# Detecting and Avoiding Wormhole Attack in MANET Using Statistical Analysis Approach

Saurabh Upadhyay[1,*] and Brijesh Kumar Chaurasia[2]

[1] Sarvottam Institute of Technology and Management , Greater Noida, India
[2] Institute of Technology and Management, Gwalior, India
{saurabh.cse.cs,bkchaurasia.itm}@gmail.com

**Abstract.** A mobile ad hoc network (MANET) consists of a collection of wireless mobile nodes that forms a temporary network without having any fixed infrastructure or centralized administration. MANET is infrastructure-less, lack of centralized monitoring and dynamic changing network topology. MANET is highly vulnerable to attack due to open error prone shared wireless medium. In this paper, we proposed an algorithm for avoiding and preventing the wormhole attacks in MANET using statistical analysis approach. Simulation and results show that efficacy of proposed algorithm and the proposed heuristics provides better security and performance than conventional AODV in the presence of wormhole attack.

**Keywords:** MANET, Wormhole attack, Wormhole detection technique, Wormhole prevention, Statistical mechanism.

## 1 Introduction

A mobile Ad hoc network (MANET) is a collection of two or more devices or nodes equipped with wireless communication and networking capabilities [1], [2], [3].These node includes laptop, computers, PDAs and wireless phones etc, have a limited transmission range. Such a wireless ad-hoc network is infrastructure less, self-organizing, adaptive and does not require any centralized administration. If two such devices are located within transmission range of each other, they can communicate directly. Each node can communicate directly with only few nodes within the communication range and has to forward messages using the neighbor nodes until the messages arrive at the destination nodes. Since the transmission between sender and receiver may use several nodes as intermediate nodes, many routing protocols [3] have been proposed for the MANETS. Most of the protocol assumes that other nodes are trustable so they do not consider the security and attack issues. The lack of infrastructure, rapid deployment practices, and the hostile environments in which MANETS are deployed make them vulnerable to a wide range of security attacks that are presented in [4], [5], [6]. However most of these attacks are performed by a single malicious node. Many solutions exist to solve single node attacks [7], [8], [9], but they cannot prevent from the attacks that are executed by colluding malicious node

[*] Corresponding author.

N. Meghanathan et al. (Eds.): CCSIT 2012, Part I, LNICST 84, pp. 402–408, 2012.

such as wormhole attack. Wormhole attack is more dangerous than single node attacks. Analysis of wormhole attack is discussed in [10]. In [11], a wormhole, an attacker connects two distant points in the network, and then replays them into the network from that point. An example is shown in Fig. 1. Here S and D are the two end-points of the wormhole link (called as wormholes). In this diagram, wormhole attack is that all the nodes in area A assume that nodes in area B are their neighbors and vice versa.

The wormhole link can be established by many types such as long-range wireless transmission in wireless networks, by using an Ethernet cable, a long-range wireless transmission and an optical link in wired medium. Wormhole attack records packets at one end-point in the network and tunnels them to other end-point. These attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as AODV/ DSR, than all the packets will transmit through this tunnel and no other route is discovered. If the attacker creates the tunnel honestly and reliably than it will not harm the network and also provides the useful service in connecting the network more efficiently. The attacker can perform the attacks even if the network communication provides confidentiality and authenticity. If single path on-demand routing protocol such as AODV [12] is being used in highly dynamic wireless ad hoc networks, a new route need to be discovered in response to every route break. Each route discovery is associated with high overhead and latency. This inefficiency will be reduced if there are multiple paths available and a new route discovery is required only in the situation when all paths break.

In this paper, we propose an approach to detect wormhole in MANET by using average time delay to detect anomalies based on statistical information of packets in the networks. Three features of the network are monitored including: the number of incoming packets, the number of outgoing packets and the average route discovery time related to each node. The network is having wormhole attacks if any abrupt change of one of these features is reported. The proposed algorithm is light weight and low computation overhead.

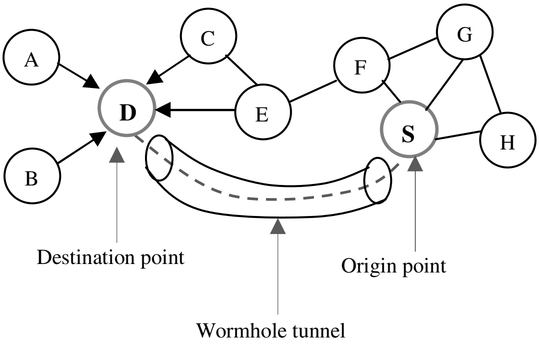

**Fig. 1.** Wormhole attack in a network

The rest of the paper is organized as follows. Section 2 describes proposed algorithm of wormhole detection model in MANET. Result and analysis is illustrated in section 3. Section 4 concludes the work.

## 2 Proposed Wormhole Attack Model

The proposed wormhole attack model method works without any extra hardware requirements, the basic idea behind this work is that the wormhole attack reduces the length of hops and the data transmission delay. The steps of proposed algorithm of wormhole attack are as follows:

1. Randomly generate a node identity, number 0 to maximum number of nodes in the network.
2. Make the node with same number as transmitter node.
3. Generate the route from selected transmitting node to destination node.
4. Start counter and send RREQ using reactive routing technique.
5. Receive the RREP packet from the each path; associate it in route list with time delay.
6. Now calculate the average time delay.
7. Select the route within covariance range of average delay.
8. The routes that are not within the covariance range are black listed hence they are not involved in future routes discovery.
9. Whole process (from step1 to step9) is repeated for limited assumed time.

## 3 Simulation and Results

In this section simulation and results are illustrated. Node distribution scenario is depicted by Fig.2. There are 18 nodes in the network. Simulation parameters are given in Table 1.

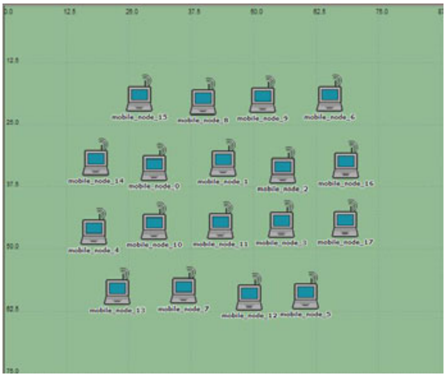

**Fig. 2.** Node distribution scanerio

Wormhole attack scenario is shown in Fig. 3. Wormhole attack is created in between *node 0* and *node 5* . Due to wormhole attack, all the traffic between *node 0* and *node 0* will go directly without using any nodes while other intermediate nodes are presented in the network.

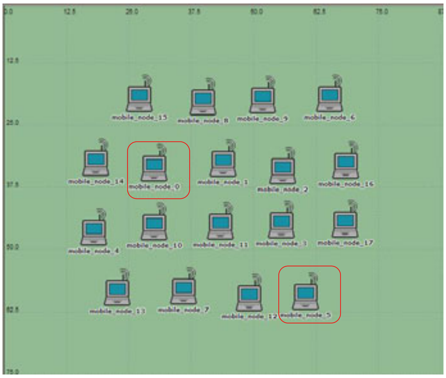

**Fig. 3.** A netwok affected by wormhole attack

**Table 1.** Simulation parameters

| Parameters | Description |
|---|---|
| Examined Protocol | AODV |
| Simulation Time | 1000 sec. |
| Simulation Area | 80x80 m |
| Number of Nodes | 18 |
| Malicious Nodes | 02 |
| Number of Wormholes | 01 |

Fig. 4 shows the average route length in terms of number of hops for all three conditions'. X direction shows the simulation time where as Y direction illustrates the number of hops. Normal condition is depicted by red color. As wormhole attack occurs wormhole affected node start sending packet by using the tunnel without using intermediate nodes so number of hopes reduces as shown by green color. Fig. 4 shows that at the time of 3 minutes the difference between the number of hops required in wormhole affected scenario and without wormhole scenario is maximum that means the minimum number of hops is required to transmit the data and most of the data is being transmitted involving the wormhole affected node. After the time of 6 min of our proposed algorithm reached very near to the without attack scenario in terms of number of hops required that means wormhole affected nodes is being avoided. By implementing the proposed algorithm wormholes are avoided in the route discovery process as number of hopes per route increases as shown by blue color.

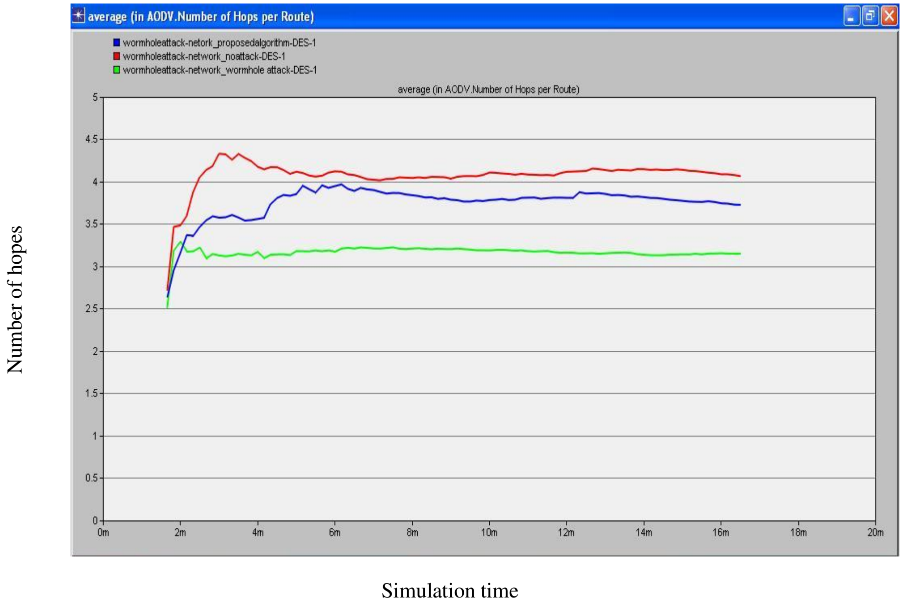

**Fig. 4.** Average number of hopes per route

Average route discovery time for all three conditions is depicted by Fig. 5. This results show that the wormhole tunnel is selected all the times by wormhole affected nodes so new routes are not discovered this will reduce the route discovery time. At

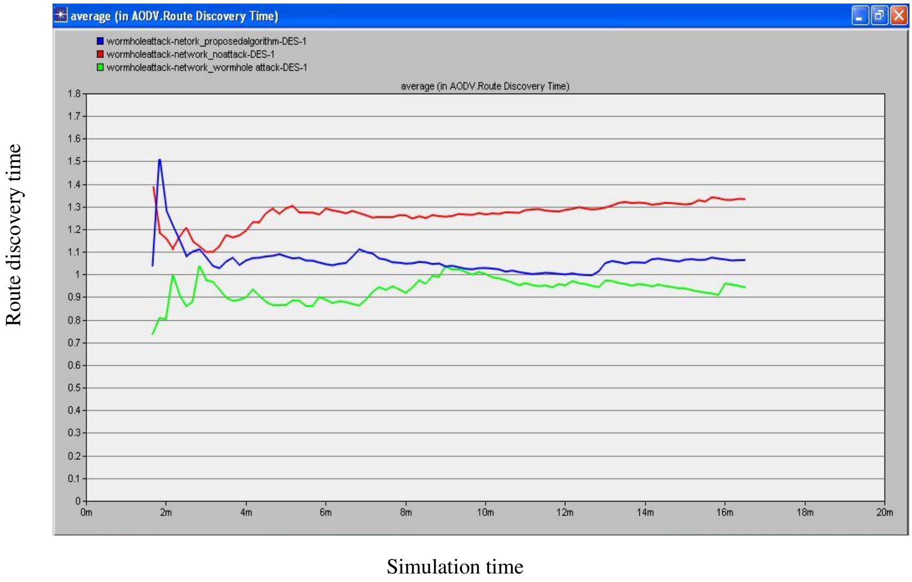

**Fig. 5.** Average route discovery time

the time of 3 minutes route discovery time of proposed algorithm almost equal to the route discovery time of without attack scenario that mean all the nodes are being checked for route discovery process. After 14 min, the route discovery time of proposed scenario has become almost steady. The proposed algorithm wormhole affected routes are avoided and the entire route is being checked so route discovery time may be increase.

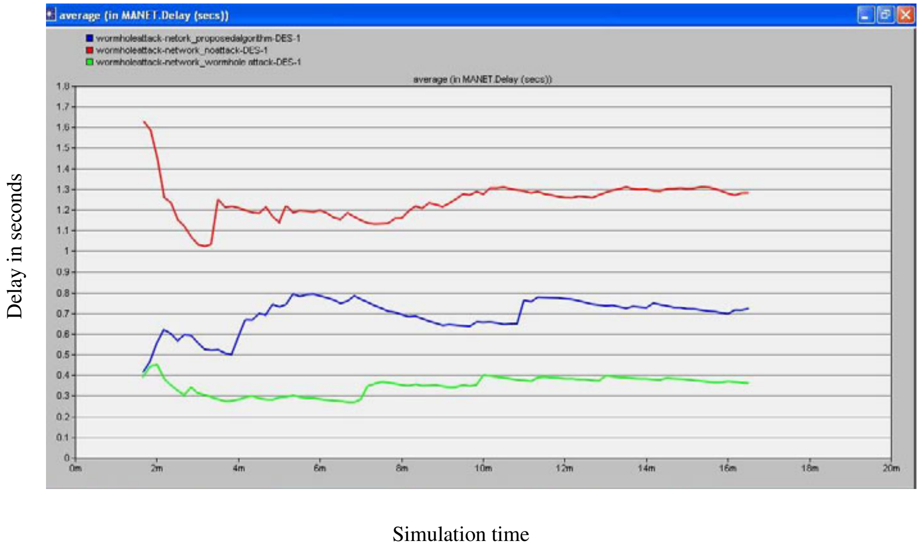

**Fig. 6.** Average delay in seconds

Fig. 6 shows, the average delay for all three conditions. Due to the wormhole attack the delay reduces because the packets are delivered without any intermediate nodes. The proposed algorithm is used the number of intermediate nodes to avoid wormhole tunnel, so delay is increased from without attack environment but it is very less from attack scenario. At the time of 3 minutes delay is around 0.5 sec. At the time of 5 minutes and after that delay is in between 0.7 to 0.8 sec of our proposed algorithm.

## 4 Conclusion

Statistical analysis is a technique used to detect routing anomaly as long as the sufficient information about the routes is available from the multi-path routing. Simulation results are shown that proposed algorithm is successful at detecting wormhole attacks and locating the malicious nodes. The simulation shows the avoidance of using the attacker nodes in data transmission. Security against wormhole attack can be provided by using our proposed algorithm. The algorithm performs better compared to existing routing protocols on three parameters hop count, route discovery time, delay. The proposed model is shown that algorithm is very light-weight and suited the security issues of MANET.

## References

1. Perkins, C., Bhagwat, P.: Highly dynamic destination-sequenc distance-vector routing (DSDV) for mobile computers. In: Proceedings of ACM Conference on Communications Architectures, Protocols and Applications (ACM SIGCOMM 1994), London, UK, pp. 234–244 (1994)
2. Perkins, C., Royer, E.: Ad hoc on-demand distance vector routing. In: Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100 (1999)
3. Perkins, C.E.: Ad hoc Networking. Addison Wesley, Boston (2001)
4. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications 11(1), 38–47 (2004)
5. Zhen, J., Srinivas, S.: Replay Attacks for Secure Routing in Ad Hoc Networks. In: Pierre, S., Barbeau, M., An, H.-C. (eds.) ADHOC-NOW 2003. LNCS, vol. 2865, pp. 140–150. Springer, Heidelberg (2003)
6. Hu, Y.-C., Perrig, A., Johnson, D.B.: Rushing attacks and defense in wireless ad hoc network routing protocols. In: Maughan, W.D., Perrig, A. (eds.) ACM Workshop on Wireless Security (WiSe), pp. 30–40 (2003)
7. Tamilselvan, L., Sankaranarayanan, D.V.: Prevention of impersonation attack in wireless mobile ad hoc networks. International Journal of Computer Science and Network Security (IJCSNS) 7(3), 118–123 (2007)
8. Papadimitratos, P., Haas, Z.J.: Secure routing for mobile ad hoc networks. In: Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (2002)
9. Hu Y.-C., Johnson, D.B., Perrig, A.: SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. In: IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 3–13 (2002)
10. Upadhyay, S., Chaurasia, B.K.: Impact of Wormhole Attacks on MANETs. International Journal of Computer Science & Emerging Technologies 2(1), 77–82 (2011)
11. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications 11(1), 38–47 (2004)
12. Perkins, C., Belding-Royer, E., Das, S.: Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561 (2003)