Study of Attacks in AODV Protocol

[1]Khushboo Patel, [2]Dr. Pooja Chauhan
[1]Research Student, [2]Assistant Professor
[1,2]BITS, Varnama

Abstract

In today's life wireless networks are much easier to use rather than wired network. As wireless network is having more mobility and scalability it is used every now and then. Mobile Ad-hoc Networks(MANETs) is a collection of self-organized mobile devices forming a temporary network without any central infrastructure. In such network, nodes must co-operate with each other so as to extend their transmission range and transfer data from one part of the network to another one. The AODV protocol is an on-demand routing protocol which initiates a route discovery process only when there is data to be transmitted, to reduce the number of broadcast messages forwarded throughout the network. The different malicious attacks prevailing in the systems are such as black hole, gray hole, worm hole. But there is a certain drawback in MANETs, that it becomes prone to malicious attacks very fast. To avoid such attacks a good intrusion detection and prevention system is needed. Study and comparative simulation analysis of various malicious attacks, their detection and prevention algorithms in AODV(Ad-hoc On Demand distance Vector)will be carried out using MATLAB/NETWORK SIMULATOR(NS).

Keywords*- MANET, Ad-hoc, AODV, Security, Gray hole, Black hole, IDS*.

Introduction

A mobile Ad hoc network (MANET) is a collection of wireless mobile hosts that are organized and maintained in a distributed manner without a fixed infrastructure. The malicious nodes are either the broken node or the selfish node that becomes non-functional and silently drops the packets. Black hole attack and Gray hole attack are involved in dropping packets. Black hole attack drops all received packets intended for forwarding,

Whereas Gray hole attack drops packets at certain frequencies. A Black Hole attack can be done by just one node which forges the sequence number and hop count of a routing message in order to forcibly grab the route[1]. The Black Hole node will then eavesdrop, or directly drop the received data packets. A Gray Hole attack is a type of Denial of Services attack. Here the node forms false routing information in the network. A Gray Hole do not drop all the packets, it just drops a part of the packets.

Intrusion Detection is the process used to identify intrusions. Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent. IDS work on the basis of examining activity on a specific machine or network and decide whether the activity is normal or suspicious [3].

LITERATURE SURVEY:

TITLE	AUTHOR	METHOD	REMARKS
Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism	Nidhi Choudhary, Dr.Lokesh Tharani	Timer based approach is proposed.	There is more packet drops in mechanism used.
Security Issues of Black Hole Attacks in MANET	Rakesh Ranjan, Nirnemesh Kumar Singh, Mr. Ajay Singh	Security attacks are studied.the shortest path is used**.**	The confidentaility and integrity of data is not fulfilled.reliable network is not available everytime.
An Energy Aware Black hole Attack for Multipath AODV	Chaitali Biswas Dutta, Utpal Biswas	The nodes are made aware and so attack scheme is power aware.	Increases end to end delay and reduce packet-delivery ratio.

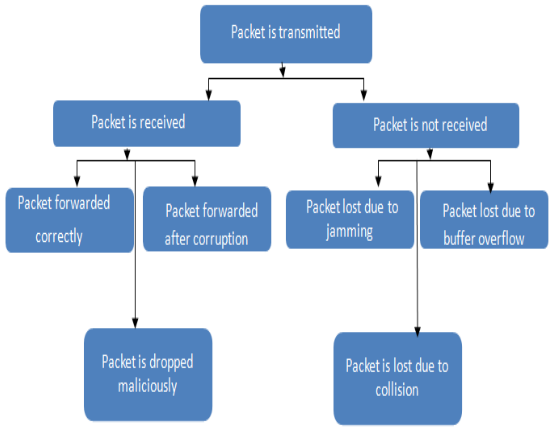
Packet is transmitted
Packet is received
Packet is not received
Packet forwarded correctly
Packet forwarded after corruption
Packet lost due to jamming
Packet lost due to buffer overflow
Packet is dropped maliciously
Packet is lost due to collision

FIG 1: Block diagram of malicious node attack

There are various attacks in AODV Protocols such as:

BLACK HOLE ATTACK:
In this attack a malicious node exploits the AODV vulnerabilities, by disseminating fake routing information

and announcing better routes to the requested destinations, to attract traffic through itself. Black hole attack is performed on two stages:
First the malicious node invades route at the discovery phase by advertising itself as having the freshness or the shortest routes to nodes whose packets it wants to intercept [5].

Afterward, the malicious node simply drops all data or control packets passing through it without any forwarding, however it runs the risk that neighbouring nodes will monitor and exposes the ongoing attack. The black hole can have more important impact when it is combined with other attacks such as wormhole and rushing attack [5].

GRAY HOLE ATTACK:
This attack is more sophisticated than the black hole attack, instead of dropping all data packets a malicious node selectively drops packets. It may drop packets originating from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes, which limits the suspicion of its wrongdoing[5]. It can also alternate by interval of time between malicious behaviour (dropping packets) and honest behaviour (forwarding packets).

In the simulation we define mobile node that move randomly and routing protocol use AODV, after that we send data using TCP and UDP technique and traffic and analyze the gray hole attack effect under that environment. The following required parameter define in table[9]:

Parameter	**Value**
Simulation Area	800*800
Mobile node	30
Mobility Model	Random way
Routing Protocol	AODV
Antenna	Omni-Directional
Attack Type	Gray hole
Simulation Time	100sec

Here, an IDS system for identifying Black Hole attack and Gray Hole attack is created under AODV protocol[3]. Most of the Black Hole attacks are invisible in the system and silently drops the packets from the incoming traffic without sending the message to the sender node that the packets have been dropped. While carrying out the simulation we defined the following simulation parameters.

STBO=R/H EXP (a)

We firstly created a protocol of Black Hole in AODV. For this the original AODV was copied and then modified to Black Hole AODV. We run the simulation using AODV and then repeated the test using Black Hole AODV over one node then slowly increasing it to ten Nodes.

The node which is programmed to exhibit Black Hole behaviour will follow a new protocol. As the simulation is carried out in AODV, we preferred to simulate Black Hole behaviour in AODV. We carried out the simulations using NS 2.35. Firstly duplicated the AODV protocol directory and renamed it as black hole aodv. This new directory is added after modification to NS to function as a black hole routing protocol.

Similar to the implementation of Black Hole AODV, we implement an Intrusion Detection System. The modified NS is compiled and installed thereafter. Simulations are carried out with Black Hole AODV and IDS AODV.

Here UDP protocol is used over CBR traffic for the simulations. In case of UDP protocol, the source node keeps on sending the packets even if the packets are being dropped, whereas in TCP, the Node finishes the connection if the return acknowledgement is not received. In case of UDP, we can also count the sent packets and the received packets separately as the UDP connection is not lost. These parameters are kept constant so that the exact network simulation is done for comparing with IDS AODV and Black Hole AODV against simple AODV.

The following parameters are calculated/analysed for the simulation criteria:

PACKET DELIVERY RATIO:
Packet delivery ratio is a ratio of the total number of packet receives by the genuine receiver to the total number of packet sends by the sender. Here we evaluate the PDR in presence of four to ten gray hole/black hole node as well as four to ten IDS nodes that cover almost entire network and get packet delivery ratio performance, here results shows where gray hole/black hole nodes present than maximum data dropped by the attacker node and decrease the packet delivery ratio but where we apply IDS node in network that performance have increases that is nearly 80% and gray hole/black hole case 52%. And calculated PDR increased 28% at the time of IDS present[6].

OVERHEAD RATIO:
This is the ratio of transmissions like RREQ, RREP and RERR[6]. Some routing packets like RREQ and QUERY packets are broadcast to all neighbours and packets like RREP and RRER travel along only in a single path.

ONE-END TO OTHER-END DELAY:
Compared to the approach our end-to-end delay is quite better. Usually the end-to-end delay is increased with higher the possibility of malicious nodes. We avoid the overhead in the system by avoiding the frequent checking of the malicious nodes that causes selective black hole attack. As the overhead is decreased involuntarily the end-to-end delay is decreased[7]. As for our approach is concerned, we implement promiscuous mode as soon the malicious node is detected. So it will avoid further data loss and our IDS nodes isolate the malicious nodes .Obviously, our overhead is decreased as such the end-to-end delay.

THROUGHPUT:
The amount of data transferred from one place to another or processed in a specified amount of time. Usually, the throughput value is indirectly proportional to the packet loss. AODV with the activation of Promiscuous mode always show good throughput value since it loss data packets in less rate[7].

The simulators used are the NS 2.35 with Linux

Conclusion

A proposed Behavioural and node performance based Gray hole/Black hole attack Detection and Amputation method in AODV protocol that provide the strength to secure communication between sender to receiver and through number of parameter base analysis finally concluded that detection technique detects nearly 90 to 96% of Gray hole/Black hole node and increases the network performance nearly 30 to 40%, it's also uses behaviour and drop status and node PDR base detection mechanism so in proposed method detection technique is more reliable and powerful as compare to existing detection mechanism..

References

[1] ShilaDevuManikantan, Cheng Yu, Anjali Tricha Channel-aware detection of selective black hole attacks in wireless mesh networks.

[2] Nasser and Y. Chen, “Enhanced Intrusion monitoring nodes with selection of Malicious nodes in mobile ad hoc networks,” in Proc. IEEE Int.Conf. on Communication (ICC’07), June 2007, pp. 1154-1159.

[3] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani, " A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE communications survey and tutorials, Vol. 10, no. 4, pp. 78-93,2008.

[4] J Arshad and M A Azad, "Perfonnance Evaluation of Secure on-Demand Rounting Protocols for Mobile Ad-hoc Networks", Sensor and Ad Hoc Communications and Networks, SECON'06, 2006 3'd Annual IEEE Communications Society on, vol.3, no., pp. 971-975, 28 Sept, 2006.

[5] A. Kush, R. Chauhan, C. Hwang and P. Gupta, "Stable and Energy Efficient Routing for Mobile Ad Hoc Networks", Proceedings of the Fifth International Conference on Information Technology: New Generations, ACM Digital Portal, pp. 1028-1033, 2008.

[6] C. Perkins, E. B. Royer, S. Das, " Ad hoc On-Demand Distance Vector (AODV) Routing Internet Draft", RFC 3561, IETF Network Working Group, July 2003.

[7] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks", Mobile Computing and Networking. (2000), pp., 255-265.

[8] Y. Hu, A. Perrig and D. B. Johnson, " A Secure On Demand Routing Protocol for ad hoc networks", 1. Wireless Netwroks, 11: pp. 2138,2002.

[9] Aswin Perti and Pradeep Sharma, "Reliable AODV protocol for wireless Ad hoc Networking", IEEE International Advance Computing Conference,Patiala, India (lCACC-2009), March 2009.

[10]Semih Dokurer, Y.M. Erten, and Can Erkin Acar, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks", IEEE Secure comm and Workshops, pp., 1-12,2006.

[11]Latha Tamilselvan and Dr. V. Sankaranarayanan, "Prevention of Blackhole Attack in MANEr", International Conference on wireless Broadband and Ultra Wideband Communication, 2007.

[12]Latha Tamilselvan and Dr. V. Sankaranarayanan, "Prevention of Cooperative Black Hole Attack in MANET", Journal of Networks, vol.3, No.5, pp. 13-20,2008.

.