm for detecting the presence of wormhole in the network has been proposed. Here, after sending the RREQ, the source waits for the RREP. The source receives many RREP coming through different routes. The link with very high frequency is checked using the following expression :

Pi= ni /N, for all Ii
Pmax = max (Pi),

where *R* is the set of all obtained routes, *Ii* is the *i*th link, *ni* is the number of times that Ii appears in *R*, *N* is the total number of links in *R*, and *Pi* is the relative frequency that *Ii* appears in *R*. If *Pmax* > *Pthreshold*, check the trust information available in the RREP of that route. If the value of correlation coefficient for packets dropped to that sent is greater than the pre-set threshold *t*, then the node is malicious, inform the operator else continue with routing process.

In reference [5], both the hop count and delay per hop indication (DelPHI) are monitored for wormhole detection. The fundamental assumption in [5] is once again that the delay a packet experiences under normal circumstances for propagating one hop will become very high under wormhole attack as the actual path between the nodes is longer than the advertised path. Like [10] the proposed methodology in [5] for wormhole detection is also a two-step process.
In the first phase the route path information are collected from a set of disjoint paths from sender to receiver. Each sender will include a timestamp on a special DREQ packet and sign it before sending it to the receiver. Each node upon receiving the packet for first time will include its node ID and increase the hop count by 1 and discards the packet next time onwards. The DREP packets will be sent by the receiver for each disjoint path received by it. This procedure is carried out for three times and the shortest delay as well as hop count information will be selected for wormhole detection. In the second phase, the round trip time (RTT) is taken by calculating the time difference between the packet it had sent to its neighbor and the reply received by it. The delay per hop value (DPH) is calculated as RTT/2h, where h is the hop count to the particular neighbor. Under normal circumstances, a smaller h will also have smaller RTT. However, under wormhole attack, even a smaller hop count would have a larger RTT. If one DPH value for node X exceeds the successive one by some threshold, then the path through node X to all other paths with DPH values larger than it is treated as under wormhole attack.

In [17] a new protocol called Multi-path Hop-count Analysis (MHA) is introduced based on hop-count analysis to avoid wormhole attack. It is assumed that too low or too high hop-count is not healthy for the network. The novelty of the hop-count analysis in detecting wormholes is however questionable. Similar works have also been reported earlier. As an example, Djenouri et al. [8] may be considered

In [15] WHIDS, a cluster based counter-measure is proposed for the wormhole attack. Simulation results using MATLAB exhibit the effectiveness of WHIDS for detecting wormhole attack. The method, however, has not been tested in presence of multiple wormhole attacks.

Vu et al. [11] also proposed to detect the presence of wormhole using two phases as in and . The first phase consists of two methods. In the first method, the measure of round-trip-time (RTT) between the source node and all of its immediate neighbors are considered. In the second method, source node identifies the one-hop and two-hop neighbors to form its neighbor set. If it is found that the destination node is not a neighbor of the source node then the link between them comes under suspicion. After detecting the suspicious links, the next phase is to confirm the existence of wormholes by using the RTS / CTS mechanism for exchange of messages.

VII. DISCUSSION AND COMPARISON

Method	**Synchronization**	**Mobility Factor**	**Quality Factor**
Geographical Leashes technique	coarse synchronization	Restrict the maximum transmission distance of packet .	Delay up to leashes factor
Temporal Leashes technique	fine-grained synchronization	Restrict the maximum transmission distance of packet .	Delay up to leashes factor
DelPHI	No need	Not required	delay
Farid et al.	Some time delay added to detect suspicious links.	Not required	Queue delay ,packet processing time
HMTIs	No need	Short range wormhole can be detected	Jilter
DaW	No need	Not required	Delay parameter
WAP	Required at source node	Maximum transmission distance is calculated.	Delay per hop
SAM	No need	Clustering required	No need
WORMEROS	RTT between source node and destination node is considered	No change in topology	Not consider

Wormhole attacks, in [6] which adversaries tunnel network data from one end of the network to another using an off-channel link, are a severe routing security concern in mobile wireless ad hoc networks. Wormhole attacks can not be prevented by cryptographic measures as in a wormhole attack they attackers do not create any packets themselves, but simply forward the packets they hear coming from valid network nodes.

Several method use distance-bounding techniques to detect network packets that travel distances beyond radio range, thus preventing packets that have gone through the wormhole from being accepted. However, majority of these techniques rely on specialized hardware, and may not be

practical. Of distance-bounding techniques, GPS-based ones are particularly interesting, as, of the specialized hardware proposed to combat wormhole attacks, GPS is perhaps the most general in purpose, most available currently, and overall most promising. The effectiveness of GPS-based wormhole attack solution is intuitively solid: a packet cannot travel to another end of the network undetected if all nodes know precisely where they are located and where their neighbors are Unfortunately, GPS-based wormhole combating techniques inherit the limitations of GPS technology. They cannot be used where GPS does not work (underwater, inside buildings, caves, etc.), or in small sensor networks (due to the resolution of GPS devices).

Nonetheless, GPS-based techniques are interesting, particularly for military or emergency situations, where GPS devices could be used for location awareness purposes, and could be added to network routing without any additional costs. Network visualization technique presented in for dense sensor networks does not require special hardware, and appears to be very interesting. In this technique, each node reports its perceived distance to its neighbors to a centralized controller. Based on the data collected from network nodes, the controller calculates the estimation of network's physical topology, to which a wormhole, in certain scenarios, introduces impossibilities. It would be very interesting to study how this technique performs on networks that are mobile and not dense. Most likely, the technique will still work, but perhaps with reduces accuracy and higher false alarm rate. If that is the case, with the use of mobile agents for network visualization instead of the central controller this technique could be applied to general MANETs rather than to sensor networks only.

CONCLUSION

Overall, a significant amount of work has been done on solving wormhole attack problem.. We can't say one solution is applicable to all situations. so there is choice of solutions available based on cost ,need of security, type of network . Implementing more hardware for increasing security may lead better result ,but can be costly , which may affect other networks need. Similarly some network require more security like military area network as compare to just local communication network, it also depending on network type like wireless sensor network have less mobility and can be described in some standard model ,but most of other mobile ad hoc network are of infrastructure less ,in this way we can say the choice of detection method depend upon different situation. A standard solution is still lacking, although several very useful solutions applicable to some networks have been described.

REFERENCES

1. S. Capkun, L. Buttyan, and J. Hubaux, *"SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks,"* In Proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (ACM SASN), Fairfax, USA, Oct. (2003).
2. Y.C. Hu, A. Perrig and D. B. Johnson "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*. "In IEEE INFOCOM, vol.3, pp. 1976 – 1986, (Apr. 2003).
3. L. Hu and D. Evans. *Using Directional Antennas to Prevent Wormhole Attacks*. In Network and Distributed System Security Symposium, San Diego California, USA,(5-6 February 2004)
4. 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).
5. H.S. Chiu and K. Lui. "*DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks"*. In proceedings of International Symposium on Wireless Pervasive Computing, pp. 6-11, (2006).
6. Maria Alexandrovna Gorlatova "*Review of Existing Wormhole Attack Discovery Techniques"* A Contractor Report at DRDC Ottawa ,pp 1-23,August (2006).
7. 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"*. In IEEE Military Communications Conference, pp. 1-7 (2006).
8. D. Djenouri, O. Mahmoudi, D. Llewellyn-Jones, M. Merabti, "*On Securing MANET Routing Protocol Against Control Packet Dropping*". In IEEE International Conference on Pervasive Services, pp. 100-108 (2007).
9. Tran Van Phuong, Ngo Trong Canh, Young-Koo Lee, Sungyoung Lee, and Heejo Le ," *Transmission Time-based Mechanism to Detect Wormhole Attacks* " In IEEE Asia pacific service computing Conference ,pp 172-178(2007)
10. F. Nait-Abdesselam, B. Bensaou, T. Taleb. "*Detecting and Avoiding Wormhole Attacks in Wireless Ad hoc Networks",* IEEE Communications Magazine, 46 (4), pp. 127 - 133(2008).
11. H. Vu, A. Kulkarni, K. Sarac, N. Mittal. "*WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks*". In Proceedings of International Confernce on Wireless Algorithms Systems and Applications, LNCS 5258, pp. 491-502, (2008).
12. S. Choi, D. Kim, D. Lee, J. Jung. "*WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks*". In International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp. 343-348, (2008).
13. Khin Sandar Win. "*Analysis of Detecting Wormhole Attack in Wireless Networks",* World Academy of Science, Engineering and Technology, 48, pp. 422-428, (2008).
14. V. Mahajan, M. Natu, A. Sethi. "*Analysis of wormhole intrusion attacks in MANETS"*. In IEEE Military Communications Conference (MILCOM*)*, pp. 1-7(2008)

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

16. M.S. Sankaran, S. Poddar, P.S. Das, S. Selvakumar. "*A Novel Security model SaW: Security against Wormhole attack in Wireless Sensor Networks*". In Proceedings of International Conference on PDCN, (2009).

17. Shang-Ming Jen, Chi-Sung Laih, Wen-Chung Kuo. "*A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET*", 9 (6), pp. 5022-5039, (2009).

18. Reshmi Maulik and Nabendu Chaki " *A Study on Wormhole Attacks in MANET*" In International Journal of Computer Information Systems and Industrial Management Applications ,ISSN 2150-7988 Volume 3 ,pp. 271-279 (2011)