"An Improved Wormhole Attack Detection and Prevention Method for Wireless Mesh Networks"

Virendra Dani[1], Vijay Birchha[2]

PG Scholar, Computer Science and Engineering, S.V.C.E., Indore, India [1]

Assistant Professor, Computer Science and Engineering, S.V.C.E., Indore, India [2]

Abstract: In the wireless mesh networks, the key role is played by the routers thus most of security threats are occurred to breach routing functionalities. Therefore, number of different kinds of attacks are deployed in networks easily i.e. Black-hole, Wormhole, Gray-hole and many others. Most of the attacks are deployed in order to degrade the performance of overall networks or bypass the network traffic. Therefore the presented work is aimed to explore the issues and challenges to design a secure network communication for wireless mesh network. One of them is wormhole attack i.e. severe kind of security threats in WMN. The proposed work is locates the wormhole link in network and tries to recover the network performance during the attack conditions. Thus, the scheme detects the malevolent nodes and prevents formation of wormholes. The Proposed mechanism based on two phase solution. In first phase the threshold value is computed using the different routing scenarios, the threshold value usage the network transmission delay in network and in second phase the threshold value is used to identify the malevolent link in the network. The implementation of the proposed concept is provided using the Ad-hoc on Demand Distance Vector routing protocol modification in network simulator 2 i.e. NS-2.

Keywords: WMN, AODV, Attacks, NS-2, Security, Routing.

I. INTRODUCTION

In the domain of communication the traditional wired networks are wear out due to the wireless technology. The wireless technology is low cost, low maintenance, and rapid installable. Thus a number of indoor and outdoor network technologies are developed to serve according to the need of services. Among a number of different technologies the wireless mesh network is one of the essential technologies. The wireless mesh networks (WMNs) are very useful because of its self-healing and self-configuring nature. That can be used for cellular mobile networks, enterprise networks, community networks; etc. The WMN is a combination routers and clients, where routers establish a wireless connectivity to the clients. WMN have several advantages such as low-setup cost, increased coverage and also provides flexible and reliable services [1]. Due to its mobile and wireless nature the normal communication can be interrupted by the malicious attackers such as Wormhole, Black-hole, Gray-hole and others. These attacks not only affect the services of the network it also affect the network performance of network significantly.

II. BACKGROUND

This section describes the key features of different routing protocols that are supporting the Mobile ad hoc network such as DSDV, OLSR, DSR, and AODV protocols. That also describes the particular parameters that are used for implementing protocols.

Destination-Sequenced Distance Vector (DSDV)

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. The improvement made to the Bellman-Ford algorithm includes freedom from loops in routing tables by using sequence numbers. It was developed by C. Perkins and P. Bhagwat in 1994. The DSDV protocol can be used in mobile ad hoc networking environments by assuming that each participating node acts as a router. Each node must maintain a table that consists of all the possible destinations. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle. Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks [2].

Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks and is based on a method known as source routing. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. Except that each intermediate node that broadcasts a route request packet adds its own address identifier to a list carried in the packet. The destination node generates a route reply message that includes the list of addresses received in the route request and transmits it back along this path to the source. Route maintenance in DSR is accomplished through the confirmations that nodes generate when they can verify that the next node successfully received a packet. These confirmations can be link-layer acknowledgements, passive acknowledgements or network-layer acknowledgements specified by the DSR protocol. However, it uses source routing instead of relying on the routing table at each intermediate device. When a node is not able to verify the successful reception

DOI 10.17148/IJARCCE.2015.412113

of a packet it tries to retransmit it. When a finite number of retransmissions fail, the node generates route error message that specifies the problematic link, transmitting it to the source node [3].

Ad-hoc on Demand Distance Vector (AODV)

AODV is essentially a combination of both DSR and DSDV. It borrows the basic on-demand mechanism of Route Discovery and Route Maintenance from DSR, plus the use of hop-by-hop routing, sequence numbers, and periodic beacons from DSDV [4].

In order to maintain routes, AODV normally requires that each node periodically transmit a HELLO message, with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbour is taken as an indication that the link to the neighbour in question is down. Alternatively, the AODV specification briefly suggests that a node may use physical layer or link layer methods to detect link breakages to nodes that it considers neighbours [4].

III. LITERATURE SURVEY

Packet Leashes

The main scheme is that by authenticating either an extremely accurate timestamp or place information joint with a slack timestamp, a receiver can decide if the packet has traversed an impractical distance for the definite network technology used. Packet leashing was added to each packet on each link to confine the transmission distance of the packet. Two types of packet leashes could be added into the packet. One is geographical leash in which the sender put up its own position and sending time into the packet, the receiver will compute the maximum distance between the sender and itself based on its own position and receiving time. If the distance exceeds the transmission range, the packet will be discarded. The other type is temporal leash. This mechanism assumes that the utmost transmission hustle of radio signal is the speed of light, thus the ending time of a packet can be estimated using the maximum transmission range and the speed of light. The ending time of the packet is inserted into the packet, and then the receiver can ensure whether the received packet has expired or not based on its receiving time. A disadvantage of packet leashes is that it requires extremely tight time synchronization and GPS [5].

TTM

Van Tran and Xuan Hung proposed a transmission time based mechanism (TTM) for detecting wormhole attacks. This method calculates each Round Trip Time (RTT) between two consecutive nodes along the route. Each node in the path will estimate RTT between it and the destination, this value will be sent back to the source. A wormhole will be recognized based on the detail that transmission time between two wormhole nodes is considerably larger than that between two genuine consecutive nodes. Although Time based protocols have advantages of providing ease of use, low division overhead and the high efficiency of the proposed mechanism. But still they need some approximations as the node that is in charge of detection has to account for the processing and propagation delay times. More significantly, these protocols are unable to detecting out-of-band physical layer wormholes because a packet suffers only the propagation delay which could be limited by for wormholes using high-speed links [6].

Directional Antenna

Hu and Evans suggested a solution via a supportive protocol in which directional information is pooled among nodes to avoid wormhole attack. In this, which all nodes are equipped with directional antennas where nodes uses precise ‘sectors’ of their antennas are communicate to each other. Each pair of nodes has to examine the direction of received signals from its neighbor. Therefore, the neighbor relation is confirming only if the directions of both pairs match. This process does not required clock synchronization and position information but it requires extra hardware [7].

SECTOR

Capkun et al. introduce a new method which also needs a specialized hardware and utilize end to end packet leashes. The method takes into account the speed of the transmission among the two nodes. They presented a new protocol named “**SEC**ure **T**racking **O**f Node Encounte**R**s in Multi-hop Wireless Networks” i.e. SECTOR, although it doesn’t need any clock synchronization and position information, by using Mutual Authentication with Distance-Bounding (MADB), though it needs accurate calculation of the distance and needs GPS coordinates of all node. MADB Protocol is used for distance estimation. Node X can estimate the distance to a node Y based on the speed of data transmitted between them. Every node uses a particular hardware that enables quick sending of one-bit challenge messages without CPU participation to reduce all possible processing delays. By using the time of flight, X identify whether or not Y is a neighbour. This technique is partial by the limitations of the GPS technology [8].

Graph Theoretical Based Approach

Lazos and Poovendran proposed Localization based method a “graph theoretical” approach to wormhole attack prevention. The whole procedure is based on the use of limited location-aware guard nodes (LAGNs) which are in the well-known location and initiation and achieved through GPS receivers. LAGNs use "local broadcast keys" that are legitimate only between direct one hop neighbors. In order to sense wormhole attack, it is not possible to decrypt a message encrypted with a local key – encrypted with the pair-wise key. Thus during the key generation, method used hashed messages from LAGNs to detect wormholes. A node can detect definite inconsistencies in messages from different LAGNs if a wormhole is present. In the absence of wormhole, a node is unable to have the sense of hearing two LAGNs that are away, and are not able to hear the similar message from one guard double [9].

Digital Signature Approach

In this mechanism, a key based method for preventing wormhole attack in wireless mesh network, planned method relies on digital signature and averts structure of

DOI 10.17148/IJARCCE.2015.412113

Wormholes throughout route detection procedure and it is intended for an on command hop-by-hop routing procedure. Here not requires additional or specialized hardware [10].

DELPHI

To avoid the need of synchronized clocks, positioning device and other special hardware Chiu et al. proposed a new technique is DELPHI i.e. **DEL**ay **P**er **H**op **I**ndicator that uses delay as a parameter. The detection method uses the delay/hop value for detecting wormhole attacks. In this Delphi collects information and perform detection at sender and obtain delay and hop count information. When the detection is initiated, the sender broadcast a request message to the receiver, and receiver replies all the request messages received. In this way sender can obtain the information of some disjoint paths to the receiver. By comparing the Delay/Hop values among these disjoint paths, a wormhole can be identified. This method has two phases: (1). Delay and hop count information is collected, (2). the sender analysis the information obtain in the first phase to detect there is any wormhole attack [11].

WAP

Choi and Kim presented Wormhole Attack Prevention algorithm (WAP) is a neighbour monitoring based method. All the nodes will observe its neighbor's behavior when they send RREQ messages to the destination with the assist of neighbor list. If the source does not get RREP message with in a wormhole prevention timer (WPT), it can sense the presence of wormhole. Once wormhole is detected, source node records them in its wormhole node list. WAP can able to detect both the hidden and exposed attacks with no requiring special hardware. This scheme does not fully support DSR because it is based on end-to-end signature verification of routing packets [12].

LITEWORP

Khalil et al presented LiteWorp, which assumes the existence of an attack-free environment before the wormhole attacks are launched, a lightweight protocol called LITEWORP to detect thee malicious nodes and remove the wormhole attacks in Ad-Hoc networks .This proposed protocol uses secure two hop neighbour discovery and information about the whole traffic to detect the malicious nodes which are part of the wormhole attack. In LITEWORP, they can take advantage of two-hop, rather than one-hop. This information can be exploited to detect wormhole attacks. These nodes also observe their neighbors' behavior to determine whether data packets are being properly forwarded by the neighbor. This technique isolates the malicious nodes and provides the secure network for future routing [13].

MDS-VOW

Wang et al. proposed a Multi-Dimensional Scaling-Visualization of Wormhole (MDS-VOW) procedure which used to detection of wormhole attack in wireless network. In this scheme using the received signal strength, each node measures the distance to its neighbour. Based on these measurements, base station computes the physical topology of the network. It is observed that the network with malevolent nodes has diverse visualization from that with usual nodes. In absence of wormholes, topology should be more or less flat, where as in their occurrence 'string' pulling different ends of network are seen. It recreates the layout of the sensors using multidimensional scaling scheme. The anomalies, which are introduced by the false connections through the wormhole, will turn the reconstructed surface to pull the sensors that are far away to each other. Therefore, MDS-VOW could place the wormhole connections. In MDS-VOW, all sensor nodes are necessary to send their neighbour lists to the base station [14].

IV. WOEMHOLE ATTACK

Wormhole attack is a particular type of internal attack, where malevolent nodes in the network plan to establish an imaginary channel between them. This channel can be an out-of-band high-speed communication link or can employ in-band tunnelling approach to bypass intermediate nodes. This wormhole link is typically established between two colluding nodes located far away in the network. Once recognized, the wormhole captures a lot of traffic as it advertises much better link metric than any other paths in the network. The wormhole nodes can then initiate various kinds of denial of service (DoS) attacks that strictly affect the routine of the network. It is very hard to detect this kind of attack as the nodes involved in the network action form genuine part of the network and just cryptographic mechanisms cannot avert such kind of attack [10].

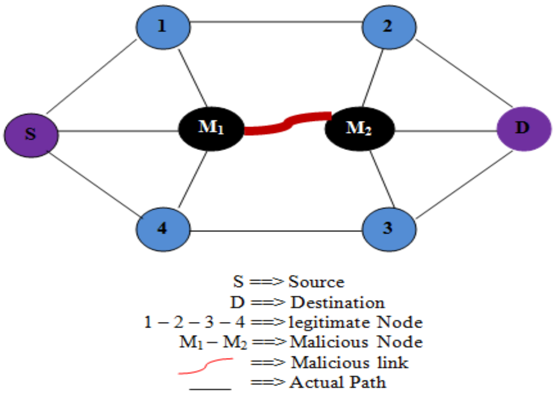

Figure 1 Wormhole Attack

V. PROPOSED SYSTEM

In networking devices, transmission of data between sources and destinations being happened through routing option. Thus, when network functionalities is discover communication path, this path can adopt new nodes and can leave previous nodes. So, in this scenario a malicious node can also join the network and harm the basic functioning of the networks. Therefore, security is key essential point for path between source and destination is required to build up

i. Threshold computation
ii. Detection
iii. Prevention

In first phase of the solution the decision making threshold is developed with the help of normal network conditions. Further the use of threshold is performed for detection of wormhole containing link. After locating the link the prevention is applied for discarding the malicious path for communication. All the phases of the solution are described as:

i. Threshold Estimation

In first phase a simple mesh network is created and using different communication scenarios the data is transmitted across the network. During the communication the numbers of hops are counted. Additionally the time to travel for the network is measured. For computation the time to travel is denoted by T_{time} and the number of hop count is denoted using h_c. Because the transmitter and receiver is obtain a route by Broadcasting RREQ and RREP messages the total RTT is estimated using the following formula.

$$RTT = \frac{T_{time}}{h_c}$$

And after the RTT computing N number of scenarios are repeated. And an average value is estimated for threshold development. Here the threshold value is denoted using α_{th} and computed as follows:

$$\alpha_{th} = \frac{1}{N}\sum_{i=1}^{N} RTT$$

After computing the threshold value α_{th} the detection process is initiated.

ii. Detection

In this phase the malicious link is discovered therefore the entire process can be understood by the route discovery phase. First the sender transmits the RREQ (route request packet) to the receiver node. During this process each node maintains a table for one hop neighbour. That contains the average time to travel α_{th} and the time for hop last hop information. When the sender receives the acknowledgment from the different sources then the table is compared with the obtained threshold and decided is route malicious or not.

iii. Prevention

If the last hop RTT is less the α_{th} then the route is not malicious else that can be involved with the malicious nodes or route. Additionally the table entry is labelled as the malicious.

Proposed algorithm

2-Phase SRM Algorithm

The entire process of the solution development is described using the summarized step of algorithm and described in two different algorithms first for creating the threshold and second for detection and prevention. The given table 1 contains the algorithm for computing the threshold value and in table 2 the detection process of malicious path is reported.

Table 1 Threshold Estimation

```
Algorithm 1: Threshold Estimation
The algorithm works on ideal conditions for finding the decision making threshold
1: Initialize the network with ideal conditions
2:Sender send RREQ message to destination
3:Wait for replay if RREP received
4:Compute the RTT using following formula
        $RTT = \frac{T_{time}}{h_c}$
5:Compute the threshold by repeating the RTT computation N times using formula
        $\alpha_{th} = \frac{1}{N}\sum_{i=1}^{N} RTT$
6. Broadcast the $\alpha_{th}$ to entire network
```

Table 2 Detection and Prevention

```
Algorithm 2: Detection and prevention
1: Sender initiate the route discovery using RREQ message
2: Receiver acknowledged with RREP message
3: Each sender put the transmission time when packet send i.e. $T_{transmission}$
4: When receiver receive the packet record the receiving time i.e. $T_{receive}$
5: Compute time difference using
        $\Delta_{time} = T_{receive} - T_{transmission}$
6: if( $\Delta_{time} \leq \alpha_{th}$ ) then
7:Make entry for previous node as legitimate
8: else
9: if( $\Delta_{time} > \alpha_{th}$ )then
9:Make entry with last hop as malicious
10: end if
```

VI. IMPLEMENTATION

This section provides the details about the experiments performed on the developed networking system.

A. simulation setup

To prepare and design the desired simulation model of communication the below given network parameters are listed in table 3.

Table 3 Simulation Parameters

PROPERTIES	VALUE
(Simulation Area) Dimension	750×550
Traffic Model	CBR
MAC Protocol	802.11
Number of Nodes	16
Channel Type	Wireless Channel
Radio Propagation Model	Two Ray Ground Model
Routing Protocol	AODV
Simulation Time	20.0 Sec
Number of Wormholes	2

B. Simulation Scenario

In order to perform the experiments the following different scenarios are prepared for simulation and network performance evaluations.

1. **Simulation under AODV Routing Protocol with Wormhole Attack:** in this network simulation the network is configured with 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.

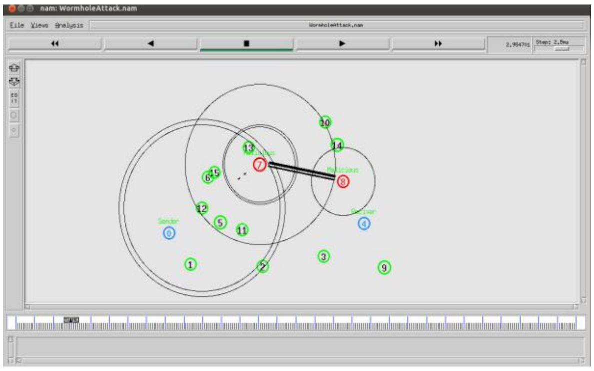

Figure 2 Networks under Attack

2. **Simulation for Proposed Method under AODV Routing Protocol with Attack Prevention:** n this simulation the proposed secure routing protocol is implemented in the network simulator 2 with the similar configuration as the other 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 estimated by result analysis.

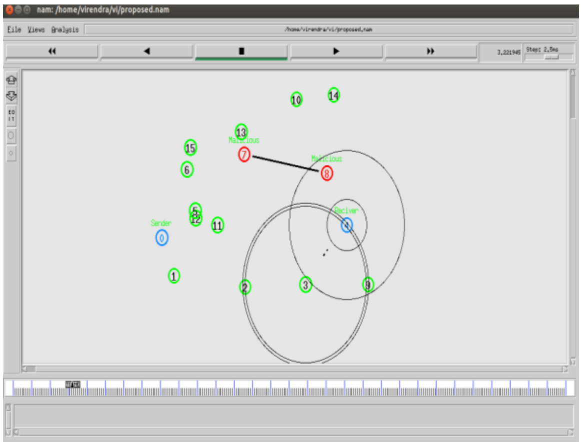
nam: /home/virendra/vi/proposed.nam
File Views Analysis
/home/virendra/vi/proposed.nam
Sender
Receiver
Malicious
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Figure 3 Proposed Method

VII. RESULTS ANALYSIS

Graphs are plotted and concluded that proposed scheme has improve throughput value and packet delivery ratio also reduces end to end routing delay.

1. End to end delay

End to end delay on network refers to the time taken for a packet to be transmitted across a network from source to destination device.

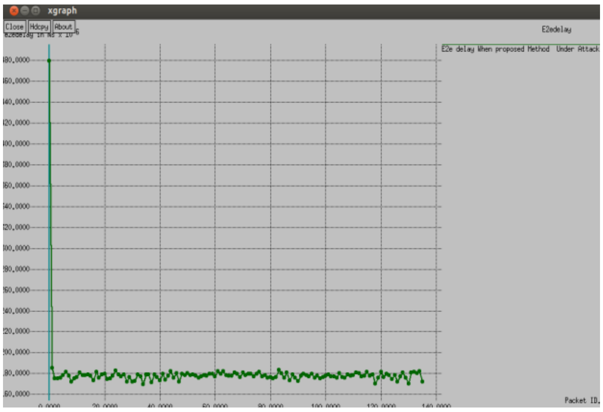

Figure 4 End-to-End Delays

In this diagram the X-axis shows the node ID available in network simulation and the Y-axis shows the corresponding end to end delay in terms of milliseconds. The performance of the proposed technique is simulated via green line.

2. Packet Delivery Ratio

Packet delivery ratio provides information about the performance of any routing protocols, where PDR is estimated using the formula given

$$\text{PacketDeliveryRatio} = \frac{\text{TotalReceivedPackets}}{\text{TotalSentPackets}}$$

In this diagram the X-axis shows the simulation time of the network and the Y-axis shows the packet delivery ratio in terms of percentage.

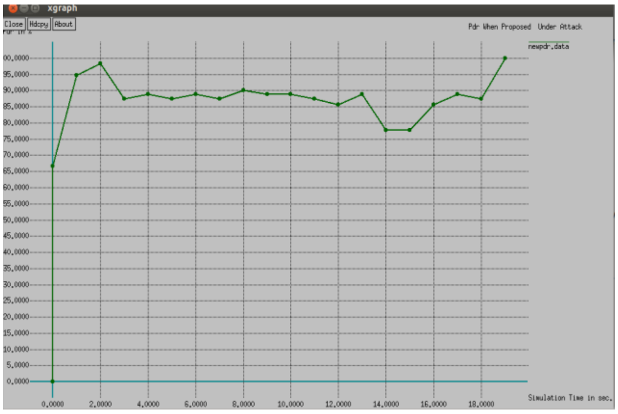

Figure 5 Packet Delivery Ratio

3. Throughput

Network throughput is the usual rate of successful delivery of a message over a communication medium. This data may be transmit over a physical or logical link, or pass by a certain network node. The throughput is calculated in terms of bit/s or bps, and occasionally in terms of data packets per time slot or data packets per second.

Received data = (bytes/ time)* 8/1000000
througput_in_mbps = bytes_recv_per_unit_of_time* 8/1000000

.In this diagram the X-axis shows the Simulation time in sec of the nodes and the Y-axis shows the throughput of the network in terms of KBPS (kilobyte per second).

DOI 10.17148/IJARCCE.2015.412113

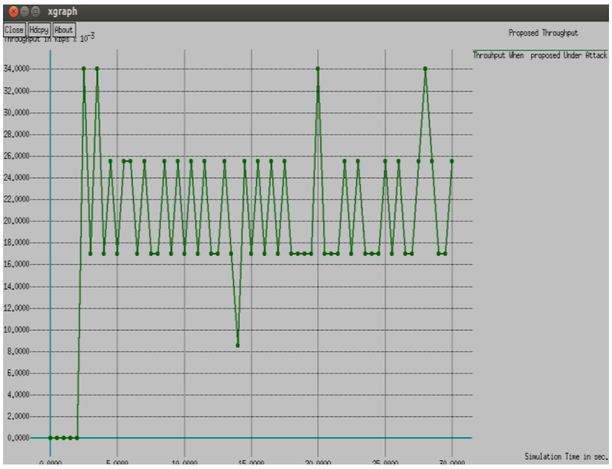

Figure 6 Network Throughput

VIII. CONCLUSION AND FUTURE WORK

Wireless mesh networks are vulnerable to wide range of security attacks because of their deployment in an open and unprotected environment. This research work investigates different wormhole detection techniques, examines various existing methods to find out how they have been implemented to detect wormhole attacks. Each technique has its own strength and weaknesses. We presented an efficient mechanism to prevent Wormholes on WMN. The proposed mechanism is simplistic and does not rely on additional like GPS systems. The implementation of the proposed method is provided using the NS2 environment. For performance analysis is performed using the generated network traces. The performance of the implemented routing method is estimated in terms of packet delivery ratio, throughput, and end to end delay.

Future Work

The proposed technique can be extended by using different scenarios in networks.

1. The given technique is a parameter based technique which utilizes the network parameters for finding the malicious link thus that method can be extended for implementing security for other attacks based on the network parameter selection.
2. The Future Scheme of the whole research is to extend the proposed scheme to other protocols rather than the AODV protocol.

The method is effective and efficient during attack conditions thus the method is used for further for improving the network security in various wireless ad hoc networks such as VANET, WSN and others.

ACKNOWLEDGMENT

I would like to honestly thank **Mr. Vijay Birchha**, Assistant Professor, dept. of Computer Science, SVCE, for his valuable suggestions and supervision. I would also like to thank to our allied faculty members for their remarks and motivations.

REFERENCES

[1] IAN F. AKYILDIZ, XUDONG WANG, "A Survey on Wireless Mesh Networks", IEEE Radio Communications, September 2005, 0163-6804/05/$20.00 © 2005 IEEE

[2] S. A. Ade and P. A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad-Hoc Networks", International Journal of Information Technology and Knowledge Management, Volume 2, No. 2, pp. 545-548, July-December 2010

[3] Nikhil Kumar, Vishant Kumar and Nitin Kumar, "Comparative Study of Reactive Routing Protocols AODV and DSR for Mobile Ad hoc Networks", International Journal of Computer Science and Information Technologies (IJCSIT), Volume 5, pp.6888-6891, 2014.

[4] M. S. karthikeyan, K. Angayarkanni, and Dr. S. Sujatha, "Throughput Enhancement in Scalable MANETs using Proactive and Reactive Routing Protocols", In Proceedings of the International Multi Conference of engineering and computer science, Volume 2, March 2010.

[5] 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.

[6] P. V. Tran, L. X. Hung, Y. Lee, S. Lee, and H. Lee, TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-Hoc Networks, In Proceeding of 4th IEEE CCNC, pp. 593-598, Las Vegas, USA, Jan. 2007.

[7] 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.

[8] S. Capkun, L. Buttyan and J.P., Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32, New York, USA, 2003.

[9] L. Lazos and R. Poovendran, "Serloc: Secure range-independent localization for Wireless Sensor Networks", In Proceedings of the ACM Workshop on Wireless Security, pp. 21−30, October 2004.

[10] P Subhash and S Ramachandram, "Preventing Wormholes in Multi-hop Wireless Mesh Networks", Third International Conference on Advanced Computing & Communication Technologies, pp. 293-300, 2013.

[11] H.S. Chiu and K.S. Lui, "DELPHI: Wormhole Discovery Device for Ad-hoc Wireless Network", 1st International Symposium on Wireless Pervasive Computing, pp. 6–11, Phuket, Thailand, 16-18 January 2006.

[12] C. Sun, K. Doo-young, L. Do-hyeon & J. Jae-il, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," In Proceeding of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), pp. 343-348, 2008.

[13] I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multi-hop Wireless Networks, International Conference on Dependable Systems and Networks, pp.612–621, 2005.

[14] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks", In Proceedings of the 3rd ACM workshop on Wireless security, October 01, Philadelphia, PA, USA, 2004.

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

DOI 10.17148/IJARCCE.2015.412113