ISSN 2250-3153

Detection of Wormhole Attack using Hop-count and Time delay Analysis

Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap

Information Technology, LNCT (RGPV) Bhopal, India

Abstract- MANET, due to the nature of wireless transmission, has more security issues compared to wired environments. In this paper we specifically considering Tunneling 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.

Index Terms- Ad hoc network, hop-count analysis, network security, Tunneling attack.

I. INTRODUCTION

The mobile ad-hoc network, MANET [1], 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) [2], DSR (Dynamic Source Routing) [3] and AODV (Ad-hoc On-Demand Vector) [4] 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 [5-7] have been proposed in these years. Recently, a novel exploit called wormhole attack was introduced [8]. In a wormhole attack, attackers "tunnel" packets to another area of the network bypassing normal routes as shown in Figure 1. 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. Its severity and influence has been analyzed in [9].

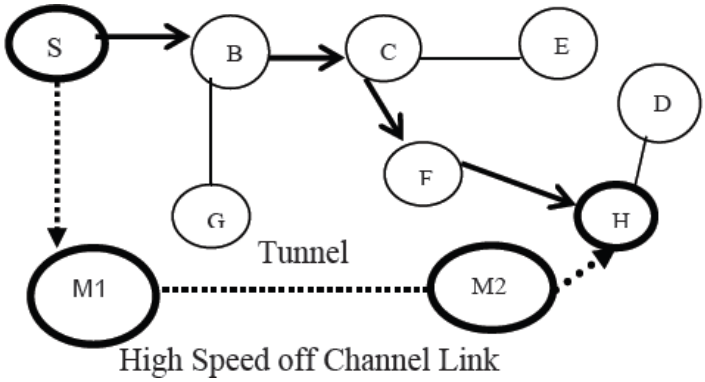

Figure 1: The wormhole attack in MANET

Mobile wireless ad hoc networks are fundamentally different from wired networks, as they use wireless medium to communicate, do not rely on fixed infrastructure, and can arrange them into a network quickly and efficiently. In a Mobile Ad Hoc Network (MANET), each node serves as a router for other nodes, which allows data to travel, utilizing multi-hop network paths, beyond the line of sight without relying on wired infrastructure. Security in such networks, however, is a great concern [1, 2, 7, 8]. The open nature of the wireless medium makes it easy for outsiders to listen to network traffic or interfere with it. Lack of centralized control authority makes deployment of traditional centralized security mechanisms difficult, if not impossible. Lack of clear network entry points also makes it difficult to implement perimeter-based defense mechanisms such as firewalls. Finally, in a MANET nodes might be battery-powered and might have very limited resources, which may make the use of heavy-weight security solutions undesirable [2, 3, 7, 8, 13]. A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network, as shown in figure 1. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid. Our method selects routes and "avoids" rather than "identify" the wormhole resulting in low cost and overhead. We propose a multipath routing protocol called Multipath Hop-count Analysis efficient protocol which does not require any special supporting hardware. Furthermore, MHA is designed to use split multipath routes, so the transmitted data is naturally split into separate route. An attacker on a particular route can not completely intercept (and subvert) our content. The rest of the paper is organized as follows: We review related works regarding wormhole attack in

Section 2. In Section 3, the proposed work. The simulations are given in Section 4, and Finally, we present our conclusions in Section 5.

II. RELATED WORK ON WORMHOLE ATTACK

In this section, we introduce the mechanism for detecting the wormhole attacks. To identifies misbehaving nodes and avoids routing through theses nodes, watchdog and pathrater is proposed in [11]. In this technique, watchdog identifies misbehavior of nodes by copying packets and maintained a buffer for recently sent packets. The overheard packet is compared with the sent packet, if there is a match then discards that packet. If the packet is timeout, increment the failure tally for the node. And if the tally exceeds the thresholds, then node will misbehave. The implementation of watchdog technique is shown in Fig.2.

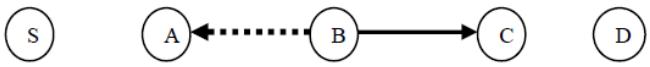

Figure 2: Watchdog implementation

In this figure, it is assumed that bidirectional communication symmetry on every link between nodes that want to communicate. If a node can receive a message from a node at time , then node could instead have received a message from node at the time will implement the watchdog. It maintain a buffer of recently sent packets and compares each overheard packet with the packet in the buffer, when forwards a packet from to with the help of , can overhear transmission and capable of verifying that has attempted to pass the packet towards . But this approach has some limitations and it is not detect the misbehaving node during ambiguous collisions, receiver collisions, false misbehavior and collusion.

The approach is used directional antenna to detect and prevent the wormhole attack [12]. The technique is assumed that nodes maintain accurate sets of their neighbors. So, an attacker cannot execute a wormhole attack if the wormhole transmitter is recognized as a false neighbor and its messages are ignored. To estimate the direction of received signal and angle of arrival of a signal it uses directional antennas. This scheme works only if two nodes are communicating with each other, they receive signal at opposite angle. But this scheme is failed only if the attacker placed wormholes residing between two directional antennas.

Statistical analysis scheme [13] is based on relative frequency of each link which is part of the wormhole tunnel and that is appears in the set of all obtained routes. In this techniques, it is possible to detect unusual route selection frequency by using statistical analysis detected and will be used in identifying wormhole links. This method do not requires any special hardware or any changes in existing routing protocols. It does not require even the aggregation of any special information, since it uses routing data that is already available to a node the main idea behind this approach resides in the fact that the relative frequency of any link that is part of the wormhole tunnel, will be much higher than other normal links.

In [14] is discussed graph theoretic model that can characterize the wormhole attack and can ascertain the necessary and sufficient conditions for the candidate solution to prevent wormhole attack. This scheme is also discussed a cryptographic based solution through local broadcast key and to set up a secure wireless ad hoc network against wormhole attacks. In this scheme, there are two types of nodes in the network named as: guards and regular nodes. Guards access uses GPS to access the location information or other localization method like secure range independent localization for wireless sensor network is presented in [15] and rebroadcast location data. Regular nodes need to calculate their location relative to the guards' beacons, thus they are able to distinguish abnormal transmission due to beacon retransmission done through the wormhole attackers. In this scheme, sender is encrypted all transmissions from local broadcast key and these information must be decrypted at the receiver end. But this scheme will be suffer the time delay to accumulate per node traveled and special localization equipment is needed to guard nodes for detecting positions.

To mitigate the wormhole attack in mobile ad hoc network, cluster based technique is proposed in [15]. In this approach clusters are formed to detect the wormhole attack. The whole network is divided into clusters. These clusters can either be overlapped or disjoint. Member nodes of cluster pass the information to the cluster head and cluster head is elected dynamically. This cluster heads maintains the routing information and sends aggregated information to all members within cluster. In this scheme, there is a node at the intersection of two clusters named as guard node. The guard node has equipped with power to monitor the activity of any node and guard the cluster from possible attack. The network is also divided into outer layer and inner layer. The cluster head of outer layer is having the responsibility of informing all nodes of the inner layer about the presence of the malicious node.

To prevent and detect the wormhole attack most common approach is discussed in [1] and [13], known as packet leashes mechanism. In this paper, they are presented two types of leashes: geographic leashes and temporal leashes also presented an authentication protocol. The authentication protocol is named as TESLA [13] with instant key disclosure and this protocol, for use with temporal leashes. In, geographic leashes each node access GPS information and based on loose clock synchronization. Whereas temporal leashes require much tighter clock synchronization (in the order of nanoseconds), but do not tightly depend on GPS information and temporal leashes that are implemented with a packet expiration time. The observation of this scheme is geographic leashes are less efficient than temporal leashes, due to broadcast authentication, where precise time synchronization is not easily achievable.

Other temporal leashes wormhole prevention technique is discussed in [13] based on time of flight of individual packets. This scheme is to measure round-trip travel time with its acknowledgment. This technique is used merkle hash tree and hash chains as explained in TESLA.

An efficient detection method known as delay per hop indication (DelPHI) for wormhole attack prevention is discussed in [14]. The protocol is developed for hidden wormhole attack and exposed wormhole attack. In this scheme, sender will check whether there are any types of malicious nodes presented in the

routing path by that they will receive and implement the wormhole attacks. This scheme will not require clock synchronization, position information of nodes and any special types of hardwares. Pathrater technique [11] calculates path metric for every path. By keeping the ratings of each node in the network, the path metric is calculated by using the node rating and connection reliability which is obtained from previous experience. Once the path metric has been calculated for all accessible paths, Pathrater will select the path with the highest metric. The path metrics would enable the Pathrater to select the shortest path. Thus it avoids routes that may have misbehaving nodes.

III. PROPOSED WORK

We have performed the simulation of the proposed scheme in Opnet Network Modeler 14.0 to prove practical efficiency of the scheme; the physical parameter considerations are same as taken in mathematical modeling. The steps of modeling in FSM (Finite State Machine) of Proposed Algorithm are as follows:

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.

IV. SIMULATION ANALYSIS AND RESULT

For the simulation we have created node models, process models, & packet models, we also used some predefined node models from library. The details of models with their technical parameters are as follows

Total Nodes = 50
Infected node=6
Packet size = 1024 bits constant
Applying protocol=DSDV
Packet inter arrival time = 1sec. constant
Data Rate = 11 Mbps.
Area = 20 square Km.
Destination Address = Random.
Modulation = BPSK
Antenna = Omni Directional

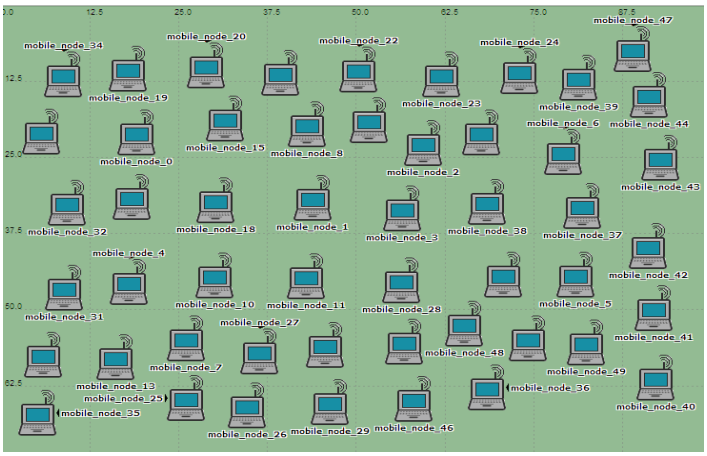

Figure: 4.1 node distribution without worm hole attack

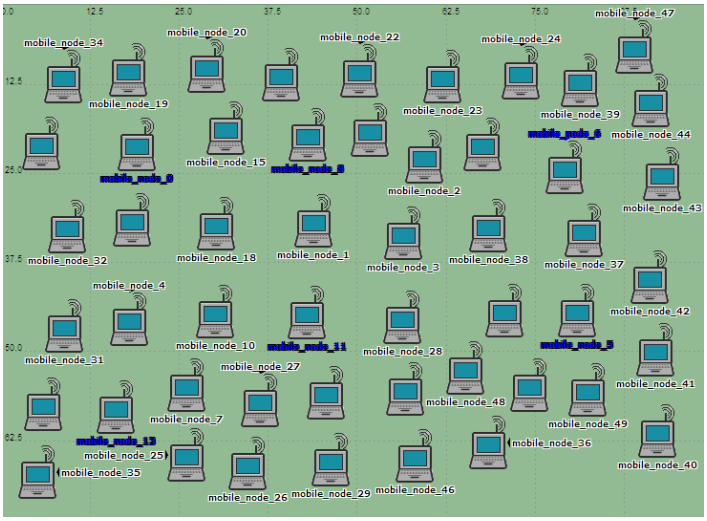

Figure: 4.2 node distribution with 6 wormhole infected node

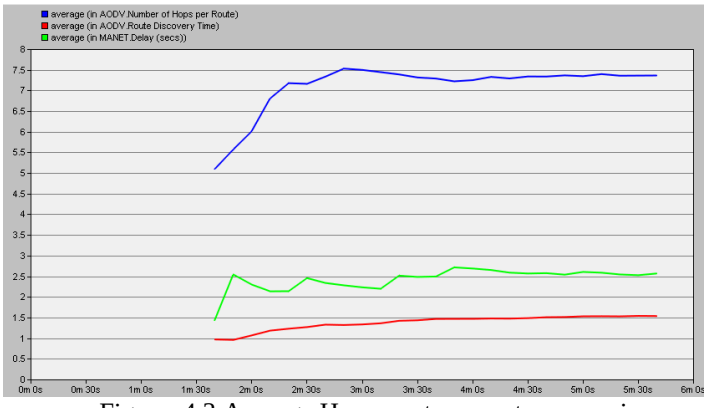

Figure: 4.3 Average Hop count per route comparison.

Attack reduces the average hop count by 25% (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)

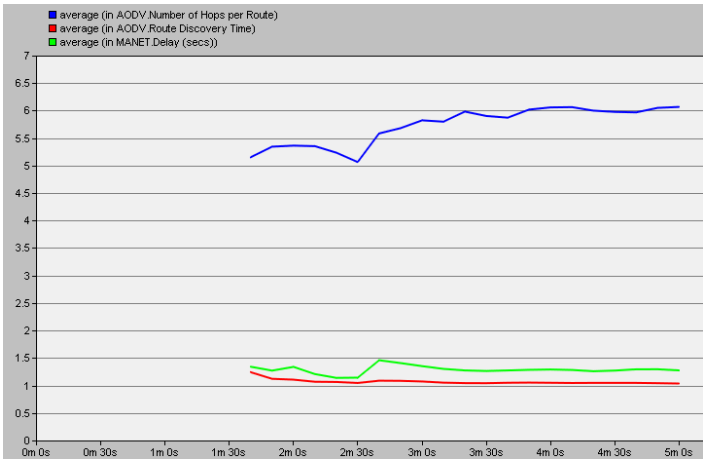

Figure: 4.4 Average delays per route comparison.

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).

V. CONCLUSION

Our method provides good performance for detecting tunneling attacks it detects 75 percent of attackers within five minutes, In addition, since we only select part of the searched routes for multi-path transmission, the probability that attacks can occupy the route are further reduced. In another scenario, attackers may maliciously modify other nodes instead of itself in the graylist. Thus the nodes that have been modified would be reported as modifiers and be blocked by the source node. To counter this, some ID-based cryptographic methods [15] such as digital signatures can be adopted to prevent this.

REFERENCES

[1] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", In Proc. 6th IFIP Commun. and Multimedia Security Conf., Sept. 2002

[2] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. 6th Ann. ACM Int'l Conf. Mobile Computing and Networking, ACM Press, 2000, pp. 255– 265.

[3] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol ", in Proc. 3rd ACM Intl. Symp., on Mobile Ad Hoc Networking and Computing, Jun 2002

[4] P.G. Argyroudis and D. O'Mahony, "Secure Routing for mobile ad hoc networks", *IEEE Communications Surveys & Tutorials, third quarter 2005, Vol. 7, no3, 2005* 258 Authorized licensed use limited to: University of Allahabad. Downloaded on July 30,2010 at 16:19:57 UTC from IEEE Xplore. Restrictions apply.

[5] R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "Performance Analysis of Secure Multipath Routing Protocols for Mobile Ad Hoc Networks", WWIC 2005, LNCS 3510, pp. 269–278, 2005.

[6] Papadimitratos, P.; Haas, Z.J. Secure Routing for Mobile Ad Hoc Networks. In SCS CNDS, San Antonio, TX, USA, January 2002.

[7] Sanzgiri, K.; Dahill, B.; Levine, B.N.; Shields, C.; Belding-Royer, E.M.A. A Secure Routing Protocol for Ad Hoc Networks. In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), Paris, France, November 2002.

[8] Hu, Y.C.; Perrig, A.; Johnson, D.B. Wormhole Attacks in Wireless Networks. IEEE J. Sel. Area Comm. 2006, 24, 370–380.

[9] Khabbazian, M.; Mercier, H.; Bhargava, V.K. Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks. IEEE Trans. Wireless Commun. 2009, 8, 736–745.

[10] Wang, W.; Bhargava, B. Visualization of Wormholes in Sensor Networks. In Proceedings of the 2004 ACM workshop on Wireless Security (WiSe), ACM WiSE'04, Philadelphia, PA, USA, October 2004; pp. 51–60.

[11] O. Kachirski and R. Guha, "Effective Intrusion Detection using Multiple Sensors in Wireless Ad hoc Networks", in Proc. 36th Annual Hawaii Int'l. Conf. on System Sciences (HICSS'03), pp.57.1, 2003.

[12] H.S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," in Proc. International Symposium on Wireless Pervasive computing, Phuket, Thailand, pp. 1-6, 2006.

[13] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Proceedings of the Network and Distributed System Security Symposium.

[14] L. Lazos, R. Poovendran, C. Meadows, P. Syverson and L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach," in IEEE WCNC 2005, Seattle, WA, USA, pp. 1193–1199, 2005

[15] L. Lazos, and R. Poovendran, "SeRLoc: Secure Range- Independent Localization for Wireless Sensor Networks," in ACM WiSE'04, New York, NY, USA, pp. 73–100, October 2004.

First Author – Pushpendra Niranjan, M.Tech, LNCT (RGPV) Bhopal, India and pusp18jan@gmail.com.

Second Author – Prashant Srivastava, M Tech, KCNIT (Banda), UPTU, Lucknow, U.P., India and ersri.prashant@gmail.com

Third Author –Raj kumar Soni, M.Tech, KCNIT (Banda), Lucknow, U.P.,India and rajksoni20@gmail.com

Fourth Author- Ram Pratap, M.Tech , KCNIT(Banda), UPTU, Lucknow, U.P., India and harry_mca11@rediffmail.com