Avoiding Wormhole Attack in MANET using Statistical Analysis Approach

Saurabh Upadhyay[1] and Aruna Bajpai[2]

[1]Sarvottam Institute of technology and Management, Greater Noida, India
saurabh.cse.cs@gmail.com
[2]Samrat Ashok Technological Institute ,Vidisha,India
arunabajpai20@gmail.com

ABSTRACT

MANET is a collection of mobile hosts with wireless network interfaces that form a temporary network without 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 results shows that proposed algorithm provides better security and performance in the presence of wormhole attack than conventional AODV.

KEYWORDS

MANET, Wormhole attack, Wormhole detection technique, Wormhole Avoidance, Statistical analysis.

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. In a MANET, nodes which are within each other's wireless transmission ranges communicates directly, nodes that are outside each other's range have to rely on some other nodes to transmit messages [13]. Thus, a multi-hop scenario occurs, where several intermediate hosts relay the packets sent by the source host before they reach the final destination . Each node functions as a router. The success of communication highly depends cooperation of other 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 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 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 neighbours 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. A potential solution is to integrate the prevention methods into intrusion detection system .However, it is difficult to isolate the attacker with a software-only approach, since the packets sent by the wormhole are similar to the packets sent by legitimate nodes. 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. Security is the combination of processes, procedures, and systems that ensures confidentiality, authentication, integrity, access control, availability and non repudiation. some kind of authentication and integrity mechanism, either by the end-to-end approach or hop-by-hop , is used to ensure the correctness of routing information.

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, throughput of the network, retransmission attempts and load on the network. 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.

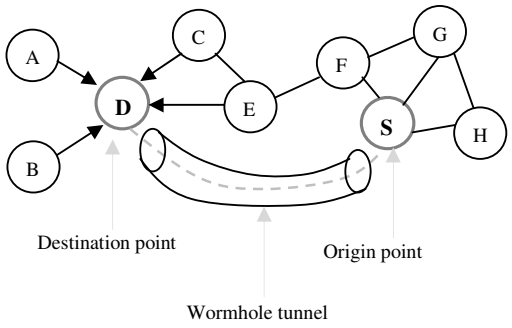


Fig. 1. Wormhole attack in a network

2 Proposed Wormhole Attack Detection 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 [13]. The steps of proposed algorithm are as follows

1. Randomly generate a number 0 to maximum number of nodes.
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 step 8) is repeated for limited assumed time.

3 Simulation and Results

In this section simulation and results is 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 $node\ 5$ will go directly without using any nodes while other intermediate nodes are presented in the network.

Fig. 3. A netwok affected by wormhole

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

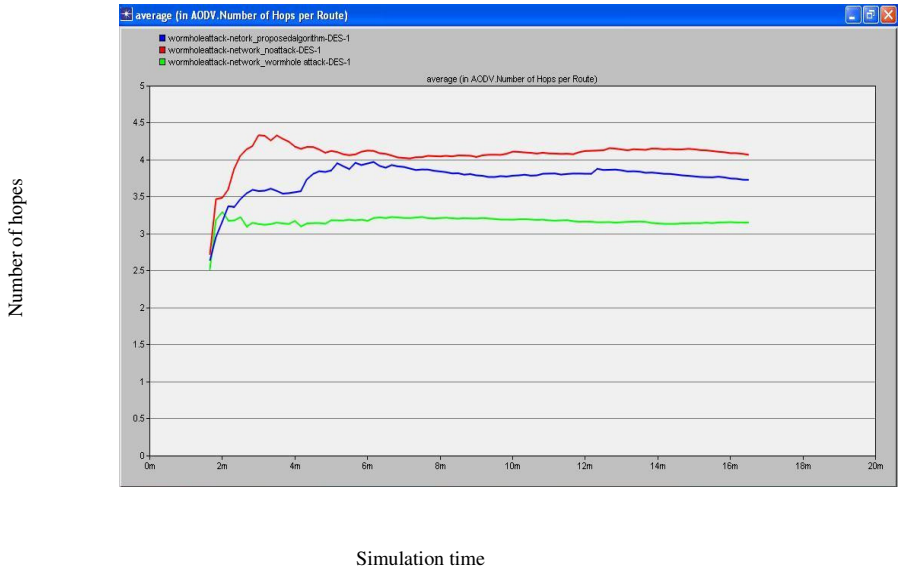


Fig. 4. Average number of hopes per route

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 shows the number of hops. No attack

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 clear from green color. 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.

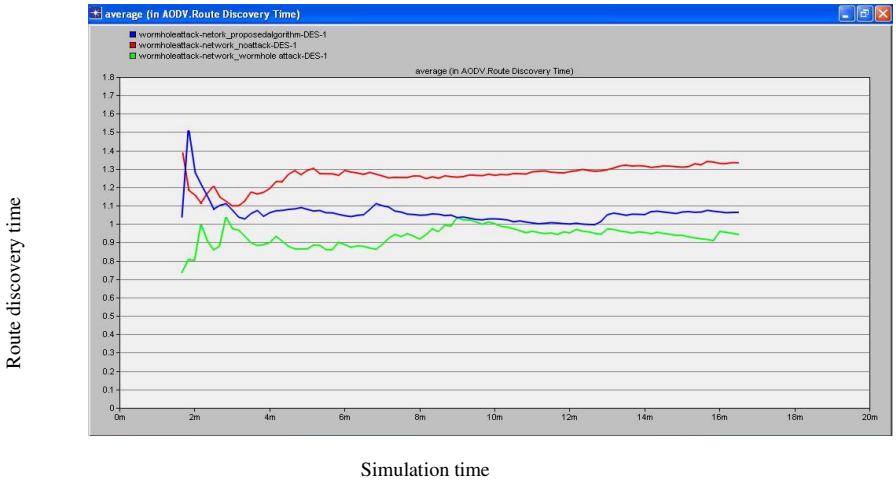
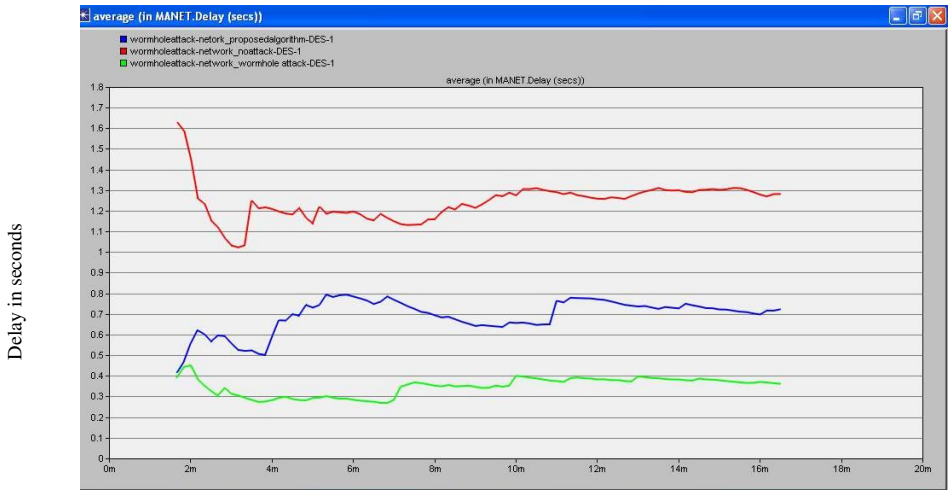


Fig. 5. Average route discovery time

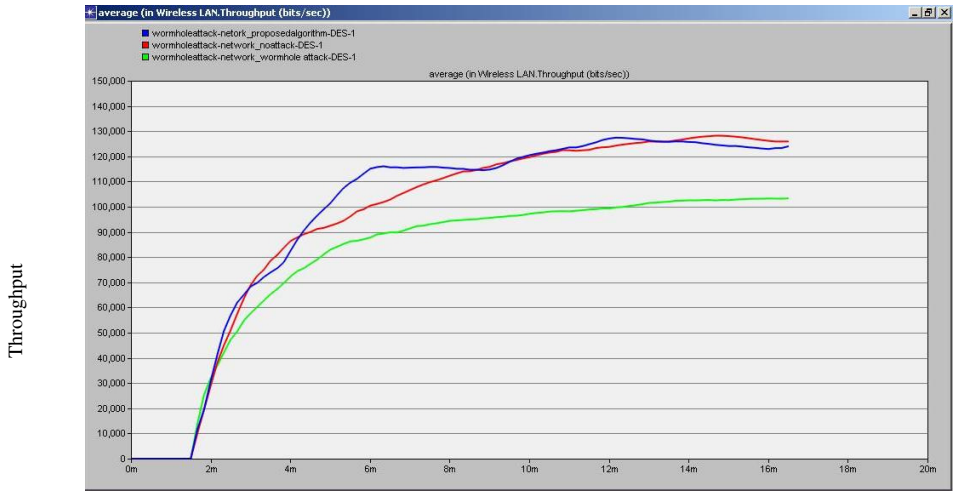
Fig. 5 shows the average route discovery time for all three conditions. X direction shows the simulation time and Y direction shows the route discovery time. No attack condition is depicted by red color. Under wormhole attack the wormhole tunnel is selected all the times by wormhole affected nodes so new routes are not discovered this will reduce route discovery time as denoted by green color. With the proposed algorithm wormhole routes are avoided so route discovery time increases denoted by blue color.



Simulation time

Fig. 6. Average delay in seconds

Fig. 6 shows the average delay for all three conditions'. X direction shows simulation time where as Y direction shows delay. No attack condition is depicted by red color, Due to the wormhole attack the delay reduces because the packets are delivered without any intermediate nodes denoted by green color where as blue color is the condition when the wormhole is avoided with the help of proposed algorithm.



Throughput

Simulation time

Fig. 7. Average Throughput in bit per seconds

Fig. 7 shows the average throughput for all three conditions'. X direction shows simulation time where as Y direction shows throughput. No attack condition is depicted by red color, Due to the wormhole attack the throughput reduces denoted by green color where as blue color is represents the scenario when the wormhole is avoided with the proposed algorithm.

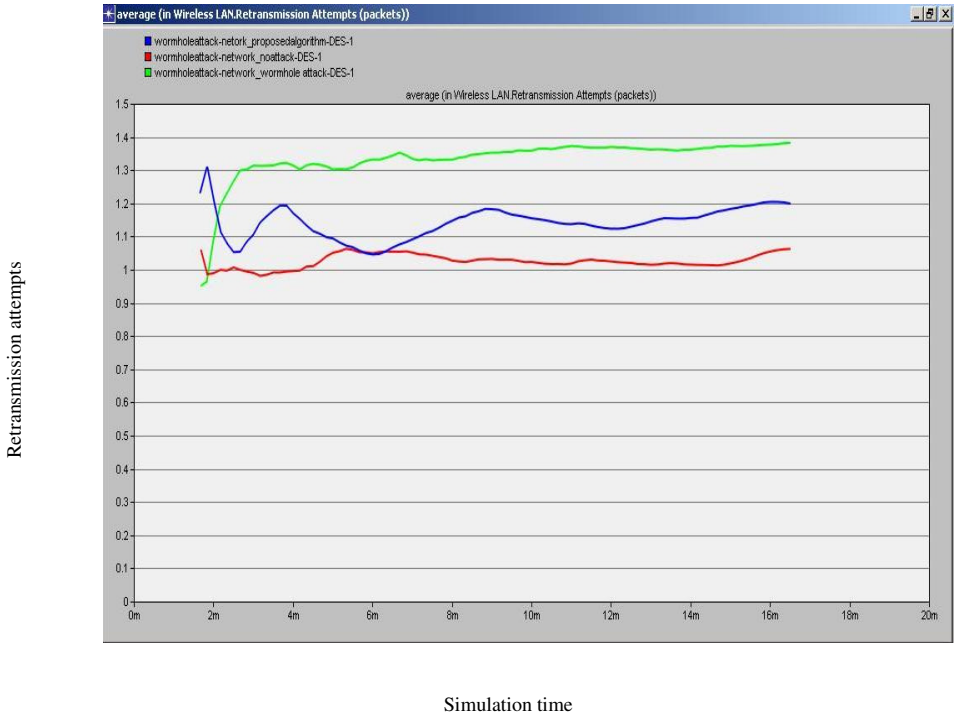


Fig. 8. Average Retransmission attempts in packets

Fig. 8 represents the retransmission attempts for all three conditions'. X direction shows simulation time where as Y direction shows Retransmission attempts. No attack condition is depicted by red color when there are minimum retransmission because all the packets are delivered to their destination, Due to the wormhole attack the retransmission increases because the packets are not reaching to their destination denoted by green color where as blue color is represents the condition when the number of retransmission are reduced and wormhole is avoided with the proposed algorithm.

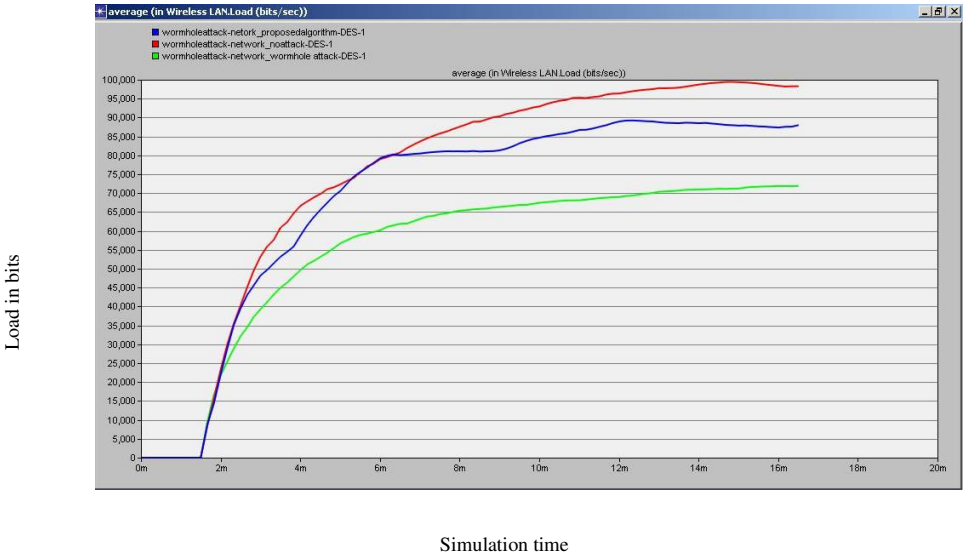


Fig. 9. Average Load in bits per second

Fig. 9 represents the average loads on the network for all three conditions'. X direction shows simulation time where as Y direction shows load in bits .No attack condition is depicted by red color when there average maximum load because load is evenly distributed , Due to the wormhole attack the wormhole affected nodes use wormhole tunnel to reach their destinations so average load on the nodes reduces their destination denoted by green color where as blue color is represents the condition when wormhole is avoided with the proposed algorithm.

3. CONCLUSIONS

Statistical analysis approach is very useful if the sufficient information about the routes is available from multi path routing and can detects the wormhole .Simulation results show s that proposed algorithm is successful at detecting wormhole attacks and locating the malicious nodes. Simulation results shows that wormhole tunnel is avoided in route discovery process so effects of wormhole attack in minimized. The proposed algorithm is light weight so it can be applied to demands and limitations of MANET providing high efficiency.

.

ACKNOWLEDGEMENT

The authors would like to thank Dr. Brijesh Kumar Chaurasia for their continuous help during the research

REFERENCES

1. Perkins C. and 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 "94), London, UK, pp. 234-244 (1994)

2. Perkins C. and 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, *Boston, Addison Wesley* (2001)
4. Yang H., Luo H., Ye F., Lu S. and Zhang L.: Security in mobile ad hoc networks: challenges and solutions, In IEEE Wireless Communications, vol. 11, no. 1, pp.38–47 (2004)
5. Zhen J. and Srinivas S.: Preventing replay attacks for secure routing in ad hoc networks, In ADHOC-NOW, LNCS 2865, pp. 140–150 (2003)
6. Hu Y.-C., Perrig A. and Johnson D. B.: Rushing attacks and defense in wireless ad hoc network routing protocols, In W. D. Maughan and A. Perrig, editors, ACM Workshopon Wireless Security (WiSe), pp. 30–40 (2003)
7. Tamilselvan L. and Sankaranarayanan D. V.: Prevention of impersonation attack in wireless mobile ad hoc networks, International Journal of Computer Science and Network Security (IJCSNS), vol. 7, no. 3, pp.118–123 (2007)
8. Papadimitratos P. and 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. and 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. and Chaurasia B. K.: Impact of Wormhole Attacks on MANETs, In International Journal of Computer Science & Emerging Technologies, vol. 2, issue 1, pp. 77-82 (2011)
11. Yang H., Luo H., Ye F., Lu S. and Zhang L.: Security in mobile ad hoc networks: challenges and solutions, IEEE Wireless Communications, vol. 11, no. 1, pp. 38–47 (2004)
12. Perkins C., Belding-Royer E. and Das S.: Ad hoc On-Demand Distance Vector (AODV) Routing, *RFC 3561* (2003)
13. Upadhyay S. and Chaurasia B. K.: Detecting and Avoiding Wormhole Attack in MANET using Statistical Analysis Approach, In the Second International Conference on Computer Science and Information Technology (CCSIT- 2012), Springer, pp. (2012)

Authors

Saurabh Upadhyay is working as Asst. Prof . With Sarvottam Institute of Technology and management ,Greater Noida . He received his M. Tech. (Software System) from SATI, Vidisha, India. His area of interest is Security in Ad-hoc network and Cyber security. (saurabh.cse.cs@gmail.com)

Aruna bajpai is persuing mtech from sati,vidisha. Her area of interest are privacy issue in data mining and security is wireless and sensor networks .(arunabajpai20@gmail.com)