The Impact of Wormhole Attack on the Performance of Wireless Ad-Hoc Networks

[1]Pirzada Gauhar Arfaat, [2]Dr. A.H. Mir
[1]Dept. of Information Techcnology, National Institute of Technology, Srinagar, India
[2]Dept. of ECE, National Institute of Technology, Srinagar, India

Abstract
In multihop wireless adhoc networks, cooperation between nodes to route each other's packets exposes these nodes to a wide range of security attacks. Also due to the vulnerability of the routing protocols, the wireless ad-hoc networks face several security risks. A particularly severe security attack that affects the adhoc network routing protocols, is known as the wormhole attack. The wormhole attack is carried out as a two phase process launched by one or more than one malicious nodes. In the first phase, these malicious nodes, called as wormhole nodes, try to lure legitimate nodes to send data via them by participating in the network. In the second phase, wormhole nodes could exploit the data & affect the communication by misbehaving. In this paper we have simulated the wormhole attack in wireless adhoc networks & Manet's. And then we evaluated & discussed the impact on the network by comparing the results without and with wormhole attack. The Wormhole attack was simulated using different scenarios. Thus we studied the impact of the wormhole attack on the respective networks. The parameters like throughput, packet loss and end-to-end delay were calculated using different scenarios for evaluating the impact on wireless adhoc networks and Manet's.

Keywords
Wormhole link, AODV, B-Pro-tocol, Wormhole nodes, Wormhole attack.

I. Introduction

Adhoc networks are vulnerable to attacks due to many reasons; amongst them are the absence of infrastructure, wireless links between nodes, limited physical Protection, and the Lack of a centralized monitoring or management, and the resource constraints. As wireless ad hoc network applications are deployed, security emerges as a central requirement. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols. Wireless ad-hoc networks are usually susceptible to different security threats and wormhole attack is one of these. In this type of attack, the malicious node or nodes pretends to be a legitimate node and participates in the network communication forming a short circuit tunnel and luring traffic flow through this high speed wormhole tunnel. Then the malicious nodes can do any misbehaviour. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to find routes longer than one or two hops, severely disrupting communication. The wormhole attack at network layer can be created by modifying the ad hoc routing protocols. Lot of research work has been done in this field, particularly on wireless networks. As the networks are open, so launching the wormhole attack is not that difficult. Various researches have been done so far regarding the detection and prevention mechanisms of wormhole attacks. Also the research of wormhole attack on wireless networks and its impact on the network has been done but there is a lot of scope of research of wormhole attack & its broader impact on the wireless ad hoc networks. Also the study of wormhole attack by launching the attack or making the adversary nodes behave from the attackers' perspective needs to be studied and the said impact of the adversary behavior on the AODV protocol in ad hoc networks and MANETs needs to be evaluated. The behavior of wormhole attack on different topologies of networks needs to be studied & implemented and the impact of the attack in different topology needs to be studied so that the effect on the various network parameters is analyzed for the impact. The previous work on the wormhole attacks in adhoc wireless networks done so far is as follows:-

To detect and defend against the wormhole attack, packet leashes have been, proposed which may be either geographic or temporal leashes, to restrict the maximum transmission distance of a packet. Finally, to implement temporal leashes, the design and performance analysis of a novel, efficient protocol, called TIK has been presented, which also provides instant authentication of received packets [1].

Another research has been done to explore the impact of wormhole attacks on network connectivity topologies, and a simple distributed method to detect wormholes called 'WormCircle' has been developed [2]. One of the scheme has been proposed to analyze the effect of the wormhole attack on shortest-path routing protocols for wireless ad hoc networks. Using analytical and simulation results, it has been shown that a strategic placement of the wormhole when the nodes are uniformly distributed can disrupt/control on average 32% of all communications across the network [3]. A novel intrusion detection scheme has been proposed that identifies wormhole attacks against wireless mesh networks by external adversaries [4]. Another scheme has been proposed to analyze wormhole attack nature in ad hoc and sensor networks and existing methods of the defending mechanism to detect wormhole attacks without requiring any specialized hardware. The analysis is able to provide in establishing a method to reduce the rate of refresh time and the response time to become faster [5].

The purpose of the paper is to simulate the wormhole attack in wireless ad-hoc networks and MANETs using NS2 (network simulator-2) and study the impact on performance of the network. Even though NS-2 contains wireless ad-hoc routing protocols, it does not have any modules to simulate malicious protocols. Thus, to simulate Wormhole attack, a new protocol, Wormhole protocol was required. So, we started by writing a new AODV protocol using C++, and then edited it in order to inject wormhole behavior in it to simulate the Wormhole attack. Having implemented a new routing protocol which simulates the wormhole we performed tests on different adhoc networks scenarios to compare the network performance with and without wormholes in the network. The metrics used to measure the performance of the network are packet loss, end-to-delay and throughput. As expected, the parameters in the network were deteriorated considerably in the presence of a wormhole attack.

As the wormhole attack can have disastrous consequences, this paper contributes in the study of the impact of the wormhole attack in depth so that better prevention mechanisms can be employed against this attack. Also the detailed study of the paper helps in determining the vulnerability of the ad-hoc routing protocols so that they can be made more robust.

II. Significance of wormhole attack

While wormhole could be a useful networking service as this simply presents a long network link to the link layer and up, the attacker may use this link to its advantage. After the attacker attracts a lot of data traffic through the wormhole, it can disrupt the data flow by selectively dropping or modifying data packets, generating unnecessary routing activities by turning off the wormhole link periodically, etc. The attacker can also simply record the traffic for later analysis. Using wormholes an attacker can also break any protocol that directly or indirectly relies on geographic proximity. For example, target tracking applications in sensor networks can be easily confused in the presence of wormholes. Similarly, wormholes will affect connectivity-based localization algorithms, as two neighboring nodes are localized nearby and the wormhole links essentially 'fold' the entire network [6].

III. Simulation setup

Implementation of the "B"-protocol (modified aodv) to exhibit wormhole behaviour In this paper, we have used the nodes that exhibit wormhole behavior in wireless ad-hoc network that use AODV protocol. Since the nodes behave as a Wormhole they have to use a new routing protocol. So we simulated the wireless adhoc networks and MANETs using "B" routing protocol. In the scenarios we used 2 nodes which exhibit Wormhole behavior. Both UDP& TCP connections between sending nodes and destination nodes were setup, and CBR (Constant Bit Rate) application that generate constant packets through the UDP connection. CBR packet size is chosen to be 1000 bytes long; interval is set to 0.08sec. and the simulations were run and results were obtained from different scenarios using NS2 simulator [7]. NS2 gives output in two different forms i.e. NAM and trace files, we used both to analyse the results. All routing protocols in NS are installed in the directory of "ns-2.29". We started the implementing by duplicating AODV protocol in this directory and changed the name of directory as "B" (AODV Wormhole code). Names of all files that are labelled as "aodv" in the directory are changed to "B" such as B.cc, B.h, B.tcl, B_rqueue.cc, B_rqueue.h etc. except for "aodv_packet.h", as AODV and B protocol will send each other the same AODV packets. All classes, functions, structs, variables and constants names in all the files in the directory except struct names that belong to AODV packet.h code are to be changed. After the above changes, two common files that are used in NS-2 globally to integrate new "B" protocol to the simulator are changed. The changes are as follow. The First file modified is "\tcl\lib\ ns-lib. tcl" where protocol agents are coded as a procedure. When the nodes use "B" protocol, this agent is scheduled at the beginning of the simulation and it is assigned to the nodes that will use "B" protocol. Second file which is modified is "\makefile" in the root directory of the "ns-2.29". After all implementations are ready, compile NS-2 again to create object files. This is done using command make clean; make; make install. So far, a new routing protocol which is labelled as B is implemented.

Now to add wormhole behaviour into the new AODV protocol B/B. cc C++ file is modified. The wormhole nodes are strategically placed and the wormhole tunnel is formed. The two cases were used viz one without wormhole attack and the other with wormhole attack. We evaluated the results in both the cases and studied the effect on the performance of the network. The different topologies using various scenarios were simulated using the modified protocol on the wormhole nodes to display malicious behaviour in the wireless adhoc network as well as in the MANETs. In different scenarios we changed the source & destination position of the nodes including the node exhibiting the wormhole behaviour. "$ns_ node-config –adhocRouting B" statement changes routing protocol of the wormhole nodes node to "B" that was implemented in NS. After the participation in the network, we can make the adversary wormholes node disrupts the communication. We launched the wormhole attack in three ways:

A. Link down and up misbehaviour periodically to decrease the network performance,

B. Node down and up periodically, and

C. Packet dropping due wormhole nodes.

A. Link switching is done over the simulation time by the functions which have been modified in Aodv protocol;

```
"$ns rtmodel-at t1 down $wormhole node 1
$wormhole node 2
$ns rtmodel-at t2 up $wormhole node 1 $wormhole node 2"
```

B. Node down and up periodically;

```
"$ns rtmodel-at t3 down $wormhole node
 $ns rtmodel-at t4 up $wormhole node
 $ns rtmodel-at t5 down $wormhole node"
```

C. Packet drops by wormhole nodes ;

When a packet is received by the "recv" function of the "aodv/ aodv.cc", it processes the packets based on its type. If the received packet is a data packet, normally AODV protocol sends it to the destination address, but behaving as a Wormhole it drops all data packets as long as the packet does not come to itself. In the code below, the "if" condition provides the node to receive data packets if it is the destination. The "else" condition drops all remaining packets.

```
"if ((u_int32_t)ih->saddr() == index)
 forward ((b_rt_entry*) 0, p, no_delay);
 Else
   drop (p, drop_rtr_route_loop);"
```

Wormhole behavior is carried out as the malicious node receives an RREQ packet. When the malicious node receives an RREQ packet it immediately sends RREP packet as if it has fresh enough path to the destination. Malicious node tries to deceive nodes by sending such an RREP packet with highest sequence number of AODV protocol (4294967295) and low hop count. Values of RREP packet that malicious node will send are described below. The sequence number is set to 4294967295 and hop count is set to 1.

```
sendReply (rq->rq_src,     //IP Destination
1,          //Hop Count
index,                  //Dest IP Address
4294967295,    //Highest Dest Sequence Num
 MY_ROUTE_TIMEOUT,    //Lifetime
rq->rq_timestamp);              //timestamp
```

After all changes NS2 files are recompiled by make clean; make command.

IV. Results & Discussions

The simulated NAM outputs of different scena-rios are analyzed. The below scenario shows the ad-hoc topology in which node (5) & node (1) are the source nodes and node 6 & node 7 are destination nodes respectively. The CBR traffic is set as traffic generator for generating the traffic.

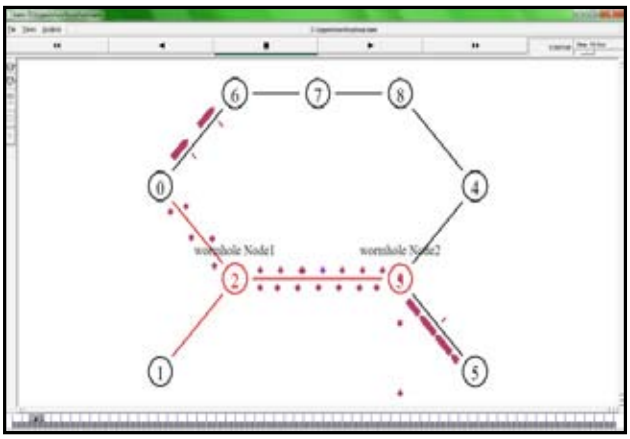


Fig. 1: Scenarios Showing More Drops Due Wormhole Node1

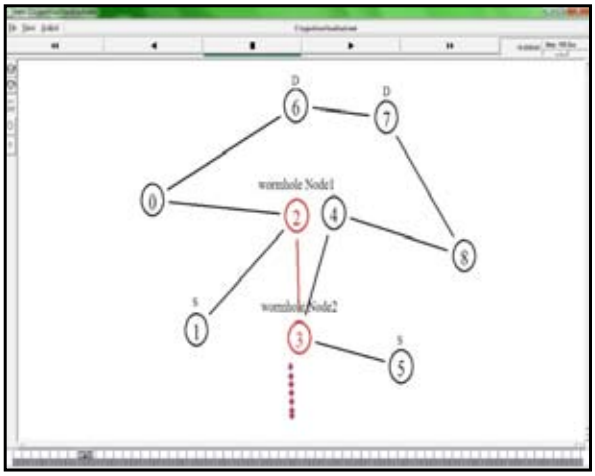


Fig. 2: Another Scenario Showing Wormhole Link Down & Drops

The simulations were extended to MANETs also to see the effect of wormhole attack. A MANET of 6 nodes was simulated. Only one node was set as wormhole and rest nodes as normal nodes.

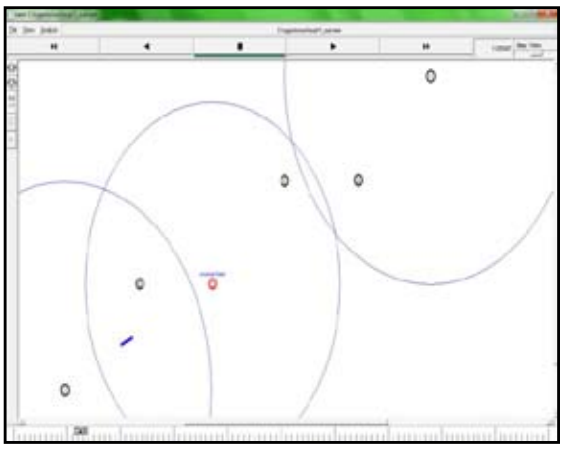
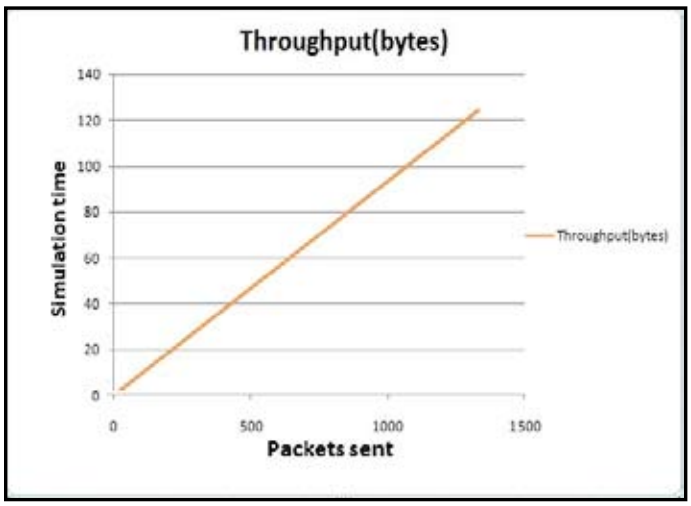
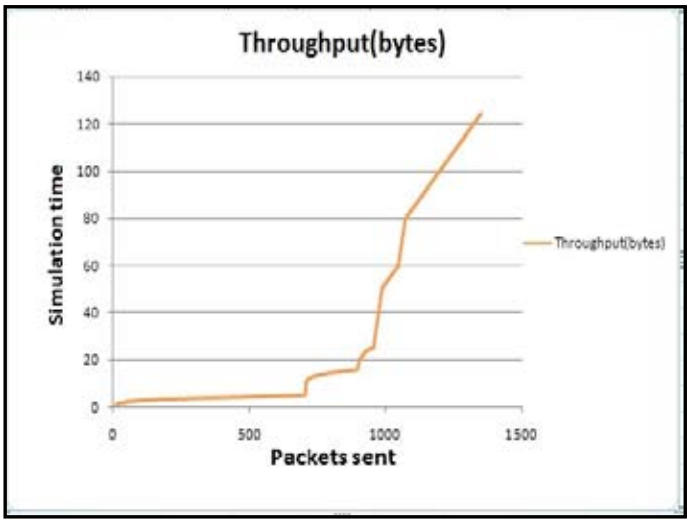


Fig. 3: Shows The Node 2 Set As Wormhole Node & Going Down



(a)



(b)

Fig. 4:(a). Shows Throughput Without Wormhole Attack (b) Shows Throughput With Wormhole Attack

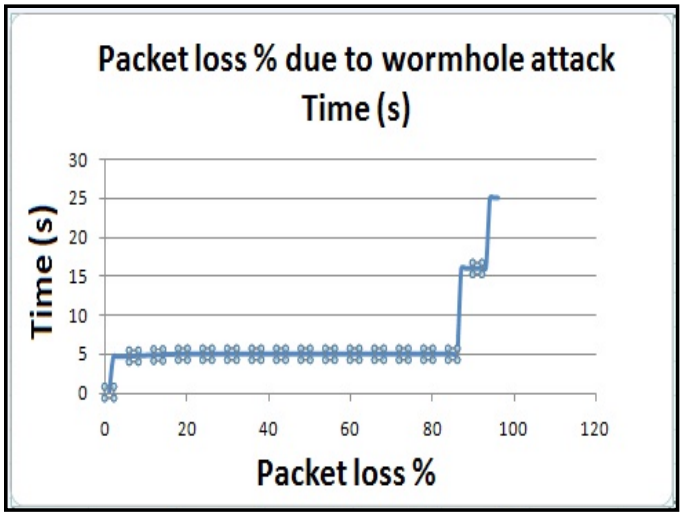
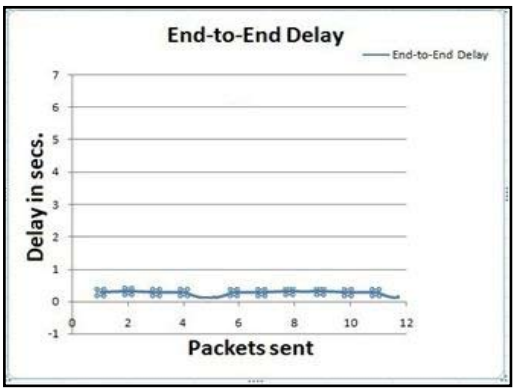
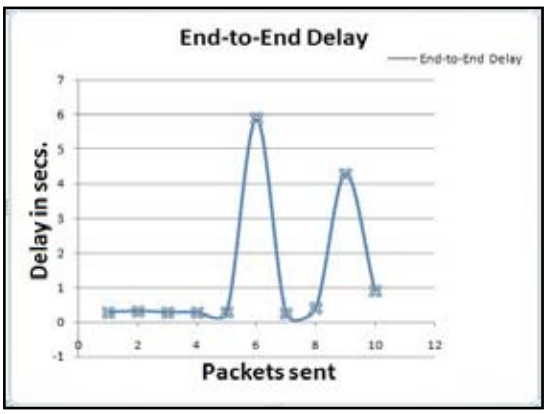


Fig. 5: Shows Packet Loss Due To Wormhole Attack



(a)



(b)

Fig. 6: (a). Shows End-to-End Delay Without Wormhole Attack (b). Shows End-to-End Delay Due to Wormhole Attack

A. Result Analysis

Thus we compared the results before and after the attack to see the impact of the wormhole attack on the network. The simulation using different scenarios has two malicious wormhole nodes that carries the wormhole attack and in the other simulations only one malicious node is introduced. In each case the wormhole nodes behave as legitimate users for a defined period of time in various scenarios. Then after a particular time of the simulation the wormhole nodes start misbehaving for a time interval. First we measured the packet loss due to node down and then due to the wormhole link down. Therefore we counted how many packets are sent by the sending nodes and how many of them reached the receiving nodes to get the lost packets. The results are obtained from the trace files and imported into the MS EXCEL. The excel sheets arrange the data into rows and columns and graphs show the effect on the parameters. Then we studied the throughput due to malicious behavior of the wormhole nodes. Therefore we counted the number of packets and size of the packets per unit time to get the throughput. Also the end –to- end delay introduced by the wormhole attack across the network is calculated to see the impact of wormhole attack. Our results show that the packet loss due to only one wormhole node is 56% and the loss in presence of two wormhole nodes increases to approximately 86%.Due to the presence of wormhole in the network the packet loss increases significantly. We concluded from the scenarios & results that the average packet loss in network with wormhole node is 86% and that of in normal AODV i.e. without wormhole attack is approx. 0.35%. The placement & number of wormhole nodes have been changed to evaluate the effect of the wormhole attack, as it is evident from the results that its impact on the results of different scenarios varies and increases with increase in the number of wormhole nodes. Also the throughput results from different scenarios are obtained e.g., the Throughput only reaches to 20% due to wormhole attack and decreases with the increase in the number of wormhole nodes. Whereas throughput calculated without wormhole attack is approximately 96% in normal conditions. Similarly we evaluated the effect on end-to-end delay after the wormhole attack from the trace files and the graphs plotted using MS Excel2010 clearly shows that the delay is increased to approx. 5.81 seconds for one packet transmission from sender to the receiver. While as the end-to-end delay without wormhole attack is approx. 0.21 seconds

V. Conclusion

Wormhole attacks in wireless adhoc networks can severely deteriorate the network performance and compromise the security through spoiling the routing protocols and weakening the security enhancements. In this paper we simulated the wormhole attack in AODV in wireless adhoc networks and Manet's and studied its impact on the performance of the network. For this purpose we modified & implemented a new AODV routing protocol which behaves as wormhole. We simulated different scenarios, where each one has one or two wormhole nodes that use the modified "B" AODV protocol. In different scenarios we changed the location of the wormhole nodes to evaluate the impact. Moreover, we changed the number of nodes in different topologies. The packet loss was measured. Similarly other parameters like throughput and end- to -end delay due to wormhole attack was calculated and results were produced in the form of graphs using MS Excel 2010. The main advantage of this paper is that it enlightens the vulnerabilities of the AODV protocol. Besides the study will help us to overcome the AODV protocol flaws so that it could be made more robust against the attack. Also the paper presents the overall measurement of the impact when a network is under the wormhole attack and helps in designing the topology which is more robust. The limitation of the simulation is that the measurement of the impact on MANETs becomes difficult when the mobility of the nodes increases too much. The possible application of this paper is that the study can help to determine the impact on other routing protocols and other layers also. Another application of our work is in determining the impact on sensor and mesh networks when under wormhole attack or other attacks as well.

References

[1] Y.C. Hu, et-al, "Packet leashes, A defense against wormhole attacks in wireless ad hoc networks", Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), April, 2003.

[2] Dezun Dong, Mo Li, et-al, "WormCircle, Connectivity-based Wormhole Detection in Wireless Ad Hoc and Sensor Networks", 15th International Conference on Parallel and Distributed Systems, 2009.

[3] Majid Khabbazian, et-al,"Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks", IEEE transactions on wireless communications, vol. 8, no. 2, 2009.

[4] Stephen Glass, Vallipuram Muthukkumurasamy, "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks", IEEE publication, 2009.
[5] Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", Proceedings of world academy of science, engineering and technology. vol 36, ISSN 2070-3740, Dec 2008.
[6] Ritesh Maheshwari, et-al, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information", IEEE INFOCOM.
[7] NS2, [Online] Available: http://www.isi.edu/nsam/ns.

Pirzada Gauhar Arfaat received his B.E. degree in Information Technology from Jammu University, J&K, India, in 2007, the M.Tech. degree in Communication & Information Technology from National Institute of Technology, srinagar, j&k, India, in 2010. At present he is engaged as assistant professor, with Department of Information Technology, National Institute of Technology, srinagar, j&k, India since 2010. His research interests include Computer Networks, network security, adhoc wireless networks, sensor networks, image processing.