Detection and Prevention of Wormhole Attack Using Decentralized Mechanism

Akanksha Gupta
RIMT College of Engineering & Technology, Mandi Gobindgarh, Fatehgarh Sahib, Punjab, India.

Anuj K.Gupta
Associate Professor & Head of CSE & MCA Department ,
RIMT College of Engineering & Technology, Mandi Gobindgarh, Fatehgarh Sahib, Punjab, India.

Abstract — Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack. A wormhole is one of prominent attack that is formed by malicious colluding nodes. This attack can results in a serious danger in computer networks, particularly against a lot of location-based wireless security systems and ad hoc network routing protocols. The wormhole is feasible still when the attacker has not cooperated as any hosts. A planned position of the wormhole can consequence in a momentous collapse in communication across a wireless sensor network. A planned position of the wormhole can consequence in a momentous collapse in communication across a wireless sensor network. In these attacks two or more wicked colluding nodes generate a high-level effective tunnel in the network, which is engaged to carry packets between the tunnel endpoints. These tunnels imitate shorter links in the network and so perform as benefit to unsuspicious network nodes which by default look for shorter routes. The detection and prevention of such wormholes in an ad-hoc network is still considered a challenging task. Numerous approaches have been proposed for the detection and isolation of wormhole nodes. In this paper we have proposed a new approach for detection and prevention of Wormhole attack. The proposed approach is an improvement over the existing technique and the simulation results of proposed technique show better performance in comparison to the existing technique.

***Keywords*— Ad hoc networks, routing table, security, tunneling, wormhole**

I. INTRODUCTION

Wireless sensor networks (WSNs) are an emerging technology consisting of small, low-power devices that integrate limited computation, sensing and radio communication capabilities. Ad Hoc network are popular and useful because of infrastructure less nature. Ad-hoc Network is a group of nodes, in which individual nodes corporate by forwarding packets for each other to allow nodes to communicate beyond direct transmission range. Wireless ad hoc and sensor networks are typically used out in an open, uncontrolled environment, often in hostile territories. In particular, several important applications for such networks come from military and defence arenas.

Most previous ad hoc networking research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing. Applications that may require secure communications include emergency response operations, military or police networks, and safety-critical business operations such as oil drilling platforms or mining operations. In order, to establish routes between nodes, which are farther than a single hop, specially configured routing protocols are engaged. Use of wireless medium and inherent collaborative nature of the network protocols make such network vulnerable to various forms of attacks. A variety of protocols (reactive, proactive and hybrid) are built; keeping in mind the routing efficiency but not catering for the security. Active routing protocols endeavor to save upon time by discovering routes only when they are essentially required while proactive routing protocols continuously establish and maintain routes, so as to avoid the latency that occurs during new route discoveries. Due to this new kind of self-organizing network combines wireless communication with a high scale of node mobility. Due to abundant constraints for example lack of pre- established trust relationships between nodes, dynamic topology, lack of infrastructure, most of the envisioned routing protocols for ad hoc networks are exposed to a number of troublesome attacks. In this paper, the center of attention is so-called wormhole attack which is known to be mainly difficult to defend against and has been causing a potential harm to a large range of ad hoc routing protocols.

The lack of infrastructure and the subsequent absence of authorization amenities in MANETs obstruct the natural practice of separating nodes into trusted and non-trusted , establishing a line of defense. As there is no earlier security classification, all nodes require to work together in network operations. Moreover in MANETs a node can connect or leave the network at any time without any notice. As a result it might be difficult in lots of cases to have a clear observation of the ad hoc network association. In such a situation, there is no assurance that a path between two nodes would be free of wicked nodes or not. The mechanisms currently integrated in MANET routing protocols cannot deal with disruptions due to malicious activities.

Security of communication in MANET is essential for secure transmission of information. In view of the nonappearance of any central co-ordination component and the vicinity of imparted wireless medium, MANET gets more vulnerable against computerized/digital assaults than wired system. As clarified in [4], the assaults could be sorted according to their origin- Inside or External, and on the behaviour of the attack- Active or passive. In active attack, the performance of the network is made upset; critical information is taken and the information is destroyed throughout the trade in the system. The active attacks are designed to damage the performance of network in such case the active attack act as internal node in the network. Unlike active attacks, in passive attacks, the typical operations of the network are not disrupted. In Passive attack, the attacker listens to network with a specific end goal to get information about the current transmissions. It listens to the network to know and understand how the nodes are interacting with one another, how they are spotted in the network. A typical example of such a cooperative attack is a wormhole in which a malicious node tunnels the packets from one end of the network to another. This paper defines a particularly challenging attack to defend against called as wormhole attack and presents a new, general mechanism for detecting and thus defending against wormhole attacks.

The remainder of this paper is organized as follows: Section II contains brief introduction of wormhole attack. Section III contains the amount of work done till date in lieu of the wormhole attacks. Section IV contains the significance of wormhole attack in MANETs. Section V details the motivation towards present work. Section VI encompasses the proposed approach and the methodology steps. Section VII presents the simulation results and the observation details. Finally section VIII concludes the paper.

II. WORMHOLE ATTACK

Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another [1]. In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point [2]. Indeed, a wormhole attack is feasible even when the network infrastructure provides confidentiality and authenticity, and the attacker does not have the cryptographic keys.

For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive with better metric than a normal multi hop route through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnelthe bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways [2]. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node.

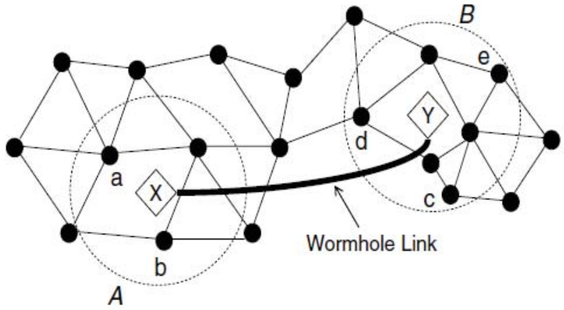

Fig. 1 Wormhole Attack

Fig. 1 shows Demonstration of a wormhole attack where X and Y denote the wormhole nodes connected through a long wormhole link. As a result of the attack, nodes in Area A consider nodes in Area B their neighbors and vice versa.

III. LITERATURE REVIEW

A considerable amount of work has been done for the detection/mitigation of wormhole attacks as well as the attackers. This section contains a short survey of the approaches proposed till date.

Jyoti Thalor et.al [2013], surveyed the existing approaches which can help to design a new approach for detecting the wormhole attack in Mobile Ad Hoc network. Overall a significant amount of work has been done on solving wormhole attack problem. There is choice of solution available based on cost, need of security may lead better result, but can be costly, which may affect other networks need. Similarly some network requires more security like military area network. A standard solution is still lacking, although several very useful solutions applicable to some networks have been described.

Ajay Prakash Rai et.al [2012], analyze wormhole attack nature in ad hoc and sensor networks and existing methods of the defending mechanism to detect wormhole attacks without require any specialized hardware. This analysis is able to provide in establishing a method to reduce the rate of refresh time and the response time to become more faster.

Zubair Ahmed Khan et.al [2012], proposed the use of the modified routing table for detection of the suspicious links, confirmation of wormhole existence, at the end isolating the confirmed wormhole nodes. The approach has been applied to DSDV and the detection of self-sufficient wormhole nodes and attacks.

Shalini Jain et.al [2010], have deviated from the customary approach of using cryptography and instead employ a trust-based scheme to detect and evade wormholes. In our scheme, we derive trust levels in neighbouring nodes based upon their sincerity in execution of the routing protocol. This derived trust is then used to influence the routing decisions, which in turn guide a node to avoid communication through the wormholes. Through extensive testing, we have established that the trust model can effectively locate dependable routes through the network in the presence of a wormhole in the network. By using Trust Based Model Packet Dropping is reduced by 15% without using any cryptography mechanism and throughput is increased up to 7-8%.

Lukman Sharif et.al [2010], focus on the wormhole routing attack in some detail. A variety of countermeasures have been proposed in the literature for such attacks. However, most of these countermeasures suffer from flaws that essentially render them ineffective for use in large scale WSN deployments.

Yih-Chun Hu et al. presents environmental and chronological leashes for detecting wormholes. A environmental leash wants each node to identify its own location and all nodes to contain loosely time synchronized clocks. The nodes require to firmly exchange location information. A sender node can next make sure that the receiver is contained in a certain distance and detect discrepancies within. With chronological leashes, all nodes should have tightly synchronized clocks. Then the receiver will contrast the sending time with the receiving time attached with the packet. It can conclude and detects the wormhole attack if the packet has travelled too far in too little time. each node should know its own location which requires the need for a Global Positioning system for the construction of geographical leash and for temporal leash all nodes should have tightly synchronized clocks. To achieve strict time synchronization between the nodes special hardware is needed which makes the setup complex and costly. The processing and queuing delays considers to be negligible in this approach and does not acquire congestion into account.

L. Hu and D. Evans proposed, wormhole detection mechanism using directional antennas based on the zone of the arriving signal . If a node uses a definite zone of its antenna to be in touch with its neighbors, this neighbor should respond using the opposite zone. This method depends upon the teamwork between nodes in sharing directional information and requires special hardware with each node and suffers from antennas directional errors but requires no location information or clock synchronization.

Hon Sun Chiu proposed that the node that is responsible for sending detects wormhole attack by finding delays of different paths to the receiver. Delay information and hop count of disjoint paths are collected and delay per hop value is calculated to serve as an indication for the presence of wormhole attacks. In normal situation, the packet experiences the delay in propagating one hop which should be comparable along each hop in the path. But due to the presence of malicious nodes along the path under the wormhole attack , the delay is unreasonably high. As a result if a path has high delay per hop value, it is considered to be a wormhole attack. A wormhole can be identified by comparing the delay per hop values between these disjoint paths. This method cannot locate wormhole attack but prevents both exposed and hidden attack . As every node can change the length of the paths, wormhole nodes might change the path length so that it makes them unable to detect.

L. Lazos et.al presented a graph theoretic approach characterizing wormhole attacks on wireless ad hoc networks. The necessary and sufficient conditions for any transformation to remove wormholes have been derived, and showed that any candidate solution preventing a wormhole attack must produce a connected subgraph of the geometric graph model of the network. A cryptography-based solution relying on local broadcast keys has been proposed. The paper showed that the appropriate choice of network parameters eliminates wormhole links with a probability close to unity and verified the validity of our results via simulations.

Ritesh Maheshwari et.al proposed a novel algorithm for detecting wormhole attacks in wireless multi-hop networks. The algorithm uses only connectivity information to look for forbidden substructures in the connectivity graph. The proposed approach is completely localized and does not use any special hardware artifact or location information. The paper present simulation results for three different communication models and two different node distributions, and show that the algorithm is able to detect wormhole attacks with a 100% detection and 0% false alarm probabilities whenever the network is connected with high probability.

Yih-Chun Hu et.al define a particularly challenging attack wormhole attack, and present a new, general mechanism for detecting and thus defending against wormhole attacks. The paper presents a general mechanism, called packet leashes, for detecting and defending against wormhole attacks, and a specific protocol called TIK has been presented that implements leashes. The paper also discusses topology-based wormhole detection, and shows that it is impossible for these approaches to detect some wormhole topologies.

Yurong Xu et.al describes a distributed wormhole detection algorithm for wireless sensor networks, which detects wormholes based on the distortions they create in a network. Since wormhole attacks are passive in nature, the algorithm uses a hop counting technique as a probe procedure, reconstructs local maps in each node, and then uses diameter" feature to detect abnormalities caused by wormholes. The main advantage of the algorithm is that it can provide the approximate location of wormholes, which is useful in implementing countermeasures. Simulation results show that the algorithm has low false toleration and false detection rates.

IV. SIGNIFICANCE OF WORMHOLE ATTACK

A wormhole assault is viewed as dangerous as it is free of MAC layer protocol and the assailant does not have to comprehend the MAC protocol. While wormhole could be a useful networking service as this basically exhibits a long network link to the link layer and up, the intruder may utilize this connection further to his advantage. After the assailant pulls in a considerable measure of data traffic through the wormhole, it can disturb the information flow by specifically dropping or modifying data parcels, producing unnecessary routing activities by turning off the wormhole link intermittently, and so on. The attacker can likewise basically record the traffic for later investigation. Utilizing wormholes an assailant can additionally break any convention that directly or indirectly relies on geographic proximity [3].

V. MOTIVATION

As explained by Nadher M. A. Al_Safwani [5], security in MANET system is one of the main concerns to provide protected communication between mobile nodes in strange environment. Unlike the wired line networks, the unique characteristics MANET create a number of nontrivial challenges to security design like open peer-to-peer network architecture, shared wireless medium, inflexible resources constraints and highly dynamic network topology.

In order to implement security in MANET, environment needs to be secured against attacks. Security services in MANET's are needed to protect from attacks and to ensure the security of the information. The wireless channel is accessible to both intended and unintended users. There is no well-defined place where traffic monitoring or access control mechanisms can be brought into life. As a result, there is no clear boundary that separates the inside network from the outside world.

VI. PROPOSED SCHEME

Several methods have been proposed for detecting wormhole attacks in ad hoc networks and WSNs, each and every one tailored according to scenarios available for the proposing researchers. Mobile Ad-Hoc Networks are able enough to deploy a network where any traditional network infrastructure environment cannot possibly be deployed. Instead of numerous advantages and utmost importance of WSNs, still there are some challenges that need to be addressed. Security of MANET is one of the important features for its deployment.

A. Proposed Method

Mobile ad hoc networks are exposed to numerous security attacks, as the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation. As studied in [6], a wormhole attack detection scheme has been proposed by Zubair AhmedKhan. The considered system includes the use of the modified routing table for identification of malicious links. The approach has been applied to DSDV which is a proactive protocol. Moreover, the existing approach only involves detection of the attack and does not provide any prevention mechanism. Considering the drawbacks of the existing system, this paper proposes an approach which involves detection and prevention of wormhole attacks in other protocols as well as comparison of the proposed technique with the existing system.

The present work emphasizes on achieving the following objectives:

1. Detection of wormhole nodes in the network using monitors
2. Preventing the wormhole attack by choosing new nodes in the neighborhood of victim node
3. Comparing the performance of the proposed technique with base study

B. Methodology

1. Deploy the nodes
2. Divide the network into clusters
3. Select the cluster head for each cluster
4. Each cluster will have one monitor node
5. First we make path from source to destination for normal communication
6. Then add one pair of wormhole nodes which will form a tunnel in the path
7. After introduction of wormhole nodes, whenever data will reach the wormhole node it will send less amount of data to the another wormhole node, now sink will receive less data
8. Now source will inform the monitor node about the number of packets it forwarded
9. Sink after receiving the data, inform its respective monitor about the number of packets it received.
10. If number of packets received by the monitor is less than number of packets sent by source then monitors start the checking process.
11. Monitor asks their nodes about the number of packets they received and packets they forwarded.
12. By comparing this, monitor nodes can detect wormholes in the path.
13. Now to prevent the wormhole nodes, monitors will chose new node in the neighborhood of the node (around which tunnel was created) .
14. Those new nodes will be added in the path and wormholes will be removed from the path.

The proposed methodology is needed to be implemented in a tool. The tool opted for simulation of the proposed work is NS2.35.

VII. EXPERIMENTAL RESULTS

In this section, simulation results demonstrating the effectiveness of our algorithm in detecting wormhole attacks have been presented. The proposed method has been implemented in NS 2.35 and the experimental results are presented.

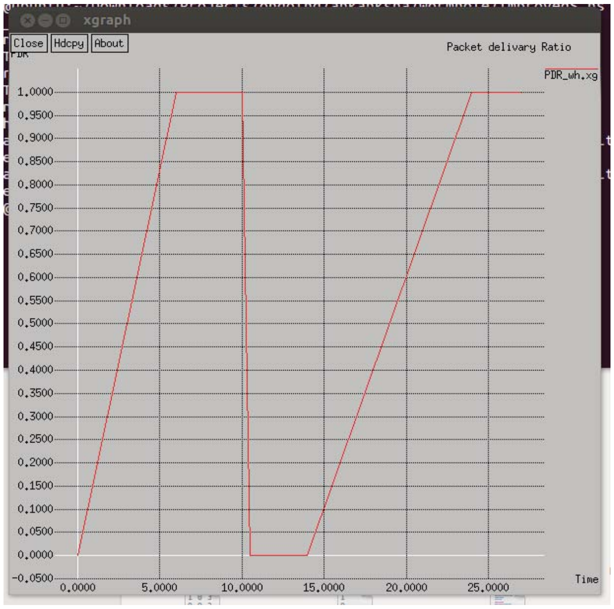

Fig. 2 Packet Delivery Ratio

When normal communication is taking place, initially the observed PDR value is 1, while during attack, node around which tunnel was created could not receive any packet so PDR observed is 0 further after detection and prevention when an alternate path is provided, again PDR value became 1.

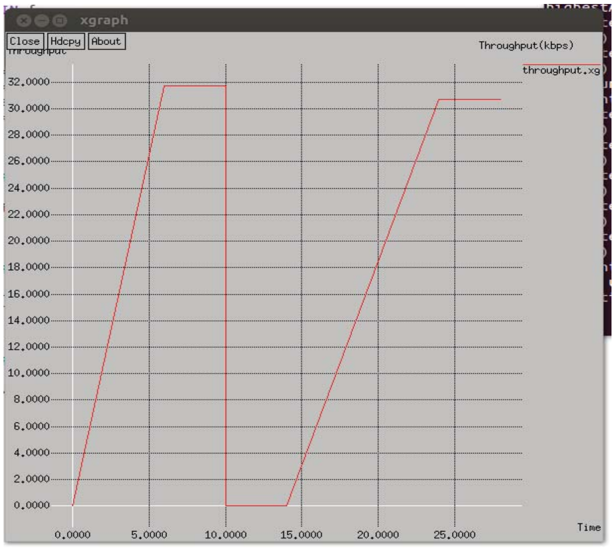

Fig. 3 Throughput

While normal communication, the observed throughput value is 1, while during attack, node around which tunnel was created could not receive any packet so throughput is 0 further after detection and prevention when an alternate path is provided, throughput value became 1.

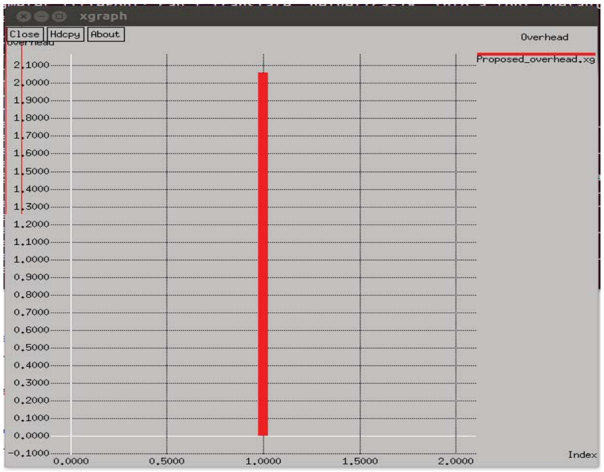

Fig. 3 Overhead

The overhead value of the simulation results is observed as 2.05 approximately.

VIII. CONCLUSIONS

The paper introduces the wormhole attack that can have serious consequences on many proposed ad hoc network routing protocols. The methodologies proposed by different authors to eliminate the Wormhole attack are discussed. In this work a solution has been proposed via simulation to give better network performance in terms of Packet Delivery ratio. The objective of the work is to detect and prevent wormhole attack in MANETs. The proposed solution has been simulated in NS-2.35 and the results are compared with the results of base paper taken into consideration. The observation shows that the proposed solution presents improved results in terms of performance metrics.

ACKNOWLEDGMENT

The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work. I would like to thank all the individuals whose encouragement and support has made the completion of this work possible.

REFERENCES

[1] Jyoti Thalor, Ms. Monika, “*Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review*”, Volume 3, Issue 2, February 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[2] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, “*Wormhole Attacks in Wireless Networks*”, IEEE

[3] Ritesh Maheshwari, Jie Gao and Samir R Das, “Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information”

[4] OCHOLA EO, ELOFF MM, “A Review of Black Hole Attack on AODV Routing in MANET”

[5] Nadher M. A. Al_Safwani, Suhaidi Hassan, and Mohammed M. Kadhum, “Mobile Ad Hoc Networks Under Wormhole Attack: A Simulation Study”, Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI 2011,8-9 June, 2011 Bandung, Indonesia

[6] Zubair Ahmed Khan, M. Hasan Islam, “Wormhole Attack: A new detection technique”

[7] Yurong Xu, Guanling Chen, James Ford and Fillia Makedon, “Detecting Wormhole Attacks In Wireless Sensor Networks”

[8] L. Lazos1, R. Poovendran1, C. Meadows2, P. Syverson2, L. W. Chang2, “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach”

[9] Shalini Jain, Dr.Satbir Jain, “Detection and prevention of wormhole attack in mobile adhoc networks”, International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010 1793-8201

[10] Mahesh Gour, , Amrit Suman†and Ankur Kulhar, “Detection and Prevention of Wormhole Attack in ALARM Protocol (MANETs)”, HCTL Open Int. J. of Technology Innovations and Research, HCTL Open IJTIR, Volume 4, July 2013, e-ISSN: 2321-1814

[11] K. Sivakumar, “Analysis of Wormhole Attack In MANET And Avoidance Using Robust Secure Routing Method”, Volume 3, Issue 1, January 2013 ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering

[12] Dhara Buch and Devesh Jinwala, “Prevention Of Wormhole Attack In Wireless Sensor Network”, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.5, Sep 2011

[13] Modirkhazeni, A.; Aghamahmoodi, S.; Modirkhazeni, A.; Niknejad, N.; , "Distributed approach to mitigate wormhole attack in wireless sensor networks," Networked Computing (INC), 2011 The 7th International Conference on , vol., no., pp.122-128, 26-28 Sept. 2011

[14] Meghdadi M, Ozdemir S, Güler I. A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks. IETE Tech Rev 2011;28:89-102

[15] W. Weichao, B. Bharat, Y. Lu, and X. Wu. "Defending against wormhole attacks in mobile ad-hoc networks," Wireless Communication and Mobile Computing, vol. 6, no. 4, pp 483□503, 2006.

[16] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W.; "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," Wireless Communications and Networking Conference, 2005 IEEE , vol.2, no., pp. 1193- 1199 Vol. 2, 13-17 March 2009.

[17] S. Özdemir, M. Meghdadi, and Ý. Güler. "A time and trust based wormhole detection algorithm for wireless sensor networks," (manuscript in Turkish), in 3rd Information Security and Cryptology Conference (ISC□08), pp. 139□4, 2008.

[18] 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.

[19] R. Maulik "A Comprehensive Review on Wormhole Attacks in MANET". In Proceedings of 9th International Conference on Computer Information Systems and Industrial Management Applications2010.

[20] Yih-Chun Hu and David B. Johnson,— Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, In Proceedings of the IEEE Conference on Computer Communications (Infocom), 2003.

[21] L. Hu —Using directional antennas to prevent wormhole attacks,‖ In Proceedings of the IEEE Symposium on Network and Distributed System Security , 2004

[22] Hon Sun Chiu and King-Shan Lui, —DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks,‖ International Symposium on Wireless Pervasive Computing , 2006.

[23] Le Xuan Hung, Young-Koo Lee and Heejo Lee, —Transmission time-based mechanism to detect wormhole attack,‖ In Proceedings of the IEEE Asia-Pacific Service Computing Conference, 2007.

[24] Mohammad Rafiqul Alam and King Sun Chan, — A Topological Comparison Based Method to Detect Wormhole Attacks in MANET,‖ 12th IEEE International Conference on Communication Technology, 2010.

[25] S. Capkun, L. Buttyan, and J.P. Hubaux., —SECTOR: Secure tracking of node encounters in multi-hop wireless networks, In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks , 2003.

[26] Rutvij H. Jhaveri, Ashish, and Bhavin I. Shah, —MANET Routing Protocols and Wormhole Attack against AODV,‖ International Journal of Computer Science and Network Security (IJCSNS), April 2010.

[27] Amrit Suman , and Bhupendra Verma, —A Behavioral Study of Wormhole Attack in Routing for MANET,‖ International Journal of Computer Application July 2011.

[28] Perkins and S. Das, —Ad hoc On-Demand Distance Vector (AODV) Routing, IETF Network Working Group, July 2003.