**World Research Journal of Telecommunications Systems**
ISSN: 2278-8573 & E-ISSN: 2278-8581, Volume 1, Issue 1, 2012, pp.-13-15.
Available online at http://www.bioinfo.in/contents.php?id=357

# EFFECTIVENESS OF WORMHOLE ATTACK ON DSR PROTOCOL IN MANET

**GULWADE M.P., DHOOT K.J., BAJAJ A. I. AND GHONGE M.M.**

Department of Computer Science and Engineering., J.D.I.E.T, Yavatmal, MS, India.
*Corresponding Author: Email- mrunalgulwade@gmail.com, khushboodht@gmail.com, abhishek.bajaj@yahoo.in, mmghonge@gmail.com

Received: April 09, 2012; Accepted: May 21, 2012

**Abstract-** Security in mobile ad hoc networks is difficult to achieve, because of the dynamic topologies, limited resources, the absence of a certification authority and the lack of a centralized monitoring point [1]. Most of the attacks in MANETs are routing protocol attacks. The wormhole effect is caused by attempts to draw all network traffic to malicious nodes that broadcast fake shortest path routing information. The wormhole nodes should be detected and detached as early as possible. This paper illustrates how wormhole attack can affect the performance of DSR routing protocols in wireless networks by using NS-2 simulator.

**Key words-** MANET, Wormhole nodes, Routing Attacks, Bogus RREQ.

**Citation:** Gulwade M.P., et al. (2012) Effectiveness of Wormhole Attack on DSR Protocol in MANET. World Research Journal of Telecommunications Systems, ISSN: 2278-8573 & E-ISSN: 2278-8581, Volume 1, Issue 1, pp.-13-15.

## Introduction

A mobile ad hoc network which is also known as a mobile mesh network is a self-configuring wireless network of mobile nodes. The mobility of the nodes is independent of each other. MANETs do not have any controlling point to regulate the traffic. Each node in the MANET has to take care of the routing aspect as well. There are many routing protocols available for routing in ad-hoc networks. The routing protocols for MANETs are broadly classified into two types proactive and reactive. The protocols like DSDV, OLSR, OSPF, TBRPF, FSR and FSLS are proactive protocols which will use periodic messages in order to know the network topology. The reactive protocols include AODV, DSR. The hierarchical routing contains the protocols like HSR, CGSR, ZRP, and LANMAR. In the geographic position assisted protocols we have GEOCAST, LAR, DREAM and GPSR [8]. MANETs are infrastructure-less and will have dynamically changing topologies which make them vulnerable to many kinds of failures and attacks. Most of the attacks in MANETs target the routing protocols. The mobility of nodes makes it more vulnerable to routing protocol attacks. By attacking the routing protocols, the attackers can absorb network traffic or inject themselves into the path between the source and destination. Some latest attacks on the routing protocol in MANETs are, wormhole attack, black hole attack, grey-hole attack, byzantine attack, rushing attack [2,9-10]. Sinkhole attack, if carried out successfully, can cause all of the above mentioned attacks possible. So it is important to detect the sinkhole nodes and prune them from the MANET. The nodes in the MANET should cooperate with each other to make the communication possible. Here comes the mutual understanding. We are going to use this property to detect the sinkhole nodes in the network. The rest of the paper is organized as follows: In section 2 we discuss about the wormhole attacks in the context of dynamic source routing (DSR). In section 3 we discuss the simulation of DSR protocol,. In section 4 we discuss simulation result and Section 5 gives the conclusion.

## Dynamic Source Routing and Wormhole Attack

DSR [4] is one of the most widely used reactive protocols in ad-hoc networks. DSR uses two kinds of messages known as RREQ – Route Request and RREP – Route Reply for route discovery process. DSR uses the RREQ message if and only if there are no routes available in the route cache to reach the destination. DSR starts the route discovery by sending Route Request (RREQ) packet. The RREQ will be uniquely identified by the sequence number, source id and destination id [4]. Node A initiates the route discovery by broadcasting the RREQ message. Each node will then add their id to the route and broadcasts it again. The nodes B, C, D are intermediate nodes and they do not have any source route to reach the node 8, which is the intended destination. The intermediate node which has the route to the destination will send a Route Reply (RREP) and if no intermediate node has the information, the RREQ will be propagated to the destination. The Fig (**3**) depicts the RREP propagation from the destination node E to the source node A. Bogus RREQ will be used to carry out the sinkhole attack. If the bogus RREQ has higher sequence number than the sequence number of the original RREQ from the target node, the intermediate nodes will treat the bogus one as the latest request and discard the original one. The attacks such as blackhole, wormhole, misdirection, and replay can cause an existing route to be broken or a new route to be prevented from being established. Among these attacks wormhole attack is hard to detect because this attack does not inject abnormal volumes of traffic into the network. In a wormhole attack, attackers “tunnel” packets to another area of the network bypassing normal routes as shown in Fig. 1.

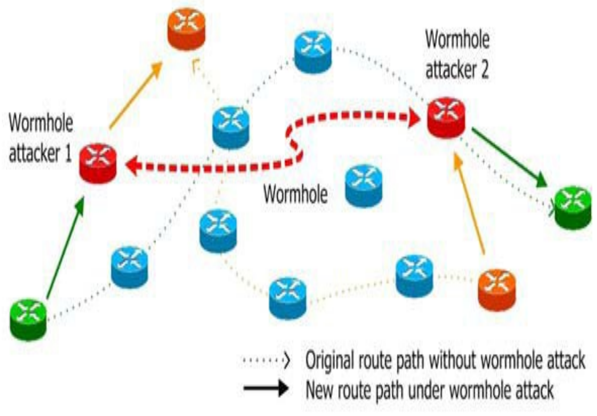
Wormhole attacker 2
Wormhole attacker 1
Wormhole
Original route path without wormhole attack
New route path under wormhole attack

**Fig. 1-** Illustration of wormhole attack in wireless network

### Simulation of DSR Protocol

We have implemented wormhole attack in NS2 [6] simulator. For our simulation, we use CBR (constant bit rate) application, IEEE 802.11 MAC, and a physical channel based on two ray propagation model. The simulated wireless mesh network consists of 10 to 50 nodes in 700*700 m2. The node transmission range is 250 meters. Random waypoint model is used for scenarios with node mobility. The size of data payload is 512 bytes. The simulation is done to analyze the performance of the network by varying node under wormhole attack. The following performance metrics are used in the above mentioned scenario

### Packet Delivery Ratio

The ratio between the number of packets originated by the “application layer” CBR sources and the number of packets received by the CBR sink at the final destination *Average End-to-End Delay:* End-to-End Delay can be defined as the time a packet takes to travel from source to destination. Average End-to-End Delay is the average of the end-to-end delays taken over all received packets.

### Simulation Result

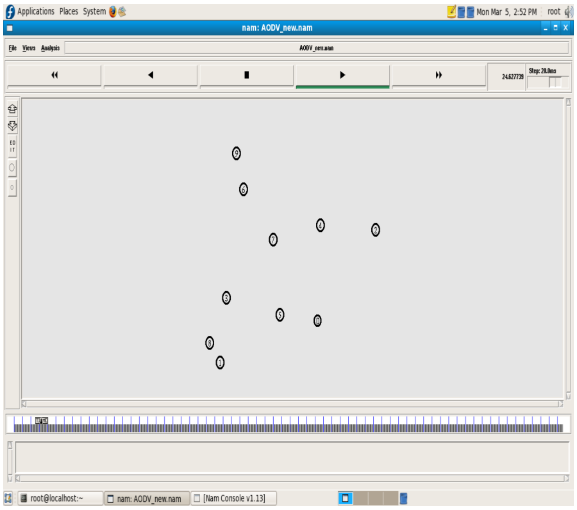

**Fig. 2-** Creation of Nodes

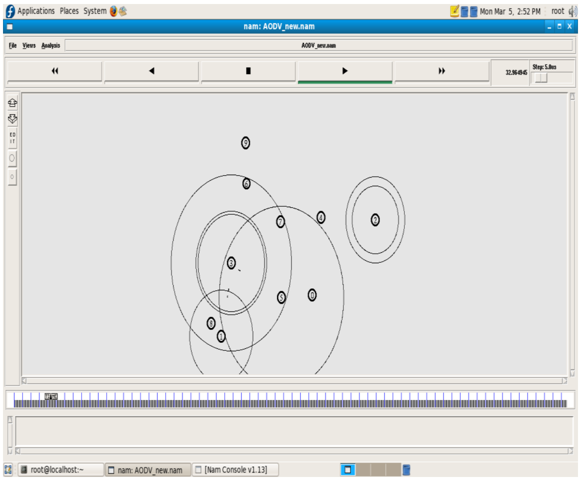

**Fig. 3-** Transmission between 10 Nodes

Fig. 4 shows the effect of Packet Delivery Ratio for DSR protocol when nodes are increased. The result shows the cases, with wormhole and without wormhole attack on DSR. It has been measured that Packet Delivery Ratio decreases with wormhole nodes in the wireless network on DSR routing protocol as compared to without wormhole nodes. Also Fig 5 shows the effect of end to end delay for DSR protocol when nodes are increased. End to end delay increases with wormhole nodes.

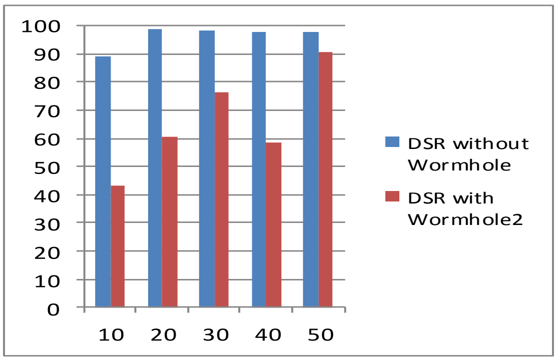

**Fig. 4-** Packet Delivery Ratio

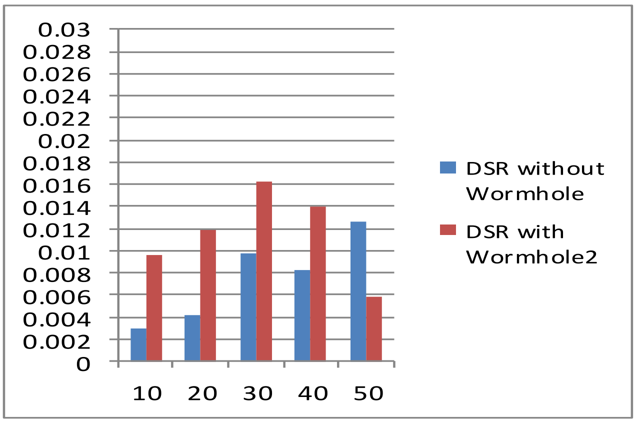

**Fig. 5-** End 2 End Delay

### Conclusion

Wormhole attack is one of the most important security problems in MANET. In a wormhole attack, attackers “tunnel” packets to another area of the network bypassing normal routes. In this paper, we have analyzed the effect of wormhole attack on DSR protocol in MANETs which shows significant degradation in performance of DSR protocol under wormhole attack.

### References

[1] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei (2006) *Wireless/Mobile Network Security*, 12.

[2] Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala. *International Journal of Computer Science and Security*, 2(3).

[3] Chris Tseng H., Jack Culpepper B. (2005) *Computers & Security,* 24, 561-570.

[4] Johnson D.B., Maltz D.A. and Broch J. (2001) *Ad Hoc Networking*. Boston, Addison-Wesley, 139-72.

[5] Marchang N. and Datta R. *Ad Hoc Networks,* 6, 508-23.

[6] The Network Simulator (2003) *http://www.isi.edu/nsnam/ns/*.

[7] Pirzada A.A. and McDonald C. (2003) *2nd Workshop on the Internet, Telecommunications and Signal Processing.*

[8] Rahman A.A. and Hailes S. (1997) *Proc. of the ACM New Security Paradigms Workshop*, 48-60.

[9] Royer E.M. and Toh C.K. (1999) *IEEE Personal Communications Magazine*, 6(2), 46-55.

[10]Stajano F. and Anderson R. (1999) *7th International Workshop on Security Protocols*, 172-194.

[11]Zhou L. and Haas Z.J. (1999) *IEEE Network Magazine*, 13(6).

[12]Singhal S.K. (2001) *The Seven Deadly Sins of Wireless LANS.*

[13]Tiantong You, Chi-Hsiang Yeh and Hossam Hassanein (2003) *3rd International, Workshop on Wireless Local Networks*.

[14]William A. Arbaugh, Narendar Shankar, and Justin Wan Y.C. (2002) *IEEE Wireless Communications Magazine*, 9, 44-51.

[15]Cisco SAFE (2003) *Wireless LAN Security in Depth*. *Cisco Systems*.

[16]Housley R. and Arbaugh W.A. (2003) *WLAN Problems and Solutions, Communications of the ACM*, 46, 31-34.