WDAP: Wormhole Detection and Avoidance Protocol for Mobile Ad-hoc Environment

Nitika Chaure
Computer Science Department
Jagadguru Dattatrya College of Technology,
Indore (India)
Rajiv Gandhi Proudyogiki Vishwavidyalaya
(State Technological University of State Madhya Pradesh, India)

Khushboo Sawant
(Asst. Prof.)
Computer Science Department
Jagadguru Dattatrya College of Technology,
Indore (India)
Rajiv Gandhi Proudyogiki Vishwavidyalaya
(State Technological University of State Madhya Pradesh, India)

ABSTRACT
Network security is an important criteria for wired and wireless communication. The advancement in wireless technologies and the high availability of wireless equipment in everyday devices is a factor in the success of infrastructure-less networks. MANETs are becoming more and more common due to their ease of deployment. The high availability of such networks and the lack in security measures of their routing protocols are alluring a number of attackers to intrude. In such environment, the presence of malevolent nodes may result in wormhole attacks. In this paper, a secured AODV-based routing scheme Wormhole Detection and Avoidance i.e. WDAP is proposed for mitigating such attacks. Implementation is performed in NS2 environment and results are provided to demonstrate the effectiveness of our approach, using the packet delivery ratio, Network throughput, Routing Overhead and the number of packets received by destination, as performance indicators.

Keywords
MANET, RREQ, RREP, AODV, Wormhole, NS–2, Security, Wireless Communication

1. INTRODUCTION
Ad-hoc networks are a key in the evolution of wireless networks [1]. Ad-hoc networks are typically composed of equal nodes, which communicate over wireless links without any central control. Although military tactical communication is still considered as the primary application for ad-hoc networks, commercial interest in this type of networks continues to grow. Applications such as rescue missions in times of natural disasters, law enforcement operation, commercial and educational use, and sensor networks are just few possible commercial examples.

Ad-hoc wireless networks inherit the traditional problems of wireless and mobile communications, such as bandwidth optimization, power control and transmission quality enhancement. In addition, the multi-hop nature and the lack of fixed infrastructure generate new research problems such as configuration advertising, discovery and maintenance, as well as ad-hoc addressing and self-routing.

A mobile ad hoc network, such as the one shown in Figure 1, is a collection of digital data terminals equipped with wireless transceivers that can communicate with one another without using any fixed networking infrastructure. Communication is maintained by the transmission of data packets over a common wireless channel. The absence of any fixed infrastructure, such as an array of base stations, makes ad hoc networks radically different from other wireless LANs. Whereas communication from a mobile terminal in an "infrastructure" network, such as a cellular network, is always maintained with a fixed base station, a mobile terminal (node) in an ad hoc network can communicate directly with another node that is located within its radio transmission range [2].

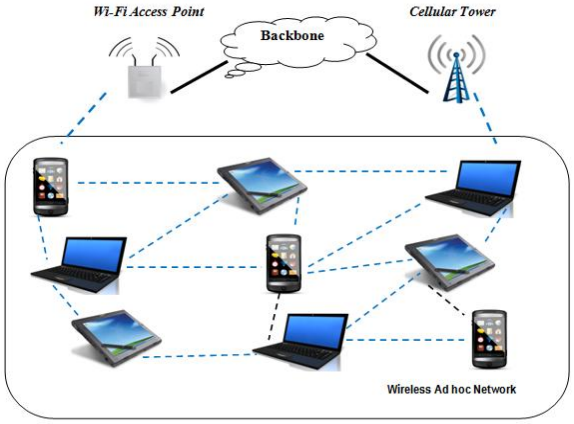

Figure 1: Mobile ad hoc network [2]

The remainder of paper is organized as follows. Section II describes related work and Section III is short note about Wormhole Attack. In Section IV, proposed scheme is discussed for making MANET free from the Wormhole attack. Implementation of the proposed scheme is covered in Section V and Result Section is VI. Finally conclusion are given in Section VII.

2. RELATED WORK
Numerous Researchers have worked on multiple detection and prevention of wormhole attacks in wireless mesh network, based on the detection mechanism, the existing techniques of detecting and preventing wormhole attacks can be illustrate in this section.

A. Distance and location Based: Packet Leash Technique
Hu et al. proposed the concept of packet leashes to detect wormholes in wireless networks. It uses two types of packet leashes one is geographical leashes and another one is temporal leashes, but this method requires GPS and tightly synchronized clocks. In geographical leashes, each node knows its precise location and all nodes have loosely synchronized clocks to determine the neighbor relation. Before sending a packet, node appends its current position and transmission time to it. On getting packet, receiving node

computes the distance with respect to the sender and the time required by the packet to traverse the path. The receiver can use this distance information to deduce whether the received packet passed through a wormhole link or not. In Temporal leashes, every node maintains a tightly synchronized clock but does not depend on GPS information [3].

B. Special Hardware Based Approaches

The Secure Tracking of Node Encounters in Multi-hop Wireless Networks (SECTOR) is a wormhole detection technique that does not depend on time synchronization (SrdjanCapkun et.al, 2003) [4].In this SECTOR method we uses Mutual Authentication with Distance-bounding (MAD) protocol for the estimation of distance between 2 nodes or users. MAD operates in the assumption that every node is appended with transceiver as extra Hardware.

Directional antenna detects the existence of wormhole nodes (Lingxuan Hu and David Evans, 2004). In this method, directional information is shared between source and destination. The destination can detect the wormhole by comparing the received signal from the malicious nodes and directional information from the source. If the both the signals from the source and intermediate nodes are different, then the wormhole link is detected [5]

C. DelPHI Technique

DelPHI provides a solution to the exposed wormhole attacks [6]. In this mechanism, delay per hop is determined in every path and it is proved that delay per hop for the genuine path is shorter than the wormhole path. If the path has noticeably high delay per hop, then the corresponding path is affected by wormhole.

D. Wormhole Geographic Distributed Detection

An algorithm for the distributed detection of wormhole attack is provided by YurongXu in 2007 [7] called wormhole geographic distributed detection (WGDD). WGDD algorithm detects the wormhole attack based on the damage caused by them and the parameter used for wormhole detection is hop count. According to the hop count measured, it reconstructs the mapping details in each node and finally it exploits diameter feature to detect distortions caused by malicious nodes. WGDD algorithm is effective in finding the exact location of the wormholes

E. Secure Neighbor Discovery and Monitoring Based Approach

This is provided by Issa Khalil in 2008 [8] which uses local observation schemes to prevent malevolent nodes in the vicinity. The position of each node in the network is traced by central authority and it is capable of even isolating the malicious nodes globally. The detection rate of this method decreases as the network mobility increases.

F. Statistical Analysis Multi-path Routing based Method

In 2005, N. Song et al. [9] proposed another detection scheme for detection of the wormhole attacks called Statistical Analysis Multi-path Routing (SAM). The authors used the highest probability of relative frequency of a link to arise in the set of all obtained routes from one route discovery and 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 innovation, which will be superior in the presence of wormhole attack. The probability mass function (PMF) is used to get that the maximum relative frequency, which is more for a system under wormhole attack as comparison with a normal system.

3. WORMHOLE ATTACK

Scarcity of various resources makes wireless sensor network vulnerable to several kinds of security attacks. Attacker possessing sufficiently large amount of memory space, power supply, processing abilities and capacity for high power radio transmission, results in generation of several malicious attacks in the network. Wormhole attack is a type of Denial of Service attack that misleads routing operations even without the knowledge of the encryptions methods unlike other kinds of attacks. This characteristic makes it very important to identify and to defend against it [10].

Wormhole attack is a severe type of attack on Wireless sensor network routing where two or more attackers are connected by high speed off-channel link called wormhole link. Wormhole attacks exists in two different modes, namely ‘hidden’ and ‘exposed’ mode, depending on whether attackers put their identity into packet headers when tunneling and replaying packets [11].

In wormhole attack, a pair of attackers forms ‘tunnels’ to transfer the data packets and replays them into the network. This attack has a tremendous effect on wireless networks, especially against routing protocols. Routing mechanisms can be confused and disrupted when routing control messages are tunneled. The tunnel formed between the two colluding attackers is referred as wormhole. Figure 1 shows the wormhole attack. Packets received by node X is replayed through node Y and vice versa.

Normally it take several hops for a packet to traverse from a location near X to a location near Y, packets transmitted near X travelling through the wormhole will arrive at Y before packets travelling through multiple hops in the network. The attacker can make A and B believe that they are neighbors by forwarding routing messages, and then selectively drop data messages to disrupt communication between A and B [12].

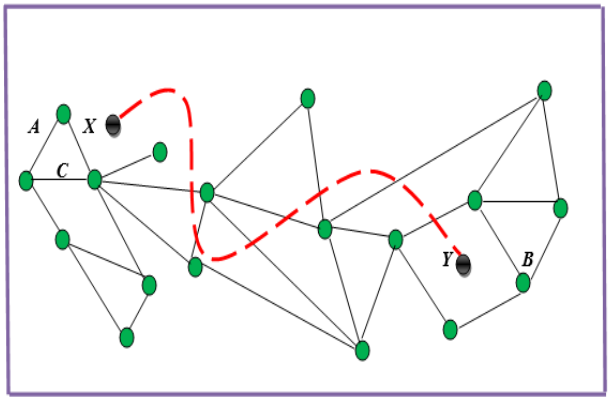

Figure 2: Wormhole Attack [13]

4. PROPOSED SYSTEM

The proposed technique needs to develop a method by which the routing algorithm self-detect and prevent the wormhole attack in network. Therefore the proposed technique needs to incorporate the following solution.

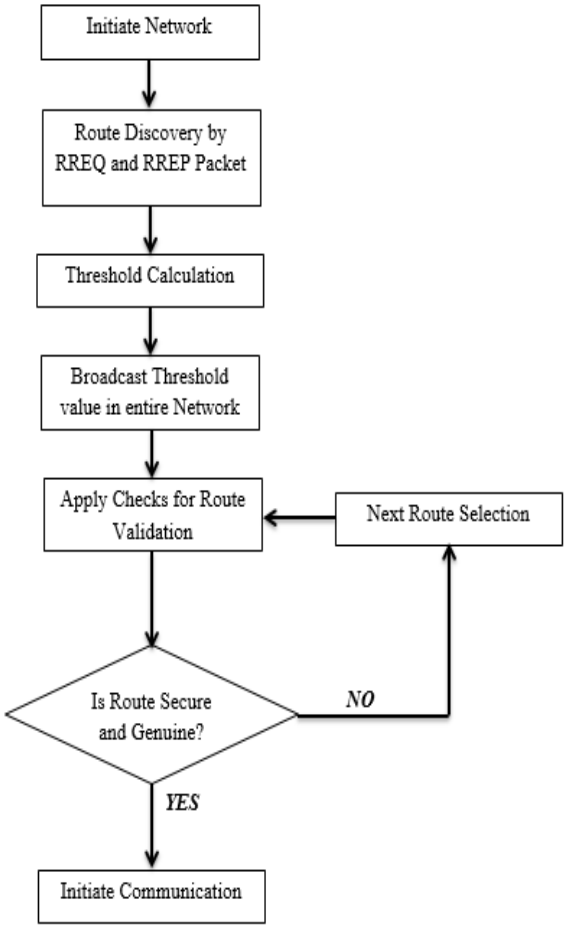

Figure 3: Flow diagram of Proposed Work

Existing detection technique based on 3 steps named Route redundancy, route aggregation and round trip time (RTT). Due to multiple RREQ & RREP there are extra overhead or load on the nodes of the routes. To overcome this load we proposed a scheme that minimizes routing overhead from the network. In this presented work a wormhole infected route is distinguished by comparing the RTT values of individual hop count, in addition of that in order to minimize the overhead in the system a load aware secure routing strategy is suggested in the proposed work. Thus if a network contains a N number of nodes and between source node S and a target node D is want communicate with secure route and optimum path then the proposed routing technique is described as:

A. Proposed Algorithm

The entire process of the solution development is described using the summarized step of algorithm and described in following table:

Table 1: Detection and Prevention

Input: No. of Nodes, ***Output:*** Found Malicious Node; Performance Measures;
Process: **1:** Source sends a RREQ message to destination with initializing a timer T_s **2:**Source waits for reply from all the RREP messages after each route reply estimate T_d **3:**Each Route Contain Numbr of Hop Counts i. e. H **4:**Set the Hop Count between source and destination is 2H **5:**Calculate RTT of Individual Node $RTT = \frac{\delta_{time}}{h_c}$ **6:**Compute the threshold by repeating the RTT computation $RTT_{total} = \frac{T_d - T_s}{2H}$ **7:**Source Node Contain Path information in entry Table **8:** ***for*** i = 0 to 2 Send a dummy message to next hop router[i] Count RTT for router [i] ***if*** (RTT ≤ RTT_{total} && $Buffer\ Length > Buffere\ Length_{total}/2$) Label Route as Malicious Route ***else if*** (Select router [i] as next hop) **9:** ***endfor*** **10:**Go to step 7 till next hop = Destination Router

5. IMPLEMENTATION

The simulation is being implemented in the Network simulator [14]. Protocol used here is AODV.

Table 2: Simulation Scenarios

Parameters	***Values***
Antenna Model	Omni Antenna
Dimension	1000X1000
Radio-Propagation	Two Ray Ground
Channel Type	Wireless Channel
Traffic Model	CBR
Routing Protocol	AODV
Mobility Model	Random Waypoint

1. **Simulation of AODV Routing under Attack**:In this network simulation the network is configured with the traditional AODV routing protocol and the network performance is evaluated. That simulation also contains a malicious wormhole link which demonstrates the effects of wormhole attack in normal network. The simulation of the proposed technique is given in the figure 4. In this diagram the green nodes show the client nodes involved in the network and the sender and receiver for the network is demonstrated using the blue colour nodes. Additionally the malicious nodes that are creating the wormhole link are demonstrated using the red color nodes.

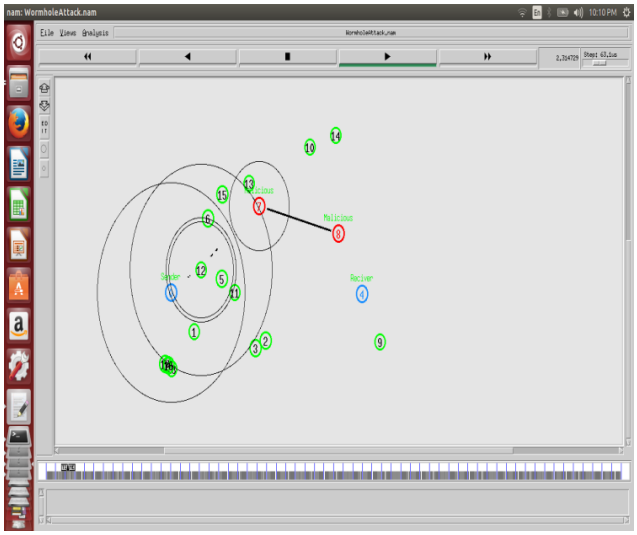

Figure 4: Network under Attack condition

2. **Simulation of Proposed Scheme of Attack Prevention:** In this simulation the proposed secure routing protocol is implemented in the network simulator 2 environment with the similar configuration as the other two networks is configured. After that for investigating the effect of the proposed solution the wormhole link is applied on the network and the network performance is evaluated and compared with the traditional approach of network security. The simulation of both the wormhole detection process is simulated and using the network trace file the simulation performance of both the techniques are extracted and used for the comparative performance study.

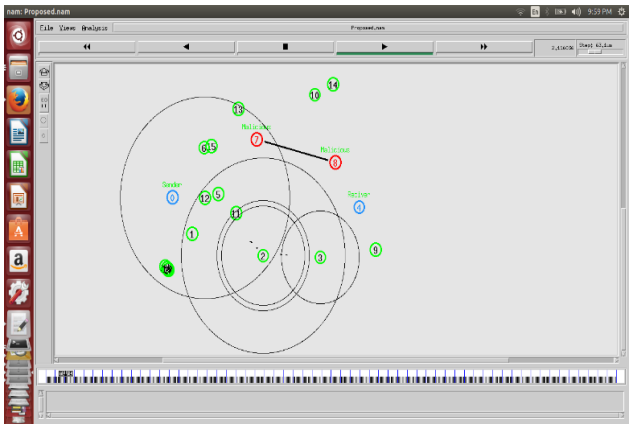

Figure 5: Proposed Solution for wormhole prevention

6. RESULT ANALYSIS

1. End to End Delay

End to end day on network refers to the time taken, for a packet to be transmitted across a network from source to destination device, this delay is calculated using the below given formula.

$$E2E\ delay = Receiving\ time - Sending\ time$$

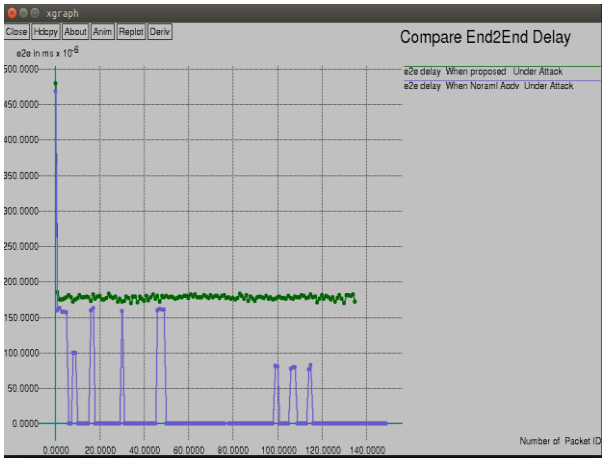

Figure 6: End to End Delays

Figure 6 shows the comparative end to end delay of old AODV routing method and the proposed secure routing technique. In this figure 5.1 the X axis contains the number of nodes in network and the Y axis shows the performance of network in terms of milliseconds. According to the obtained results the proposed technique is produces less end to end delay as compared to traditional routing technique under attack conditions. Therefore the proposed technique is an efficient technique and produces less amount of time.

2. Packet Delivery Ratio

The performance parameter Packet delivery ratio sometimes termed as the PDR ratio provides information about the performance of any routing protocols by the successfully delivered packets to the destination, where PDR can be estimated using the formula given

$$Packet\ Delivery\ Ratio = \frac{Total\ Delivered\ Packets}{Total\ Sent\ Packets}$$

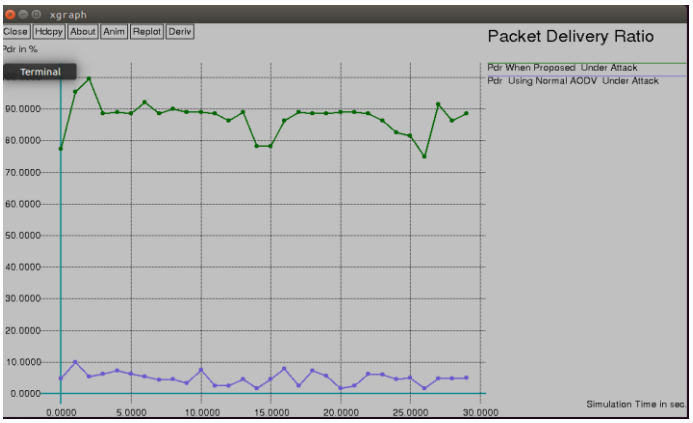

Figure 7: Packet Delivery Ratios

The comparative packet delivery ratio of the networks is given using figure 7 in this diagram the X axis shows the number of nodes in the network and the Y axis shows the amount of packets successfully delivered in terms of the percentage.

The red line of diagram represents the performance of the old method and the green line shows the performance of the proposed technique. According to the obtained results the proposed technique delivers more packets as compared to the traditional technique even when the network contains the attacker node therefore the proposed technique able to avoid the attack effect and improve the network performance.

3. Throughput

Throughput is a measure of how many units of information a system can process in a given amount of time. This information may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

The comparative throughput of the network is demonstrated using figure 8 in this diagram the X axis shows the number of nodes in network and the Y axis shows the throughput of the network in terms of KBPS. The green line in this diagram shows the performance of the proposed technique and the red line shows the performance of the old technique.

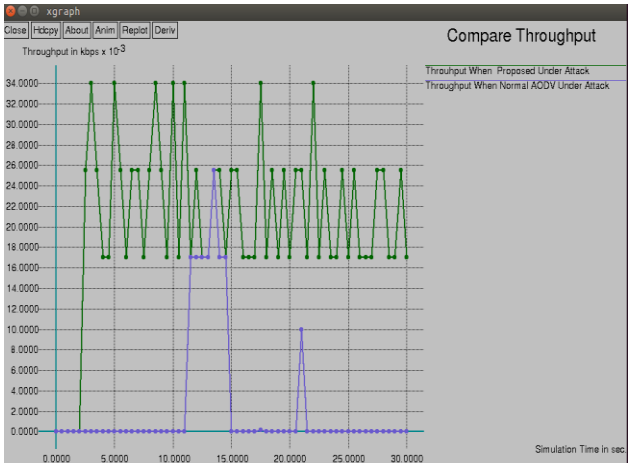

Figure 8: Throughput

According to the obtained performance the proposed technique improve the throughput of the network during the attack conditions also therefore the technique is effectively avoid the attack effect as compared to the traditional routing technique.

4. Energy Consumption

The amount of energy consumed during the network events is termed as the energy consumption or the energy drop of the network. In networking for each individual event a significant amount of energy is consumed. The given figure 9 shows the energy

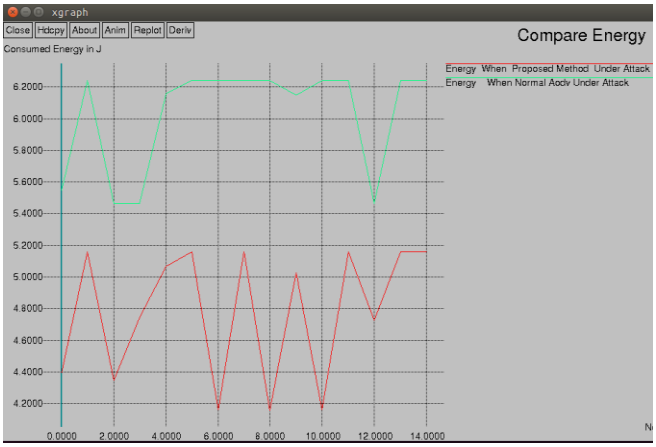

Figure 9: Energy Consumption

Figure shows Energy Consumption of the network in both the simulation scenarios. The red line of the diagram shows the amount of energy consumed with the AODV routing protocol under attack condition additionally the green line shows the amount of energy consumed during the proposed algorithm based network. In the traditional AODV the network energy is frequently consumed as compared to the proposed routing protocol because the Wormhole Attack attack targeting the network by consuming the resources of the network. Therefore the proposed technique is effective and able to recover the network from the attack situations.

5. Packet Drop Ratio

The packet delivery ratio shows the amount of packets failed to deliver in destination device, thus the percentage amount of data dropped in network is termed as the packet drop ratio.

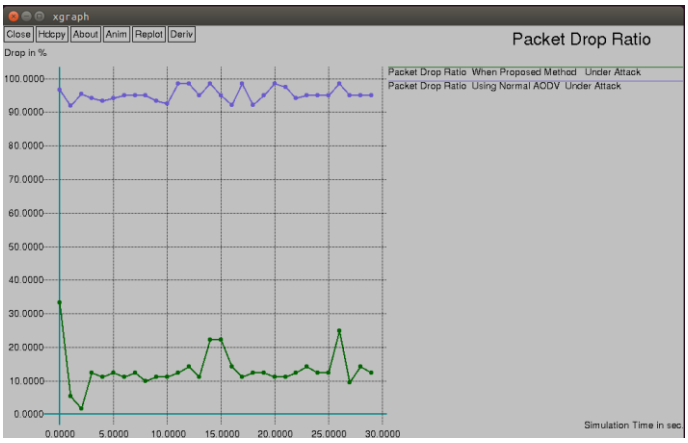

Figure 10: Packet Drop Ratio

The amount of packets dropped in both the implemented solution scenarios is given using figure 10 in terms of percentage drop. In this diagram the performance of the proposed technique is simulated using green line and blue line shows the performance of network under attack. In addition of that in the given figure the X axis shows the simulation time in seconds and the Y axis shows the amount of packet dropped. According to the obtained performance the proposed technique drops fewer amounts of packets as compared to the normal AODV condition.

7. CONCLUSION

There is not a single protocol which can give the best performance in ad hoc network. Performance of the protocol varies according to the variation in the network parameters and ad hoc network properties continuously vary. So, the choice of the protocol is the basis to perform in a particular type of network. MANETs require a reliable, efficient, and scalable most importantly, a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. The mobile ad hoc network is one of the most popular network technologies now in these days. The study here establishes the foundation for future work towards designing a mechanism to identify the nodes which are actively involved in any attack. In this presented work the security aspects of the ad hoc network is investigated and a new solutionWDAP for securing the network against the Wormhole attack is proposed. Thus the WDAP technique provides effective performance even when the network contains more than one malicious links.

8. REFERENCES

[1] Indrani Das and D. K Lobiyal, "Effect of Mobility Models on the Performance of Multipath Routing Protocol in MANET", Computer Science & Information Technology (CS & IT) Computer Science Conference Proceedings (CSCP), PP. 149–155, 2014

[2] AsisNasipuri Chapter 3 Mobile Ad Hoc Networks Handbook of RF and Wireless Technologies, Newnes is an imprint of Elsevier. 200 Wheeler Road, Burlington, MA 01803, USA, 2004

[3] T DivyaSaiKeerthi and PallapaVenkataram, "Locating the Attacker of Wormhole Attack by Using the Honeypot", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, PP. 1175 – 1180, 2012

[4] Hu, Y. Perrig, A., and Johnson D., Packet Leashes: "A Defense Against Wormhole Attacks in Wireless Network", In Proceedings of the 22nd IEEE International Conference Computer and Communications, Volume 3, pp.1976–1986, April 2003.

[5] SrdjanCapkun, LeventeButtyan and Jean-Pierre Hubaux, 2003 "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks" SASN'03 Proceedings of 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21-32.

[6] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," In Network and Distributed System Security Symposium (NDSS), San Diego California,USA, 5-6 February, 2004.

[7] Chiu, HS; Wong Lui, KS, 2006 "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks" 1st International Symposium on Wireless Pervasive Computing

[8] YurongXu, Guanling Chen, James Ford and FilliaMakedon, 2007 "Detecting wormhole attacks in wireless sensor networks" International Federation for Information Processing proceedings on critical infrastructure protection, volume 253, pp. 267-279

[9] Issa Khalil, SaurabhBagchi, and Ness B. Shroff, 2008 "MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multi-hop Wireless Networks" Ad Hoc Networks, Volume 6, Issue 3, pp. 344-362

[10] N. Song, L. Quin, and X. Li., "Wormhole Attack 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.

[11] DharaBuch, DeveshJinwala, "Detection of Wormhole Attacks in Wireless Sensor Networks", IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.

[12] Majid Meghdadi, SuatOzdemir and InanGuler, "A Survey of Wormhole based Attacks and their Countermeasures in Wireless Sensor Networks", IETE Technical Review, VOL 28, ISSUE 2, Mar-Apr 2011.

[13] Mani Arora, Rama Krishna Challa," Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", Second International Conference on Computer and Network Technology, pp 102-104, 2010.

[14] The Network Simulator. NS-2 [Online] http://www.isi.edu/nsnam/ns/