Wormhole attack on On Demand routing protocols in mobile ad hoc networks

Sumet Mehta[1], Gaurav Monga[2]

[1,2]Electronics and Communication Department,
[1,2]JCDM College of Engineering, Haryana, India

Abstract— A mobile ad hoc network (MANET) consists of mobile wireless nodes. In MANET nodes are self-motivated topologies can randomly change their geographic locations. Wireless networks are susceptible to many attacks, including an attack known as the wormhole attack. On occurrence of wormhole can cause a significant breakdown in communication across a wireless network. This paper explores and compares the effect of wormhole attacks on the performance of on demand routing protocols in mobile ad hoc network (MANET). The evaluation has been done by studying and comparing end to end delay, packet delivery ratio and throughput for wormhole attack and without wormhole attack.

Key words: Mobile ad hoc networks, routing protocol; wormhole attacks, end to end delay, throughput, packet delivery ratio.

I. Introduction

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies as shown in fig. where three mobile nodes are communicate with each wirelessly. In the mobile ad hoc networks, nodes are can directly communicate with all the other nodes within their ratio ranges whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. With the rapid development in wireless technology, Ad hoc networks have emerged in many forms. These networks operate in the license free frequency band and do not require any investment in infrastructure, making them attractive for military and selected commercial applications. However there are many unsolved problems in ad hoc networks, securing the network being one of the major concerns. The characteristics of these networks are summarized as follows:

- Nodes can perform the roles of both hosts and routers.
- No centralized controller and infra structure.
- Intrinsic mutual trust.
- Dynamic network topology

Routing Protocols in mobile ad hoc networks can be divided into two major categories,

- Proactive or Table-Driven
- Reactive or On-Demand

Proactive or Table-Driven routing protocols discover routes automatically and periodically maintain a table of the network topology. Therefore, routes are discovered for every mobile node of the network, without any requests for communications by the hosts. Some examples of such protocols are Destination Sequenced Distance Vector Routing (DSDV**),** Wireless Routing Protocol (WRP), Cluster- Head Gateway Switch Routing Protocol (CGSR) and Source Tree Adaptive Routing Protocol (STAR). In On-Demand routing protocols when communication between hosts of a mobile network is required the route discovery process takes place. Reactive protocols perform route discovery and path establishment by using specialized sets of packets known as control packets**.** Examples of Reactive routing protocols include Ad hoc on Demand Distance Vector Routing Protocol (AODV), Dynamic Source Routing Protocol (DSR), and Temporally Ordered Routing Algorithm (TORA).

Due to the dynamic nature of MANET, a secure routing becomes a tricky task. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node. In this paper performance of MANET is studied for On demand routing protocols namely AODV and DSR with analysis of different types of wormhole attacks. End to End delay, Packet delivery ratio and Throughput are studied for wormhole attack and without wormhole attack.

This paper has been organized as follows: Section II describes about the AODV, Section III discusses the functioning of DSR, Section IV explains the Wormhole Attacks, Section V illustrates the performance of network under Wormhole Attack and Section VI concludes the paper and proposes the future work.

II. Adhoc on Demand Distance Vector Routing Protocol

AODV is a practical implementation of the Reactive route discovery mechanism [5]. AODV maintain routing information by using traditional routing tables, one entry per destination without source routing. Different from Destination Sequenced Distance Vector Routing (DSDV), AODV broadcasts the routing messages on a demand basis to reduce the routing overhead and relies on routing table entries to propagate an Route Reply Packet (RREP) back to the source and, subsequently, to route data packets to the destination. AODV uses sequence numbers maintained at each destination to update the routing information and to prevent routing loops. All routing packets carry these sequence numbers. AODV uses control packets such as Route Request (RREQ), Route Reply, and Route Error (RERR) to maintain routes between communicating nodes [6]. When a node needs to determine a route to a destination node, it floods the network with a Route Request (RREQ) message that contains RREQ ID, Destination IP address, Destination Seq no., Source IP address, Source seq. no. and hop count to its neighboring nodes, which broadcast the message to their neighbors, and so on. Each node remembers recently forwarded route requests in a route request buffer to avoid cycles. As these requests spread through the network, intermediate nodes store reverse routes RREP message propagates through intermediate nodes, these nodes update their routing tables for future route establishment [7]. If data is flowing and link break is detected a RERR message is generated and sent to the source in hop by hop fashion As RERR propagates towards the source, message each intermediate node invalidate routs to any unreachable destination. When source of the data receives the RERR, it invalidate the route and reinitiate route discovery. In contrast to DSR, RERR packets in AODV are intended to inform all sources using a link when a failure occurs. Each node maintains a route request buffer, that contains a list of recently broadcasted route requests that prevent nodes from resending the same RREQs repeatedly, AODV is also able to maintain multicast routing. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules and can make changes in address field, sequence number and hop count field to mislead the routes back to the originating node. An intermediate node stores the route only with the smallest hop count. Sequence numbers are used to eliminate the stale routes. When a node receiving the request either knows of a fresh route to the destination or is itself the destination, the node generates a RREP message, and sends this message along the reverse path back towards the originating node. If data is flowing and link break is detected a RERR message is generated and sent to the source in hop by hop fashion As RERR propagates towards the source, message each intermediate node invalidate routs to any unreachable destination. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules and can make changes in address field, sequence number and hop count field to mislead the routes.

III. Dynamic source routing (DSR) protocol

Dynamic Source Routing (DSR) uses source routing to deliver packets from one node in the network to some other node. The source node adds the full path to the destination in terms of intermediate nodes in every packet. This information is used by intermediate node to determine whether to accept the packet and to whom to forward it. DSR operates on two mechanisms: Route Discovery and Route Maintainance. Route Discovery is used when the sender does not know the path upto the destination. In this mechanism, the sender broadcasts a ROUTE REQUEST message which contains Source Address, Destination Address, Identier. Each intermediate node adds its address in ROUTE REQUEST message and rebroadcast it, unless it has not rebroadcasted earlier. With this controlled broadcast, the ROUTE REQUEST will ultimately reach the destination. The destination then sends a unicast ROUTE REPLY message in reverse direction whose information is obtained from list of intermediate nodes in ROUTE REQUEST message. When the ROUTE REPLY packet reaches the source, it records the route contained in it and saves in its cache for the specic destination. For better performance, an intermediate node also records this route information from the two route messages. All nodes overhearing these packets adds meaningful route entries in their caches. Finally, Route Maintainance Mechanism is used to notify source and potentially trigger new route discovery events when changes in the network topology invalidates a cached route.

IV. Classification of Attacks on MANETs

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described on individual layer are as under:

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Location disclosure etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
- Physical: Interference, Traffic Jamming, Eavesdropping

A. WORMHOLE ATTACK:

A wormhole attack [8] is one of the most complicated and severe attacks in network. The operation of this attack is to record packets at one location and rerun them at another location using a private high speed network by a group of conspiring attackers. An attacker situated close to the network can completely destroy the routing path. The worst can happen that nodes can be in problem that they are close to the destination even though they are at far distance [7]-[4]. These attacks are specifically precarious in ad hoc network routing protocols in which the nodes calculates its position by hearing packet transmission directly from some node and consider themselves to be in their neighbor. For example, when used against an on-demand routing protocol such as DSR [3] or AODV [2]-[3], a powerful application of the wormhole attack can be mounted by tunneling each Route Request packet directly to the destination target node of the Request. When the destination node’s neighbors hear this request packet, they will follow normal routing protocol processing to rebroadcast that copy of the request, and then discard without processing all other received Route Request packets originating from this same route discovery. This attack, thus, prohibits any routes other than passing through the wormholes from being revealed, and if the attacker is near the start up of the route discovery, this attack can even avert routes more than two hops long from being discovered. Potential ways for the attacker to utilize the wormhole include abandon rather than forwarding all data packets, thereby forming a permanent Denial-of- Service (DoS) attack (no other route to the destination can be discovered as long as the attacker maintains the wormhole for Route Request packets), or selectively abandoning or altering certain data packets.

V. Simulation and results

The performance of network under wormhole attack was evaluated using NS2.34 network simulator. The simulation area was set 1000m x 1000m flat areas. The MAC protocol IEEE 802.11 was used with a channel data rate of 11 Mbps. The size of data packet was 1024 bytes of constant bit rate

(CBR) application based on TCP have been used as traffic source. Here the scenario is static scenario. The Network simulator is used to set up the simulation environment and compute the actions of all nodes between route discovery processes. Then the simulation results were visualized. Simulation results are classified in four categories: Without wormhole Aodv, Wormhole- Aodv, Without Wormhole-DSR and Wormhole- DSR, and then compared to study the impact of attack.

Channel type	**Wireless Channel**
Network interface type	Phy / Wireless Phy
MAC type	Mac 802.11
Interface queue type	Queue/Drop Tail/PriQueue
Type of attack	Wormhole
No. of Wormhole nodes	5
Antenna model	Omni Antenna
Packet size	1024
Number of mobile nodes	50
Routing protocol	AODV, DSR
X dimension of topography	1000
Y dimension of topography	1000
Time of simulation end	300.0
Traffic type	CBR

Table. 1 : Simulation and Parameter Used

A. *A. Packet Delivery Ratio:*

It is the ratio of the data packets delivered to the destinations to those generated by the sources. Packet Delivery Ratio (PDR) = Total Packets Delivered to destination / Total Packets Generated.

Mathematically, it can be expressed as:

$$P = 1/C\sum_{f=1}^{e} \mathrm{Rf/NF}$$

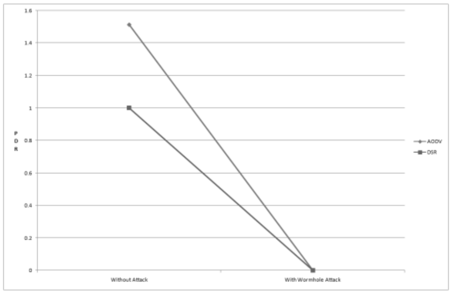

Fig. 1: Packet Delivery Ratio

Where, P is the fraction of successfully delivered packets, C is the total number of flow or connections, f is the unique flow id serving as index, R is the count of packets received from flow f and N is the count of packets transmitted to f. The PDR values obtained for the simulation parameters of table-I. The graph shown in Fig. 1 indicates the PDF comparison of routing protocols, AODV and DSR with and without Wormhole.

B. *Throughput:*

Throughput of the routing protocol is that in certain time the total size of useful packets that received at all the destination nodes. The unit of throughput is MB/s, however we have taken Kilo bits per second (Kb/s). The throughput values obtained for the simulation parameters of table-I. The graph shown in Fig. 2 indicates the throughput comparison of routing protocols, AODV and DSR with and without Wormhole.

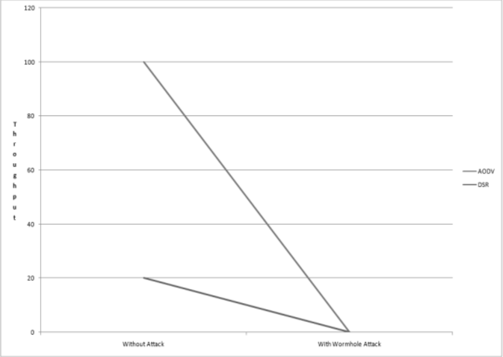

Fig. 2: Throughput

	End To End Delay	**Packet Delivery Ratio**	**Throughput**
Aodv without Wormhole	104.47	1	99.97
Aodv with Wormhole	89.128	0	300.0
DSR without Wormhole	20.93	.97	20.13
DSR with Wormhole	92.90	0	300.0

Table. 2 : Comparison of Average End to End Delay, Packet Delivery throughput.

C. *End To End Delay:*

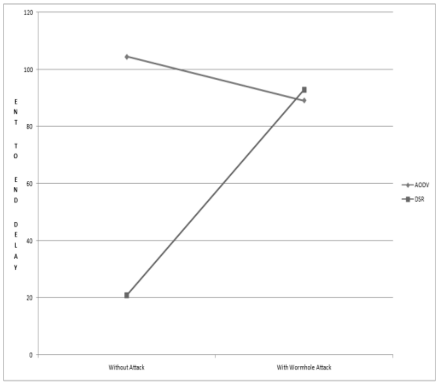

Fig. 3: End To End Delay

The delay experienced by a packet from the time it was sent by a source till the time it was received at the destination. Fig.3 show the End-End Delay for the two protocols as a function of the number of nodes. The performance of DSR is better than AODV for varying number of nodes.

VI. CONCLUSION

This paper evaluated the performance of AODV and DSR routing protocols for Ad hoc networks using NS-2.34 event simulator. AODV and DSR uses the reactive on demand routing strategy with different routing mechanisms. Experimental results showed that AODV and DSR performs better for Packet Delivery Ratio, End to End Delay as well as Throughput when there is no wormhole attack on the network.

REFERENCES

[1] Sanjay Keer, Anil Suryavanshi, "To Prevent Wormhole Attacks Using Wireless Protocol in MANET" "ICCCT" 2010

[2] Yih-chunh, Adrian Perrig, David B. Johnson, "Wormhole attacks in wireless networks" IEEE journal on selected areas in communications, vol. 24, no. 2, Feb 2006.

[3] Reshmi Maulik, Nabendu Chakil, "A Comprehensive Review on Wormhole Attacks in MANET"3rd ed., vol. 2. CISIM 2010

[4] Preeti Nagrath and Bhawna Gupta, "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey" 978-1-4244-8679-3/11©2011 IEEE.

[5] Majid khabbazian, hugues mercier, vijay k. Bhargava, "Severity analysis and countermeasure for the Wormhole attack in wireless ad hoc networks" ieee transactions on wireless communications, vol. 8, no. 2, february 2009.

[6] Sikkandar Ali Vashik Ali, W.R.Salem JeyaseeJan, Shanmugasundaram Hariharan, "Enhanced Route Discovery in Mobile Adhoc Networks" ICCCNT'12 26th_28th July 2012, Coimbatore, India.

[7] VINOTHKUMAR.S, ASOKAN.R, "Improving the Quality of Service Based on Route Stability in MANETs Using Dynamic Source Routing Protocol" ICCCNT July 2012, Coimbatore, India

[8] Rajeshkumar.G, K.R.Valluvan, " A Comparative Study of Secure Intrusion-Detection Systems for Discovering Malicious Nodes on MANETs" International Journal of Computer Applications Vol 67– No.18, April 2013.