ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

A Study of Behaviour And Performance Analysis Of Wormhole Attack In Mobile Ad-Hoc Networks

Karthik Pai B.H[1], Dr.Nagesh H.R[2], Dr.Niranjan N.Chiplunkar[3], Sharath Kumar[4]

Assistant Professor, Department of ISE, NMAMIT, Autonomous Institution under VTU, Nitte, Karnataka, India [1]
Professor and Head, Department of CSE, MITE, Institution under VTU, Moodabidri, Karnataka,India[2]
Principal, NMAMIT, Nitte, Autonomous Institution under VTU, Karnataka, India[3]
II year MTech, Department of ISE, NMAMIT, Autonomous Institution under VTU, Nitte, Karnataka, India [4]

ABSTRACT: The recent developments in the wireless technology and their wide-spread utilization have made remarkable enhancements in productivity in the corporate and industrial sectors. However, these recent developments have also introduced new security threats. Since the wireless shared medium is completely exposed to outsiders, it is susceptible to attacks that could target any of the OSI layers in the network stack. Wormhole attack is one of the most common DoS attacks in MANET. During the wormhole attack, a malicious node captures packets from one location in the network, and "tunnels" them to another malicious node at a different point (where other attacker is located), which replays them locally. In the wormhole attack, malicious nodes do not take part in finding routes, meaning that, legitimate nodes do not know their existence. AODV is an one of the well known on demand reactive routing protocol and it has been chosen for implementation of this attack for mobile ad hoc networks. Due to this malicious behaviour introduced by the malicious nodes all the data packets are not delivered to the destination under attacking scenario.

KEYWORDS: DoS, Wormhole attack, AODV, MANET

I. INTRODUCTION

A. *DoS Attack.*

Denial of Service (DoS) attack is one of the active network attack. An attacker actively participates and disrupts the normal operation of the network services[4]. A Denial of Service (DoS) is one of the intentional attempt made by malicious users or attackers to completely disrupt or degrade availability of service or resource to legitimate or authorized users. DoS attack may target on a specific component of computer, entire computer system, certain networking infrastructure, or even entire Internet infrastructure.

B. *Types of DoS attack.*

- Grayhole attack: It is a kind of DoS attack(active) in mobile ad hoc networks. It is specialized type of black hole attack which changes its state from honest to malicious and vice versa(based on the priority set) [3]
- Wormhole attack: In a wormhole attack, an attacker receives packets at one point in the network and sends it to the other point in the network(another attacker) by using a tunnel another node used to replays that to intended destination or even it may have some malicious activity such as dropping the packets [6][8].
- Blackhole attack: In this type of attack, attacker provides wrong information to its neighbours (in its vicinity) saying that it has route to the destination and starts malicious behaviour when it receives data packets[3].
- TCP SYN Flooding**:** A SYN flood is a form of denial of service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic[2].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

II. RELATED WORK

Wormhole attack is considered to be one of the most sophisticated forms of network attack in MANET[1][5]. In this attack, an attacker captures packets at one location, tunnels them to another location of the network, where it is retransmitted by another attacker. The tunnel can be established by using either out-of band private link (e.g., a wired link, or a long-range wireless transmission), or logical link via packet encapsulation. As a result, the tunnelled packets arrive either sooner or with less number of hops compared to the packets transmitted over multi-hop routes. Based on the tunnelling mechanism they use, wormholes can be classified into the following categories:
Out-of-band wormhole
In-band wormhole
The major differences between in-band and out-of-band wormholes are noted below:
a. In an out-of-band wormhole, the attackers create a direct link between the two end-points, whereas in-band wormhole does not use any external communication medium in between them.
b. Out-of-band wormhole requires special hardware to support the external communication medium between the two end-points of the attacker. On the other hand, in-band wormhole does not require any special hardware or special routing protocol.
c. In out-of-band wormhole, the tunnelled packets arrive faster compared to the multi-hop packets, but the in-band wormhole works comparatively slower than its counterpart. In both forms of wormhole, the attacker nodes create the illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbours.

A. *Different ways in which wormhole scenario can be created.*

- Wormhole attack by using packet encapsulation: In encapsulation-based wormhole attacks, several nodes exist between two malicious nodes and the data packets are encapsulated between the malicious nodes. Since encapsulated data packets are sent between the malicious nodes, the actual hop count does not increase during the traversal. Hence, routing protocols that use hop count for path selection are particularly susceptible to encapsulation-based wormhole attacks.
- Wormhole using high quality out of band channel: In this mode, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. This tunnel can be achieved, for example, by using a direct wired link or a long-range directional wireless link.
- Wormhole using high power transmission capability: In this type of wormhole attack, only one malicious node with high-power transmission capability exists in the network and this node can communicate with other normal nodes from a long distance.
- Wormhole using packet relay: Packet-relay-based wormhole attacks can be launched by one or more malicious nodes. In this attack type, a malicious node relays data packets of two distant sensor nodes to convince them that they are neighbours.

III. PROPOSED METHOD

Wormhole could be a useful networking service while it provides a long link to the link layer until and unless the attacker is not disturbing the ongoing transmission. However, the attackers may use the wormhole link for their own purposes. The existence of wormhole links can disrupt the routing mechanism in a number of ways. The attackers can attract a significant amount of traffic from their surroundings (saying that it had route to the destination). If the attackers keep the wormhole tunnel active at all times and do not drop any packets, they would actually perform a useful service for the network. But they can be also responsible for disrupting the data flow by selectively dropping few packets or modifying packets, generating unnecessary routing activities by turning off the wormhole link periodically.

In the below figures a two-hop wormhole attack scenario is represented, where A1 and A3 are the main attackers(active) and A2 acts as a relay node. The attackers A1 and A3 encapsulate RREQs packets received from the nodes in their locality, and then forward them to the tunnel node A2(relay node). The attackers decapsulate the packets received from the relay node A2, and then rebroadcast them in their vicinity. For example, RREQs from nodes D and M will be tunnelled from A3 to A1 and then rebroadcasted by A1 and received by nodes E, F and S. These nodes will reply with RREP to acknowledge the RREQ. As a result a source node, for example S, will select a route to a destination (e.g. node D) which passes through the wormhole tunnel.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

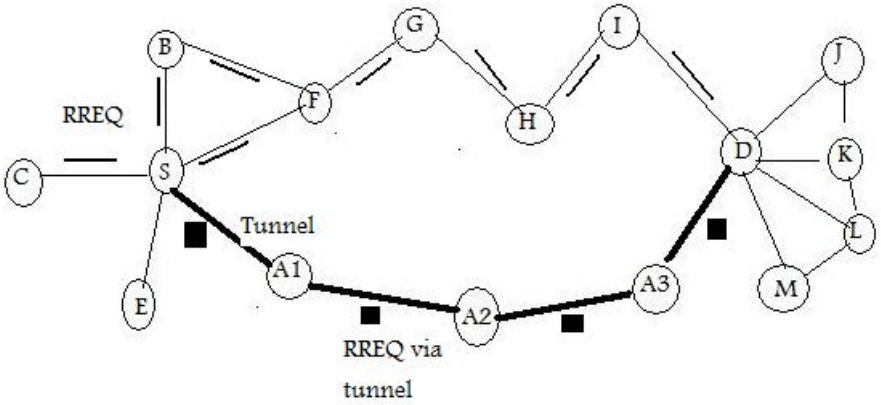

Fig 1. Route request from source to desination in the presence of wormhole

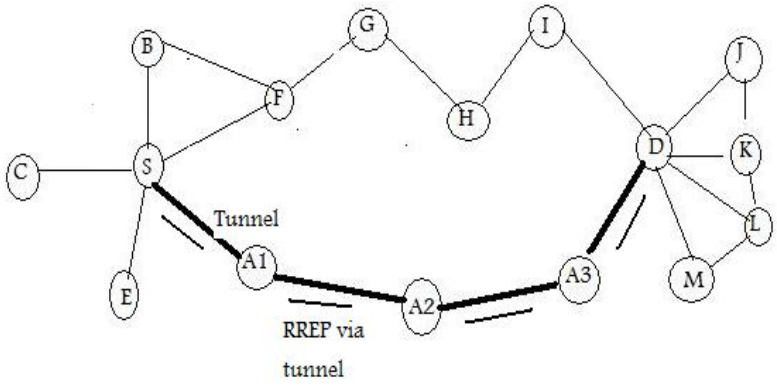

Fig 1. Route response from dest to source In the presence of wormhole.

IV. IMPLEMENTATION

Simulations are executed using ns-2 network simulator (ver-2.34) and new routing protocols are cloned to perform attack. While simulating the wormhole attack nodes which exhibit wormhole behavior use the protocol wormholeaodv[7]. For this purpose new routing protocol wormholeAODV is created. All the existing protocols in NS will be installed inside "ns-2.34". Intial step towards the project will be cloning mirror image of AODV protocol by replacing the name of the directory as wormholeaodv. Names of all files inside the newly created directory wormholeaodv is changed from aodv to wormholeaodv such aswormholeaodv.cc, wormholeaodv_rqueue.cc, wormholeaodv_rqueue.h etc. In this changed directory one file will be retained as it is that is aodv_packet.h, the reason behind this is both AODV and wormholeAODV protocol will send each other the same AODV packets.Even inside all these files all the function name structure variables class name and constant names also changed correspondingly except aodv_packet.h.

In order to simulate the wormhole attack behaviour receive function of the wormholeaodv.cc is changed. Here packets are processed based on its type. If the packet received is a data packet, under normal AODV it forward the packet towards destination, while behaving as a Wormhole it drops 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)
```

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

forward ((wormholeaodv_rt_entry*) 0, p, no_delay);
Else
drop (p, drop_rtr_route_loop);

A. *Wormhole creation*

Here special recv() and send() functions which can encapsulate the packet and decapsulate it at other end of the wormhole and replays it in the network. In implementation, instead of just creating a new packet type in which we can send the whole packet(which we want to encapsulate) as data we can just extend the existing IP header of the packet to hold the encapsulated packet values, which will get decapsulated(removed) at the other end of the tunnel. By decapsulation means that all the new values(extension part) of IP header will get zero as soon as it reaches other side of the tunnel and the old packet is dispatched from that node. The IP header is extended to include the new encapsulation parameters, these parameters are NULL by default for normal packets(by default the parameter values are 0 ,except for en_type which have default value as 0 & 2 for normal packets).
Following conditions are checked while processing the packet
if(ch->ptype() == PT_AODV **&& >en_type!=1**)) {
ih->ttl_ -= 1;
recvAODV(p);
return;
}

if(ih->en_type==1) //only 1 should be their if packet is encapsulated otherwise 0 and 2 are values for other normal packets.
{
decapsulate(p);
}

The encapsulation function (wormhole()), first checks if the node currently processing the packet is a wormhole or not. If the given node is defined as wormhole in the TCL, then the second function checks the SRC/DST of the packet and if this wormhole is defined for the packet's SRC/DST address, then the packet type is checked and accordingly the encapsulated parameters are set.
The decapsulate() function is called when the packet is received at the other end of the tunnel and this function again restores the packet to it's original form (in the form when packet is received by first node before encapsulation).
The decapsulation(), first checks the cmn_header of the packet and then the cases are defined how to decapsulate each specific packet (remove the encapsulated values and bring the packet back to it's original values(values packet have before entering the wormhole).

B. *Recompilation of NS-2*

Change the path to ~/ns-allinone-2.34/ns-2.34 and do $./configure (the Makefile will be replaced with modified one).
$make clean (it will recompile the whole ns2 and remove all the object files in NS2).
$make (removes all object files which are old and generates new object files).
#make install (login as superuser)
When the compile is finished, run the tcl script using
$ns wormhole.tcl

V. DETECTION TECHNIQUE

Our Proposal for the definition of Packet Delivery Fraction of system is to account for the maximal performance degradation (damage) that malicious users can inflict on the system using a specific amount of resources normalized by the performance degradation attributed to regular users using the same resources.

Packet Delivery Fraction (PDF) = þ (r)/þ (s) (1)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

Equation (1) proposes the new metric that evaluates the packet loss that occurs during communication. Formally we define packet delivery fraction as follows: Let r be the number of packets that has been received by the destination. Let s be the number of packets that has been sent by the source. It is the ratio of the data packets delivered to the destinations to those packets generated by the sources. Next, we use awk script to extract the values from the trace file for calculation of PDF.

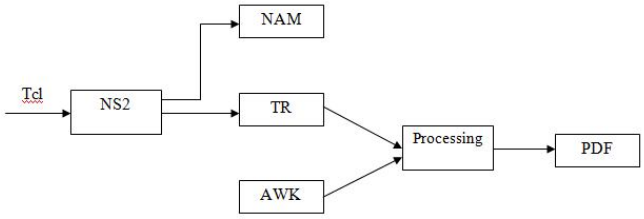

Fig 3. System Design of Detection Technique

VI. PERFORMANCE EVALUATION

The performance analysis of the wormhole attack is evaluated using the simulation tool Network Simulator-2 (NS-2). The performance parameter here is the packet delivery fraction. The results obtained are compared to the normal flow in the network without introducing the attacker(without making those two nodes as end of wormhole). The simulation is carried out with two different conditions

A. *Simulation under normal flow*

In this scenario, the simulation is performed when number of nodes will be 14, 18,22 and 26.which are distributed in a 500 x 500m boundary.Simulation is performed for 100 seconds with AODV routing protocol. We set the Radio Propagation model of wireless network as TwoRayGround reflection model and set the maximum transmission range of nodes as 250 meters. The medium Access Control (MAC) protocol is set to IEEE 802.11 and the bandwidth of the channel is set 10Mbps.First normal readings are taken for 14-26 numbers of nodes.

B. *Simulation under malicious flow*

In this scenario, required modifications are done in wormholeaodv.cc and wormholeaodv.h files.NS2 is recompiled after modifications. The TCL code for this scenario has only few changes as compared to the code for the previous scenario. In this code, an attacker node is introduced in tcl script with the set up time for next readings.

Table 1. Performance analysis of wormhole attack

No of nodes	PDF under normal flow	PDF under attacker
14	0.8846	0.2872
18	0.7642	0.3204
22	0.7236	0.2462
26	0.7442	0.2340

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 4, April 2014

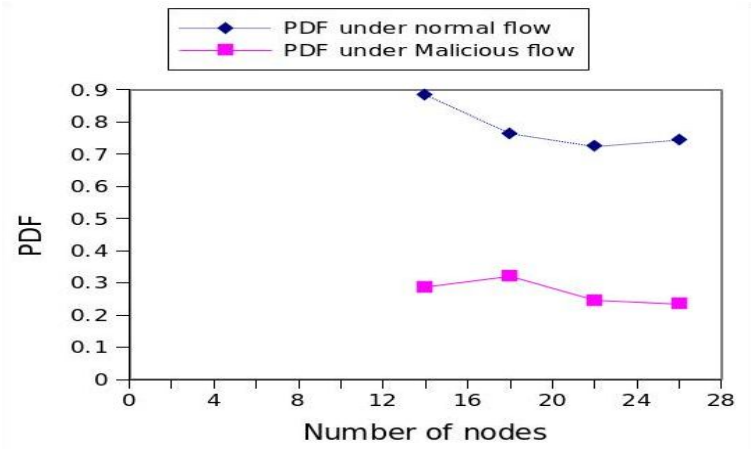

Fig 4. Performance analysis of wormhole attack

VII. CONCLUSION AND FUTURE WORK

Popular adhoc routing protocols are subject to wide variety of attacks which through the modification(changes) of routing messages. It can allow attackers to influence a victim's selection of routes or enable DoS attacks. Mobile adhoc network is likely to be attacked by Wormhole attack. For this we created wormhole aodv protocol with modification required to simulate wormhole behaviour and impact of this is studied in terms of packet delivery fraction. This also shows that these attacks degrade the overall network connectivity and data loss could show the existence of these attacks in the network. Packet loss is more in the network under these attacks. If the number of attacker is increased then the data loss would also be expected to increase. As a future work we can analyse the performance of MANET under byzantine attacking environment.

REFERENCES.

1. Mohammad Rafiqul Alam, "Detecting Wormhole and Byzantine Attacks in Mobile ad hoc Networks", International Journal of Computer Applications", may 2011.
2. Priyanka Goyal, Sahil Batra, Ajit Singh, "A literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications (0975-8887), Volume 9- No.12, November 2010.
3. Jhaveri R. H, Patel S. J.Jinwala D.C,"A Novel Approach for Gray Hole and Black Hole Attacks in Mobile Ad Hoc Networks
4. Saman Taghavi, James Joshi and David Tipper " A survey of defense mechanisms against distributed denial of service(DDoS) flooding attack.
5 Mohit Jain, Himanshu Kandwal A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks Majid Meghdadi, Suat Ozdemir and Inan Guler "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks"
5. Anil Kumar Fatehpuria, Sandeep Raghuwanshi An Efficient Wormhole Prevention in MANET Through Digital Signature.
6. Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay Different Types of Attacks on Integrated MANET-Internet Communication
8. A.VANI, D.Sreenivasa Rao A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks