ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

Wormhole Attack Detection in Mobile Ad Hoc Networks

Ajay Prakash Rai, Vineet Srivastava, Rinkoo Bhatia
Institute Of Technology and Management, Gwalior (M.P), India

Abstract*— A Mobile Ad hoc Network (MANET) is a collection of self configurable mobile node connected through wireless links. In MANET nodes which are within the range of each other can connect directly where as nodes which are not in the vicinity of each other rely on the intermediate node for communication. Each node in MANET can work as a sender, receiver as well as router. Communication in the network depends upon the trust on each other. In wormhole attacks, one malicious node tunnels packets from its location to the other malicious node. Such wormhole attacks result in a false route with fewer. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them. It is difficult to detect wormhole attacks because malicious nodes impersonate legitimate nodes The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In this paper, we 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 able to provide in establishing a method to reduce the rate of refresh time and the response time to become more faster.

Index Terms— **Ad Hoc Network, Sensor Network, Wormhole Attack, Defending Mechanism.**

I. INTRODUCTION

MANET's, A Collection of Mobile Hosts with Wireless Network Interfaces Form a Temporary Network without the Aid of Any Fixed Infrastructure or Centralized Administration. These Nodes, Such as Laptop Computers, Pdas and Wireless Phones, have a Limited Transmission Range. Hence, Each Node has the ability to Communicate Directly with another Node and Forward Messages to Neighbors until the Messages Arrive at the Destination Nodes. Security of Such Network is a Major Concern [3]. The Open Nature Of The Wireless Medium Makes It Easy For Outsiders To Listen To Network Traffic Or Interfere With It. These Factors Make Sensor Networks Potentially Vulnerable To Several Different Types Of Malicious Attacks. These Malicious Nodes Can Carry Out both Passive and Active Attacks against the Network. In Passive Attacks A Malicious Node Only Eavesdrop Upon Packet Contents, While In Active Attacks It May Imitate, Drop Or Modify Legitimate Packets [1]. A Typical Example of Particularly Devastating Security Active Attack Is Known As a Wormhole Attack. In Which, A Malicious Ease Of Use Node Captures Packets From One Location In The Network, And Tunnels Them To Another Malicious Node At A Distant Point, Which Replays Them Locally. The Wormhole Attack Can Affect Network Routing, Data Aggregation And Clustering Protocols, And Location-Based Wireless Security Systems. Finally, The Wormhole Attack Can Be Launched Even without Having Access To Any Cryptographic Keys Or Compromising Any Legitimate Node In The Network In [2].The Rest Of This Paper Is Organized As Follows; Section 3 Presents The Significance Of Wormhole Attack Nature; Section 4 Studies Analysis Of Detection And Countermeasure Of Wormhole Attacks And Presents Discussion And Summary. In Section 5 Presents Our Proposed Model and In Section 6 Followed By the Simulation Setup and Results. Section 7 Concludes the Paper.

II. RELATED WORK

In order to avoid the problem of using special hardware, a Round Trip Time (RTT) mechanism [5] is proposed by Jane Zhen and Sampalli. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node A to Route Reply (RREP) message receiving time from a node B. A will calculate the RTT between A and all its neighbors. Because the RTT between two fake neighbors is higher than between two real neighbors, node A can identify both the fake and real neighbors. In this mechanism, each node calculates the RTT between itself and all its neighbors. This mechanism does not require any special hardware and it is easy to implement; however it can not detect exposed attacks because fake neighbors are created in exposed attacks. The Delay per Hop Indicator (DelPHI) [13] proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to find every available disjoint route between a sender and a receiver. Then, the delay time and length of each route are calculated and the average delay time per hop along each route is computed. These values are used to identify wormhole. The route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both types of wormhole attack; however, it cannot pinpoint the location of a wormhole. Moreover, because the lengths of the routes are changed by every node, including wormhole nodes, wormhole nodes can change the route length in a certain manner so that they cannot be detected. Packet Leash [4] is an approach in which some information in added to restrict the maximum transmission distance of packet. There are two types of packet leashes: geographic

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

leash and temporal leash. In geographic leash, when a node A sends a packet to another node B, the node must include its location information and sending time into the packet. B can estimate the distance between them. The geographic leash computes an upper bound on the distance, whereas the temporal leash ensures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes must have tight time synchronization. The maximum difference between any two nodes' clocks is bounded by Δ, and this value should be known to all the nodes. By using metrics mentioned above, each node checks the expiration time in the packet and determine whether or not wormhole attacks have occurred. If a packet receiving time exceed the expiration time, the packet is discarded. Unlike Packet Leash, Capkun et al. [7] presented SECTOR, which does not require any clock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD). Node A estimates the distance to another node B in its transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of flight, A detects whether or not B is a neighbor or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash.

III. OVERVIEW OF WORMHOLE ATTACK

This section describes wormhole attacks nature and problem statement. A wormhole attack is a particularly severe attack on MANET routing where two attackers connected by a high-speed off-channel link called the wormhole link. The wormhole link can be established by using a network cable and any form of "wired" link technology or a long-range wireless transmission in a different band. The end-point of this link (wormhole nodes) is equipped with radio transceivers compatible with the ad hoc or sensor network to be attacked. Once the wormhole link is established, the adversary record the wireless data they overhear, forward it to each other, and replays the packets through the wormhole link at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go though them. In general, ad hoc routing protocols fall into two categories: proactive routing protocols that rely on periodic transmission of routing updates, and on-demand routing protocols that search for routes only when necessary[4]. A wormhole attack is equally dangerous for both proactive and on-demand protocols. It should be nodded that wormholes are dangerous by themselves, even if attackers are diligently forwarding all packets without any disruptions, on some level, providing a communication service to the network. With wormhole in place, affected network nodes do not have a true picture of the network, which may disrupt the localization-based schemes, lead to the wrong decisions, etc. Wormhole can also be used to simply aggregate a large number of network packets for the purpose of traffic analysis or encryption compromise. Finally, a wormhole link is simply unreliable, as there is no way to protect what the attackers can do and when. Simply put the wormholes are compromising network security whether they are actively disrupting routing or not.

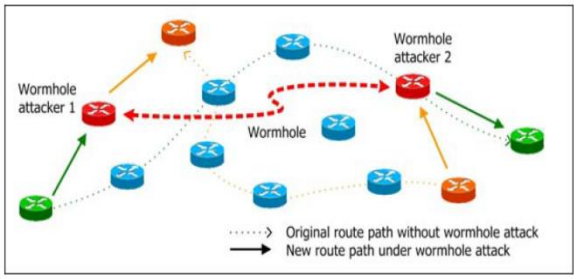


Fig 1: Wormhole Attack in MANET

IV. DETECTING WORMHOLE ATTACK

In this section, we introduce the notion of a packet leash as a general mechanism for detecting and thus defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed of light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows.

A. Packet Leashes

Packet Leash in [8], [15], [16] is a mechanism to detect and defend against wormhole attacks. The mechanism proposes two types of leashes for this purpose: Geographic and Temporal. In Geographic Leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to traverse the path. The receiver can use this distance anytime information to deduce whether the received packet passed through a wormhole or not. In Temporal Leashes, all nodes are required to maintain a tightly synchronized clock but do not rely on GPS information. When temporal leashes are used, the sending node append the time of transmission to each sent packet *ts* in a packet leash, and the receiving node uses its own packet reception time *tr* for verification. The sending node calculates an expiration time *te* after which a packet should not be accepted, and puts that information in the leash. To prevent a packet from traveling farther than distance L, the expiration time is set to:

$$te = ts + (L/C) - \Delta \qquad (1)$$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

Where *c* is the speed of light and Δ is the maximum clock synchronization error. All sending nodes append the time of transmission to each sent packet. The receiver compares the time to its locally maintained time and assuming that the transmission propagation speed is equal to the speed of light, computes the distance to the sender. The receiver is thus able to detect, whether the packet has travelled on additional number of hops before reaching the receiver. Both types of leashes require that all nodes can obtain an authenticated symmetric key of every other node in the network. These keys enable a receiver to authenticate the location and time information in a received packet.

B. Time-of-flight

Another set of wormhole prevention techniques is similar to temporal packet leashes in [6], is based on the time of flight of individual packets. One possible way to prevent wormholes, as used by Capkun et al in [9] is to measure round-trip travel time of a message and its acknowledgement, estimate the distance between the nodes based on this travel time, and determines whether the calculated distance is within the maximum possible communication range. The basis of all these approaches is the following. The Round Trip Travel Time (RTT) α of a message in a wireless medium can, theoretically, be related to the distance *d* between nodes, assuming that the wireless signal travels with a speed of light *c*:

$$d = \delta * c/2 \quad (2)$$

$$\delta = 2d/c \quad (3)$$

The neighbour status of nodes is verified if *d* is within the radio transmission range *R*:

R > *d* (*d* within transmission range)

$$R > \delta * c/2 \quad (4)$$

$$\delta < 2R/c \quad (5)$$

In essence, the use of RTT eliminates the need for tight clock synchronization required in temporal leashes: a node only uses its own clock to measure time. When a de-facto standard of wireless ad hoc networks 802.11 Medium Access Control (MAC) protocol is used, such calculations are downright impossible. 802.11 impose a short wait time of 10μs Short Inter frame Space (SIFS) between the reception of a packet and sending of 802.11 acknowledgements. When 802.11 is used, transmission range *R* is generally about 300 meters. The speed of light *c* is 3×10–8 *m/s*. Then, from equation 4:

$$\delta = 2d/c = 600m/3 \times 10{-}8\ m/s$$

$$= 0.000002s = 2 \times 10\text{-}6 = 2\mu s \quad (6)$$

Therefore, the RTT is an order of magnitude smaller than the delay required by the protocol. We could, of course, account for this processing time by modifying formula 4 in the following manner:

$$\delta = 2d/c + S \quad (7)$$

Where S is SIFS (Short Inter frame Space). However, note that wormhole attackers are not limited by the rules of the network, and could send their packets without 802.11-imposed delay. Approaches based on RTT that one node sends a packet to another; the answer should arrive very shortly, ideally within the amount of time a wireless signal would travel between the nodes. If there is a wormhole attacker involved, packets end up traveling farther, and thus can not be returned within a short time.

V. PROBLEM DEFINITION

The mobile ad-hoc network, MANET, is a developing wireless technology that has been discussed in many academic research projects in the last decade. An ad-hoc network is inherently a self-organized network system without any infrastructure. Typically, the nodes act as both host and router at the same time, i.e., each node in the network can be independent and based on different hardware, but when communication is needed it serves as a data transmitting router after a route discovery procedure. So far, many routing protocols have been proposed for MANET, such as DSDV (Destination Sequence Distance Vector) , DSR (Dynamic Source Routing) and AODV (Ad-hoc On-Demand Vector) and so on. To the best of our knowledge, most previous research has focused on protocol establishment and its efficiency in MANET, but secure routing is very important, and some secure routing protocols based on DSR and AODV have been proposed in these years. Recently, a novel exploit called wormhole attack was introduced. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes. In practice, attackers can use high power antennas or a wired link, or other methods. The resulting route through the wormhole may have a better metric, i.e., a lower hop-count than normal routes. With this leverage, attackers using wormholes can easily manipulate the routing priority in MANET to perform eavesdropping, packet modification or perform a DoS (Denial of Service) attack, and so on. The entire routing system in MANET can even be brought down using the wormhole attack. In wireless network many types of attacks can be initiated but most of them are relative easy to detect because of their property of dramatically altering the network statistics but one different type of attack we consider in this thesis. it is very important when considering security issues of network, is wormhole attack, which is difficult to detect & can harm by directing important data to unauthorized nodes. During the route discovery process, a wormhole can relay route request and response messages between distant nodes, creating the appearance of shorter routes to destinations. Since the wormhole can be anywhere along a route, a source will have to detect its existence somewhere along the route when a node sets up the route (on-demand).

Proposed Method Using Performance Evaluation Multipath Algorithm:MANET, due to the nature of wireless transmission, has more security issues compared to wired environments. In this method we specifically

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

considering Wormhole attack which does not require exploiting any nodes in the network and can interfere with the route establishment process. Instead of detecting suspicious routes as in previous methods, we implement a new method which detects the attacker nodes and works without modification of protocol, using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions. The proposed work is simulated using OPNET and results showing the advantages of proposed work.

1 The steps of modeling of Proposed Algorithm

Step1. Randomly Generate a Number in between 0 to maximum number of nodes.

Step2. Make the Node with same number as transmitter node.

Step3. Generate the Route from selected transmitting node to any destination node with specified average route length.

Step4. Send packet According to selected destination and start timer to count hops and delay.

Step5. Repeat the process and store routes and their hops and delay.

Step6. Now if the hop count for a particular route decreases abruptly for average hop count then at least one node in the route must be attacker.

Step7. Now check the delay of all previous routes which involve any on node of the suspicious route. Now the node not encounter previously should be malicious let there are N such nodes.

Step8. In N == 1 then it is the attacker else wait for future sequences which shows deviation and involve only one of N nodes.

Step9. These nodes are black listed by the nodes hence they are not involved in future routes.

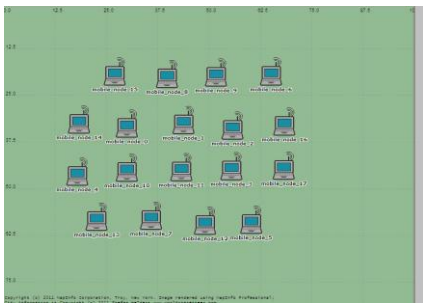
Step10. Whole process (from step1 to step9) is repeated until we didn't get the specified goal (goal can be

1. To get complete list of malicious nodes.
2. To run for specified time.
3. To run for specific number of packets etc.

VI. SIMULATION RESULTS

The simulation results from Opnet Network Modeler 14.0 with respect to the Average Hop count per route comparison and Average delays per route comparison.

Scenario 1:- Node Distribution without Wormhole Attack



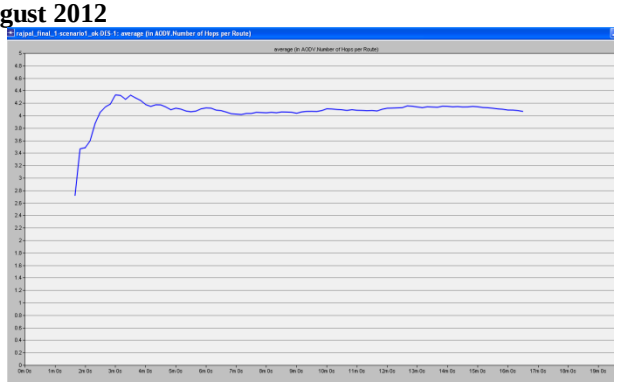


Fig2: Average Hop Count per Route in Scenario 1 without Wormhole Attack

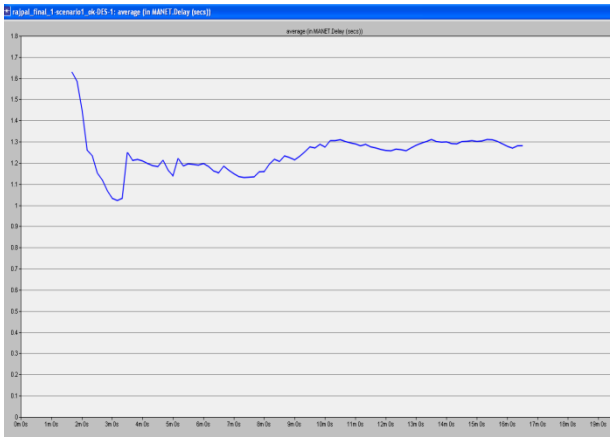
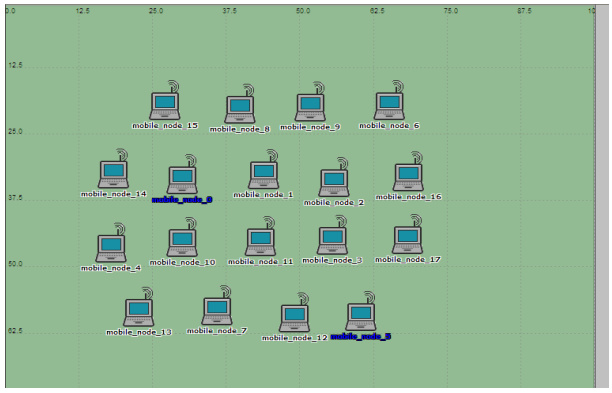


Fig3: Average Delays per Route in Scenario 1 without Wormhole Attack

Scenario 2:- Node Distribution with Wormhole Attack



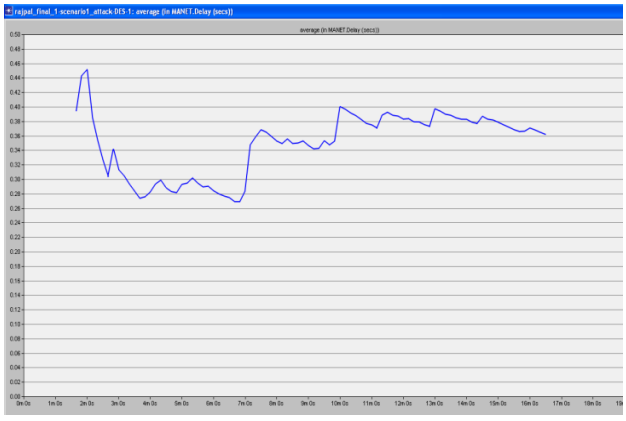


Fig4: Average Hop Count per Route in Scenario 2 with Wormhole Attack

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

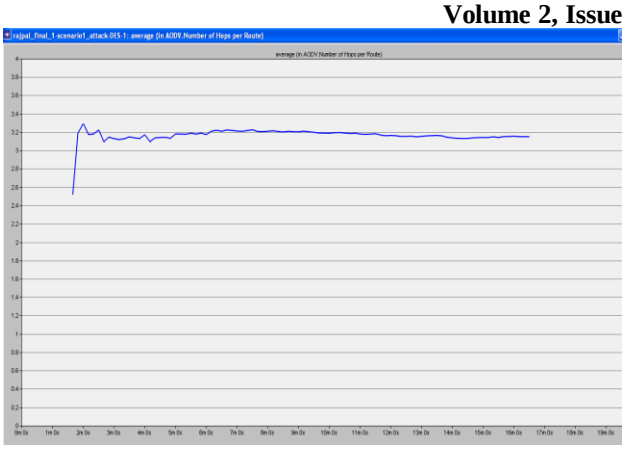


Fig5: Average Delays per Route in Scenario 2 with Wormhole Attack

Scenario 3:- Node Distribution with Wormhole Attack

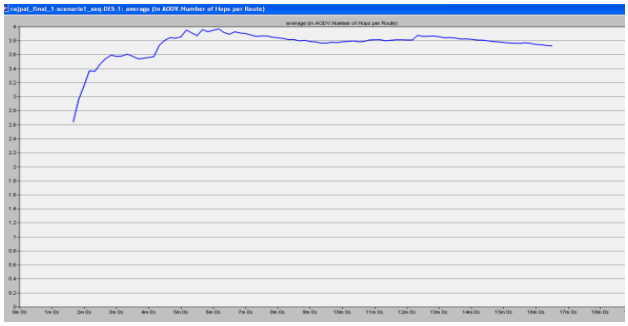


Fig6: Average Hop Count per Route in Scenario 3 with Wormhole Attack and Applied Proposed Algorithm

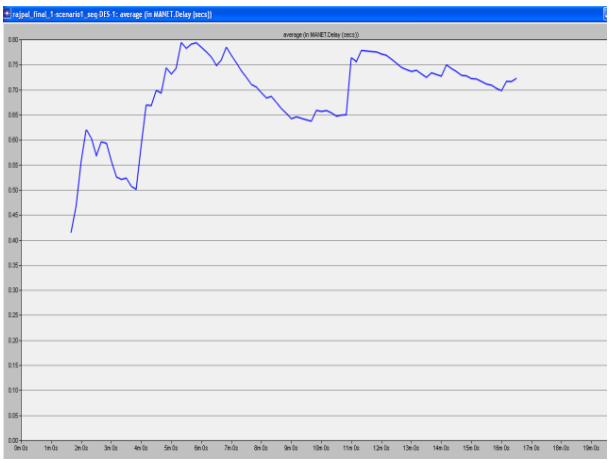


Fig7: Average Delays per Route in Scenario 3 with Wormhole Attack and Applied Proposed Algorithm

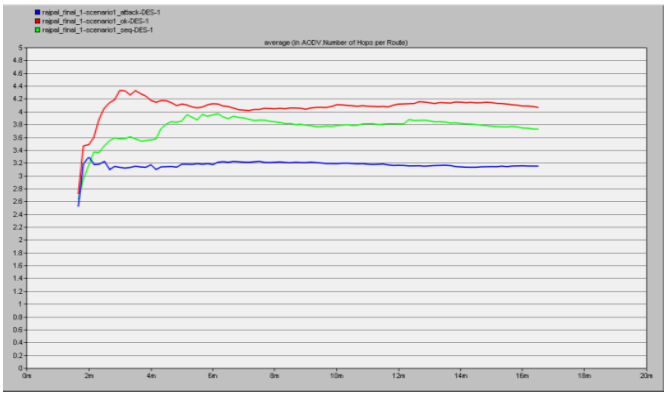


Fig8: Average Hop Count per Route Comparison

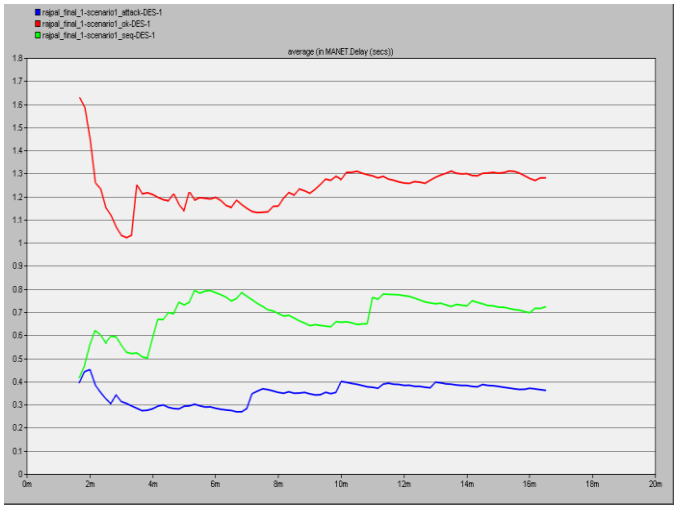


Fig9: Average Delays per Route Comparison

Attack reduces the average hop count by 20% (shown in blue) from normal condition (shown in red) which shows the selection of attaching node in route, the proposed algorithm significantly regains the hop counts by avoiding the attacker (shown in green)

Attack reduces the average delay by 75% (shown in blue) from normal condition (shown in red) which shows the shorting of route by attacking route, the proposed algorithm have much better delay which presents the elimination of attacker (shown in green).

REFERENCES

[1] R.E.Kassi, A.Chehab, and Z. Dway, "DAWWSEN: A Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks", in proceeding of the second International conference on innovations in information Technology (ITT' 05), UAE, September 2005.

[2] T. Park and K. Shin, "LISP: A Lightweight Security Protocol for Wireless Sensor Networks", in proceedings of ACM transaction on Embedded Computing systems, August 2004.

[3] Y.-C. Hu, A. Perrig, A Survey of Secure Wireless Ad Hoc Routing, Security and Privacy Magazine, IEEE, vol. 2, issue 3, pp. 28-39, May 2004.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

[4] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks.IEEE INFOCOM, Mar 2003.

[5] J. Zhen and S. Srinivas. Preventing replay attacks for secure routing in ad hoc networks. In ADHOC-NOW, LNCS 2865,

[6] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless AdHoc Networks", in proceedings of INFOCOM, 2004.

[7] S. Capkun, L. Butty´an, and J.-P. Hubaux. SECTOR: secure tracking of node encounters in multi-hop wireless networks. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), pages 21–32, Oct 2003.

[8] S. Capkun, L. Buttyan, J.-P. Hubaux, SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks, October 2003, Processing's of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks.

[9]. On the Survivability of Routing Protocols in Ad Hoc Wireless Networks, A. Baruch, R. Curmola, C. Nita- Rotaru, D. Holmer, H. Rubens, Convergence on Security and Privacy for Emerging Areas Communications, Secure Comm 2005, September2005.

[10] L. Hu, D. Evans, Using Directional Antennas to Prevent Wormhole Attacks, 14 Proceedings of the 11th Network and Distributed System Security Symposium, pp. 2003.

[11] W. Wang, B. Bhargava., Visualization of wormholes in sensor networks, Proceedings of the 2004 ACM workshop on Wireless Security, pp. 51-60, 2004.

[12] L. Lazos, R. Poovendran, and Serloc: Secure Range-Independent Localization for 21- 30, Wireless Sensor Networks, Proceedings of the ACM Workshop on Wireless Security, pp. October 2004.

[13] D. A. Maltz and D. B. Johnson and Y. Hu. The dynamic source routing protocol (DSR) for mobile ad hoc.

[14]. N. Song, L. Qian, X. Li, Wormhole Attack Detection in Wireless Ad Hoc Networks: a Statistical Analysis Approach, Parallel and Distributed Processing.

[15] Y. Hu, A. Perrig, and D. Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless AdHoc Networks", in proceedings of INFOCOM, 2004.

[16] W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Interscience, "Defending agains Wormhole Attacks in Mobile Ad Hoc Networks," Wireless Communication and Mobile Computing, January 2006.