WORMHOLE ATTACK DETECTION AND PREVENTION IN MOBILE AD-HOC NETWORK USING AUTHENTICATION BASED DELPHI

***Shraddha S. Mahajan, **Dr. Hitendra D. Patil**

**Master Student, Computer Engineering, SSVPS'S B.S.Deore College of Engineering, India*

***Professor and Head, Computer Engineering, SSVPS'S B.S.Deore College of Engineering, India*

ABSTRACT

As Mobile Ad-hoc network is infrastructure less network in which every node can take part in data transmission and reception process. Various kinds of attacks have been arises in the network during transmission, which affects on the performance of the network. Wormhole attack is one attack from them which is created by collaborative attackers. Different techniques have developed to detect & prevent wormhole. But perfect solution is yet to be covered. Delay per Hop Indication (DelPHI) is a technique for wormhole detection in which authentication is essential in order to provide prevention. This is an effective approach to detect the fake route and also adopt preventive measure against wormhole nodes so that it will not appear in the route discovery phase. The focus of this paper is to provide a better solution in terms of wormhole detection of wormhole and to take some preventive measurement against the wormhole by considering the pros and cons.

Keywords—Mobile Ad-hoc Network, Wormhole Attack, AODV protocol, DSR protocol

INTRODUCTION

Ad-hoc network is self-configuring network in which each node can take part in the process of data sending and receiving. Day by day issues related to the network performance and security has increase while uses of network take big part. There is no guarantee that nodes in the network can communicate without affection of malicious node. Most of the routing protocol also get failed to comply with such malicious nodes or attackers. The purpose of ad-hoc network is to provide secured communication in hostile environment. As MANET is self-dependent network, each node can establish routing. As MANET is foundation-less network, each node can directly transmit or receive data to each other indirectly through intermediate nodes. Therefore each node can act as a router. Each node that participating in some routing protocol required for deciding and maintaining the routes. As MANET is rapidly deployable, self organizing, it is highly suitable for military operations or government uses. Many routing protocols are used in mobile ad-hoc network such as Ad-hoc On-demand Distance Vector Routing (AODV), Destination Sequence Distance Vector (DSDV) and Dynamic Source Routing (DSR), since it is critical task because of highly dynamic environment which is given below [1].

1. Ad hoc On Demand Distance Vector Routing (AODV)

AODV is basically an improvement of DSDV (Destination Sequence Distance Vector). As DSDV is proactive in nature, AODV is not so. Ad hoc On Demand Distance Vector Routing (AODV) is reactive routing protocol. Based on demand, it minimizes the number of broadcasts by making routes available. This thing is not done in DSDV routing protocol [3].

2. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a reactive protocol based on the source route approach. Dynamic Source Routing (DSR) protocol is based on the link state algorithm in which source initiates route discovery on demand basis. As MANET works with infrastructure less network that is untrusted environment, various attackers tries to reduce the performance of the network [2].

Attacks in MANET

As use of networking is grown up, security related issue is also increases. During utilization of network for data transmission and reception process, it is responsibility of the user to take care that performance of the network should not degrade. Hackers always try to add intrusion into authorized data in the network. Black hole attacks, white hole attacks, wormhole attack is attacks which affects on the performance of the network. In white hole attack, large amount of traffic floods in the network which creates collusion inside the network. In black hole attack, attacker drops the traffic which is passing through it. Black hole attack and white hole attack s created by single attacker.

WORMHOLE ATTACK

This is attack which is created by two or more attackers called as collaborative attackers. Malicious nodes try to create tunnel in the network and try to send data via that wormhole nodes created which detects the wormhole attack in MANET, but all works is quite insufficient eliminate wormhole from the networks. All the attacks mentioned above are performed by a single attacker. It is mainly focus on that attack which launch by collaborative attackers which is in pair. It focuses on attacks which launch by a pair of collaborating attackers. In a wormhole attack, an attacker records packets at one location and just tunnels them to second attacker which resides at another location. It obtains hop count information and delay of some disjoint paths between the sender and the receiver and uses the information to indicate whether a certain path among these disjoint paths is subjected to wormhole attacks. Wormholes cannot be detected by cryptographic techniques, since the contents of the packets are not modified. These two malicious nodes are acting as neighbors in network, and hiding the fact that they are several hops away by tunneling in actual. This attack creates serious threats in ad hoc network routing protocols. The advantage of DelPHI is that it does not require clock synchronization and position information. It does not require the mobile nodes to be equipped with some special hardware which in turns provides higher power efficiency [1].

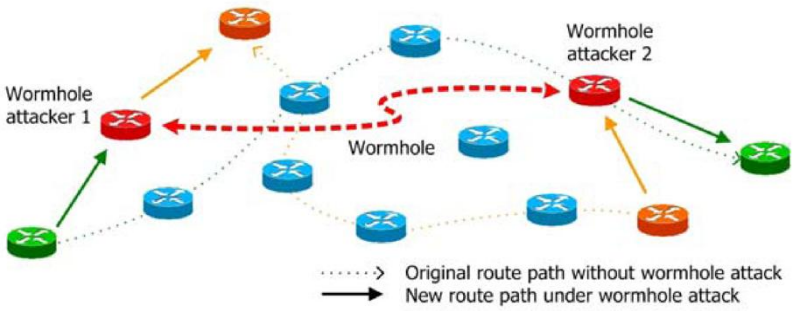

Figure 1: Wormhole Attack

Wormhole attack can be categorized into two groups.

1. Hidden wormhole attack
2. Exposed wormhole attack

Hidden attack is also called as out of band wormhole in which authorized nodes doesn't know the existence of malicious nodes. Exposed attack is also called as in band wormhole in which authorized nodes are aware about existence of malicious nodes [1].

RELATED WORK

Various researches had been done to detect and prevent wormhole or tunneling in the network. In ad-hoc network, multihop wireless mobile nodes can transmit and receive data to each other without having any centralized control of the network. This protocol helps to increase the performance of the network. Different technique like DelPHI (Delay Per Hop Indication), DAW (Distributed Antiworm Detection), WAP (Wormhole Attack Prevention), Packet Leashes has developed which work effectively against wormhole attack by using different routing protocols like, AODV, DSR, DSDV etc. Number of techniques has developed to detect the wormhole and to take preventive measurement against wormhole [2].

Pushpendra Niranjan, Prashant Srivastav, Rajkumar Soni & Ram Pratap develop a technique called as Detection of Wormhole using Hop count and Time Delay Analysis. In this method instead of detecting suspicious routes, they implement a new method which detects the wormhole using Hop count and Time delay method. Here to identify misbehaving nodes Watchdog and Pathrater techniques had been created which worked effectively against wormhole detection mechanism. Watchdog method just compare incoming packet with outgoing or sent packet. If both packets are same then it considered that packet is valid and then discard that packet. Pathrater is a technique which calculates the path metric for every path. It enables the parameter to select the shortest path. Thus it avoid routes in which misbehaving nodes are resides. But one of the biggest cons of this technique is that it cannot detect misbehaving node in the process of ambiguous collision. Scheme get failed nodes receive the signal at opposite angle [9].

Yih-Chun Hu, Adrian Perrig David B. Johnson introduced this technique called "Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks". In this technique they present an effective protocol called as TIK (TELSA with Instant Key Discloser) leashes. Two types of leashes are presented in this technique such as temporal leashes & geographical leashes. TELSA used symmetric cryptographic primitives for wormhole detection. Drawback is that, this mechanism is not designed to replace cryptographic authentication [7].

Lijun Qian and Ning Song, Xiangfang Li introduced a new technique called as "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path (SAM)". This system use Statistical Analysis of Multipath approach for wormhole detection. By just analyzing the information collected by multi-path routing statistically, it detects wormhole attacks and identifies the attackers. Its drawback is fixed positions of two attackers which make them enable to tunnel RREQ between each other during all simulations. Node mobility is not considered here [3].

Wormhole can also detected by using Hound Packet. Saurabh Gupta, Subrat Kar & S. Dharmaraja had developed this mechanism. This mechanism is generally developed for the discovery of wormhole which has large tunnel length. In established path, source node initiate wormhole detection process after the phase of route discovery. Route difference between neighbor node and one hop away node is counted in the route. Ann if the hop difference between neighbors exceeds than acceptable level then destination node detects the wormhole. Drawback is that if tunnel length is smaller than 4 then detection rate of normal path is less [10].

Choi, Kim, Lee & Jung had also presented a new technique called as WAP (Wormhole Attack Prevention. This mechanism is work with two phases such as Neighbor Node Monitoring and Wormhole Route Detection. In first neighbor node table is created for each node entry. It checks for malicious behavior of neighbors. Wormhole Prevention timer detects the wormhole using WPT timer. In second phase wormhole route is detected and wormhole entry is done in Wormhole Node List so that it will not appear in the list again [2].

ANALYSIS OF PROBLEM

Data transmission and reception is risky process since MANET is infrastructure less network and here each node can take participation in this process. Various types of hackers try to hack the data during the process of data travelling from one node to other. Wormhole attack is one from those which is created by two or more attackers. Here two unauthorized node or malicious node create a large tunnel between each other and passes unauthorized data through it otherwise it increase the size of the network or create unnecessary delay in the data transmission process which indirectly degrade the overall performance of the network. Existing system cannot take some preventive measurements against wormhole attacks. It also needs to add some more performance factor to

increase the performance. Some techniques required special types of hardware as well as clock synchronization which may lead better results but can be costly [4][5].

PROPOSED METHOD

Proposed method is developing to resolve all the problems which have occurred in previous method. Proposed method is based on DelPHI (Delay per Hop Indication)**.** By considering the base of this mechanism a new method is proposed that is authenticated DelPHI. As DelPHI is AODV based method, proposed method is also AODV based in which routes are obtained as demand or needed. The entire route set up procedure of this technique is based on AODV protocol. Therefore proposed system is divided into two modules.

I. DelPHI
II. Authenticated DelPHI

For wormhole detection, DelPHI is used and for prevention of wormhole proposed system that is authenticated based DelPHI is used. Let see these two phases in details.

I. DelPHI

DelPHI can detect both, hidden and exposed attack. It has ability to detect wormhole by just observing delay and hop count information from each node. DelPHI works with three different modules given below.

1. Data Collection

In this phase, route related information like delay, hop count etc. is collected. Two possible disjoint paths are created here that is DREQ roadmap and DREP roadmap. These two disjoint paths help to detect wormhole easily. DREQ (Data request) is broadcasted from sender to receiver with timestamp field, hop count field and node id. These all fields are updated by each node during DREQ transmission. The principle of DREQ is to collect route information at each node. When request (DREQ) reach at destination then acknowledgment is given by receiver using data reply (DREP) roadmap. Receiver first update each field and then unicasts DREP request through exactly reverse path from destination to source. Here receiver must have to reply for each DREQ request. Round Trip Time (RTT) is a time required for sending packets from source to destination. In this method, delay/hop and RTT value is calculated by sender and according to the difference value of it, sender analyzed that whether wormhole is located or not. According to the network simulator, it is observed that delay per hop value in normal path is smaller than tunneled/wormhole path. Advantage of DelPHI is that it does not required clock synchronization and special hardware. It also has higher power efficiency. Biggest drawback of DelPHI is that if wormhole is located at all side, DelPHI get failed to locate it. It cannot find pin point location of wormhole. It cannot take preventive measurement against wormhole attack.

2. Data Analysis & Detection

The sender initiates the detection broadcast the DREQ packet at the time t_s, then it receives DREP packet from its neighbor node at t_i time. Round trip time of the path through node is given by RTT = $t_i - t_s$. DPHi value is then calculated using this RTT value. If the hop count field in the DREP from node is h_i then the delay hop value of the path to the path to the receiver through node is given by

$$DPHi = \frac{RTTi}{2hi} = \frac{ti-ts}{2hi} \quad (1)$$

Smaller h provides smaller RTT value in normal path. Shorter path have shorter RTT value. Hence the DPHi value of normal paths should have similar values independent to h.

3. Measurement of Delay & Hopcount

In this phase collected information is analyzed by the sender that is whether wormhole is located in the path or not. It is observed that path in which wormhole is located has a larger network size than normal path. That means that the path in which wormhole is resides, its hop count and delay value has increases than normal path. So that it may be indirectly degrade the performance of the network. The DPHi values usually appear smaller than tunneled path. DPH values of normal and tunneled paths can be observed easily from two separate groups. The difference between the smallest DPH value in the tunneled group and the largest DPH value in the normal group is always larger than the gap between any two DPH values within the same group. If the DPH is larger than the next DPH value by a threshold then the path through node and all other paths with DPH values larger than DPH_i are treated as wormhole attack.

II. Authenticated DelPHI

As like DelPHI, Authenticated DelPHI is also used AODV protocol for route set up procedure. DelPHI can only used to detect the wormhole. But this method is able to take some preventive measurement against wormhole attack so that it will not reappear in the network. DelPHI used delay and hopcount parameter for performance evolution. In order to increase the performance factor of the network four more parameters are added in proposed mechanism that is throughput, packet delivery ratio, dropped packet and overhead which create this technique more effective. Authenticated DelPHI works with two different modules given below.

1. Authentication and Forwarding

Every transmitting or receiving node has its own signature. Nodes must be able to authenticate that the data has been sent by the legitimate node. RSA is applied for authentication. A node receiving the RREQ verifies that the sender is authenticated user or not along with the checking of proposed rate limiting classification technique and it forwards the request to its neighbors only if it is received from authenticated user otherwise it will not forward the RREQ. Each node sends the request with its original ID and the encrypted id (signature) for authentication. Encryption process is done at sender side with specific key and decryption process is done at receiver side with same key. If key

is matching then its proved that node is authenticated, otherwise node is unauthenticated. At the end authenticated user and unauthenticated user is classified using RSA algorithm. Of course the path in which wormhole is located is unauthorized path. Valid data is forwarded through authenticated that are normal path.

2. Performance Evaluation

For evaluating the performance of the network some performance factor is used like Delay, Packet drops, Throughput, Packet Delivery Ratio and Overhead. Let see them in details.

Throughput is the amount of time taken by the packet to reach the destination.

$$\text{Throughput (bits/s)} = \text{Total Data} / \text{Data Transmission duration}$$

Delay is nothing but the average time taken by data packet to arrive in the destination. It includes the delay caused by queue in data packet transmission and route discovery process. Only the data packets that successfully delivered to destinations that counted.

$$\text{End to End delay} = \sum (\text{arrive time} - \text{send time}) / \sum \text{Number of connections}$$

Packet delivery ratio is the ratio of the number of delivered data packet to the destination. It indicates the level of delivered data to the destination.

$$\text{Packet delivery ratio} = \sum \text{Number of packet receive} / \sum \text{Number of packet send}$$

Packet drop is the total number of packets which drops during the communication process. Packet drops should be less in order to increase the performance of the network.

Overhead is defined as total number of beacon update messages involved in the communication. Data that you send across a wireless network is housed in a data envelope called a packet. Each data transmission includes additional information which is nothing but overhead, It is essential to route the data to the proper location. Network overhead can be easily calculated by sending a fixed-size data transmission across the network and observing the number of extra bytes of data transmitted for the action to be completed.

$$\text{Overhead} = \text{Number of messages involved in beacon update process.}$$

SIMULATION SCENARIO

The performance of Authenticated DelPHI is evaluated using NS-2 (v2.35) Network Simulator. For implementation of this method N number of nodes are arrange in topological order. And this topology is created randomly with size L x L. Node number with label is assign to sender S receiver R, Malicious node M1 & M2. These all nodes are put into corresponding places.

Simulation model is as follows:

Table 1: Simulation Scenario

Simulation Parameter	Value
Simulator	NS2
Number of nodes	30, 40, 50, 60
Topology	Random
Network Area	1000 X 1000
Queue type	Drop tail/Priority Queue
Antenna type	Omni Antenna
Propagation type/model	Tworay Ground
Routing protocol	AODV
Transport agent	UDP
Application agent	CBR
Packet size	512 bytes
Packet interval	0.25
Transmission range	250m
Simulation time	100sec

RESULTS

Performance is evaluated using network simulator. Here some results are generated and based method is compared with contributed method. Performance factors are throughput, packet delivery ratio, overhead, delay and hop count. Table given below shows the results generated by DelPHI and Authenticated DelPHI.

Table 2: Performance Evaluation

Performance Parameter	DelPHI	Authenticated DelPHI
Throughput	0.135606	0.173477
Packet Delivery Ratio	88.05548	113.3195
Overhead	1525.75	980.5
Delay	0.102355	0.077454
Dropped Packet	183	102.5

1. Throughput

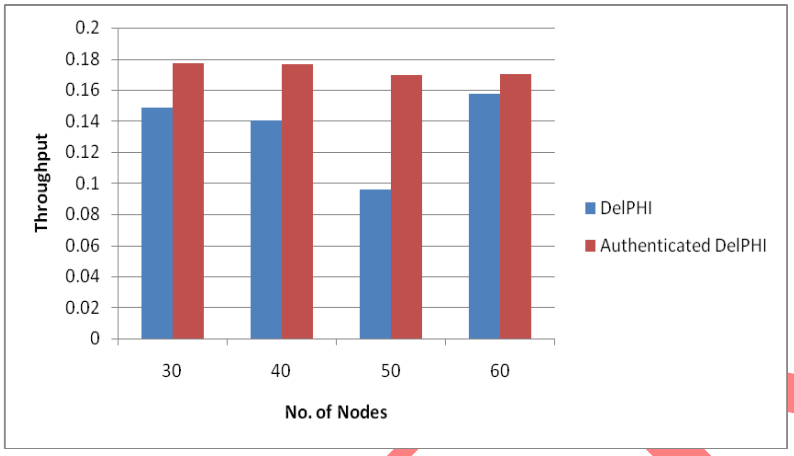

Figure 1: Comparison of Throughput

2. Packet Delivery Ratio

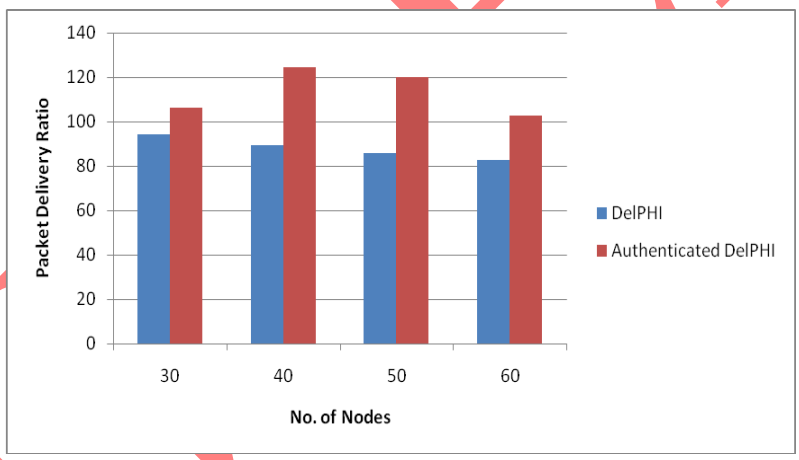

Figure 2: Comparison of Packet Delivery Ratio

3. Overhead

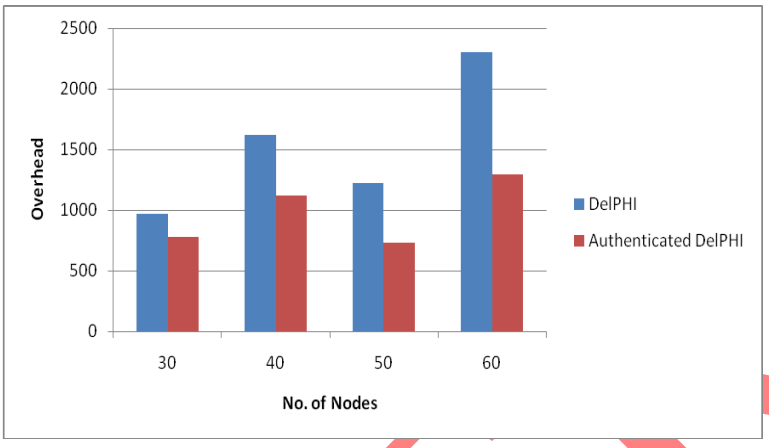

Figure 3: Comparison of Overhead

4. Delay

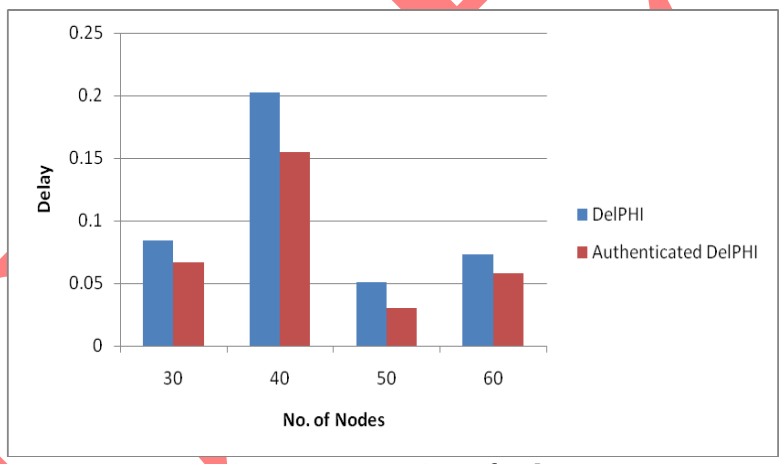

Figure 4: Comparison of Delay

5. Dropped Packet

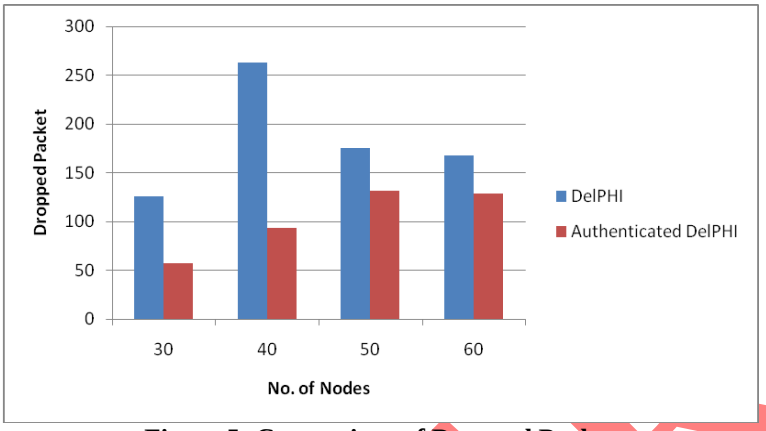

Figure 5: Comparison of Dropped Packet

CONCLUSION

DelPHI is an effective technique for detecting a wormhole attack in network, since it can observe the path using just delay and hopcount. In order to increase the performance of network it is essential to take some preventive measurement against wormhole attack. Authenticated based method can take preventive action against wormhole. Proposed method can also increase the performance of the network. It used some extra parameter like throughput, packet delivery ratio, dropped packet and overhead. So that mechanism works effectively. In proposed system RSA algorithm is used for encryption & decryption. Data can be forwarded from only authenticated rather than wormhole path, so that wormhole will not reappear in the network. No special hardware is required for this method. Detection and prevention rate is higher than other techniques. Overhead, packet drops and delay is also decreases in this method. Throughput and packet delivery ratio is increases in this method.

BIBLIOGRAPHY

[1] Hon Sun Chiu and King Shan Lui, "DelPHI : The Efficient Wormhole Detection Mechanism for Ad Hoc Wireless Network," *1st International Symposium on Wireless Pervasive Computing IEEE Transaction on Mobile Computing*, pp. 1-6, 16 Jan 2007.

[2] Sun Choi, Doo-young Kim, Do-hyeon and Jae-il Jung, "WAP : Wormhole Attack Prevention Algorithm in Mobile Ad-hoc Networks," *IEEE International Conference on Sensor Network, Ubiquitous and Trustworthy Computing*, pp. 343-348, 2008.

[3] Deepesh Namdev and Shikha Singhal, "Wormhole Attack Detection and Prevention Mechanism for Mobile Adhoc Nework," *Quest Journal of Electronics and Communication Engineering Research*, vol.

2, no. 6, pp. 7-16, 7-July 2014.

[4] Anil Kumar Fathepura and Sandeep Raghuwanshi, "An Efficient Wormhole Prevention in MANET through Digital Signature," *Inteand Advancedrnational Journal of Emerging Technology anced Engineeringnd Adv*, vol. 2, no. 6, pp. 360-367, March 2013.

[5] Motjaba Ghanaatpisheh Sanaei, Babak Emami Abarghouei, Hadi Zamani and Miranda Dabiranzohouri, "An Overview on Wormhole Attack Detection in Ad-Hoc Network," *Journal of Theorotical and Apllied Information Technology*, vol. 5, no. 3, pp. 291-300, 30 Jun 2013.

[6] Shigang Chen and Yong Tang , "DAW : A Distributed Antiworm System," *IEEE parallel an Distributed System*, vol. 18, no. 7, pp. 893-906, July 2007.

[7] Yih-Chun, Adrian Perrig and Daavid B. Johnson, "Packet Leashes : A Defense against Wormhole Attacks in Wireless Networks," in *In Proceeding of IEEE INFOCOM*, April 2003, pp. 1976-1986.

[8] S. Capcum and I. Buttyan, "SECTOR : Secure Tracking of Node Encounters in Multihop Wireless Network," in *In Proceeding of the ACM Workshop on Security of Ad-hoc and Sensor Network*, 2003, pp. 21-31.

[9] Pushpendra Niranjan, Prashant Srivastav, Rajkumar Soni & Ram Pratap, "Detection of Wormhole using Hope-count and Time delay Analysis," *International Journal of Scientific & Research Publication*, vol. 2, no. 4, pp. 1-4, April 2012.

[10] Saurabh Gupta, Subrat Kar & S. Dharmaraha, "WHOP : Wormhole Attack Detection using Hound Packet," in *International Conference on Innovation in Information Technology*, 2011, pp. 226-231.