

Comparative Study of Analysis of Black Hole Attack in MANET

Dr.Hariganesh S¹ Jemimma Ilakia Nancy.C²

¹Assistant Professor ²M.Phil. Scholar

^{1,2}Department of Computer Applications

^{1,2}Bishop Heber College (Autonomous), Trichirappalli

Abstract— Mobile ad-hoc network (MANET) is a collection of wireless mobile nodes dynamically forming a temporary network without any standard infrastructure. The network topology changes in MANET. manet cannot prevent itself from the attack. one of the attack is black hole attack. It creates the malicious node to get the packet itself. This survey paper says about attack on ad-hoc network using aodv protocol.

Key words: MANET, AODV RREQ, RREP, RERR, BLACK HOLE ATTACK, OPNET

I. INTRODUCTION

Mobile ad-hoc network (MANET) is a wireless nodes of connections. It is a decentralized system. Without any centralized access or the base stations the nodes communicate with each other. MANET act itself as a router and at a host at same time. MANET has the advantage of dynamic nature. its workstations are easy to handle. the limited transmission range and due to this multiple hops are needed. MANET works on TCP/IP structure in order to provide communication between the work stations. Manet provide efficient functionality of network.

II. AODV ROUTING PROTOCOL

AODV protocol is used to find a special route between source and destination. it has three types of messages, route request(RREQ), route reply (RREP) and route error(RERR), AODV has its capability of both unicast and multicast routing. When the network needs a connections then it broadcast a request for connections.if the route is not available.

III. BLACK HOLE ATTACK

The possible attack in the manet is black hole attack. in the black hole attack a malicious node send the message to the source node the it has the shortest path to the destination node. if this route is created, malicious node receives the data packet black hole attack is of two types:

A. Internal black hole attack

This attack is internally caused.the internal malicious node sits in between the routes of source and destination it make an internal attack in the active data riute element. it has the conducting attack inside of data transmission. this is called internal attack.

B. External black hole attack

This type of attack present externally outside of the network it won't access the network traffic in the network. External attack can be changed to internal attack when it gets control of the malicious node.

IV. COMPARATIVE STUDY OF BLACK HOLE ATTACK IN MANET

A. Related Works

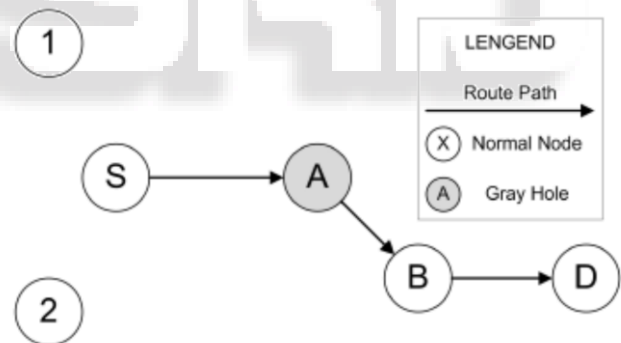
1) Irshad Ullah,Shoaib Ur Rehman[1]

analyzed the black hole attack on manet using different manet routing protocols and he used the approaches of OLSR and AODV and found it is not effective in DSR,TORA,GRP

Simulator Parameter	Value
simulator	OPNET 14.5
simulation time	300 ms
Traffic type	HTTP,FTP,VIDEO CONFERENCING

2) Surana K.A,Rathi S.T.B Thosar T.P And Snehal Mehatre[2]

faced the challenges of how to secure the black hole attack in routing protocol in manet and they used the dynamic leaning method In this detection it does not bother about wat is next hop or previous hope simply it passes messages to the destination path



3) E.A Mary Anita,V.Vasu Devan[3]

developed the prevention in multicast routing protocol for mobile ad hoc network based on demand distance vector using certificate chaining

Simulator	Ms	PDR	Attacker	Reciever
ODMRP	10	0.98	0	20
ODMRP	10	1.2	2	20
ODMRP	10	1	5	20

4) Shyamala Ramachandran,Valli Shanmugam[4]

Has the performance comparison of routing attack in manet and he used (LEACH)(PEGASIS)(GMR)(GPS) protocols to avoid the rushing attacks in manet

Attack	Percentage	Micro Second
Sybil attack	52.51%	100

Worm hole attack	51.16%	200
Black hole attack	44.12%	50
Rushing attack	44.16%	30

5) Ekta Barkhodia, Parulpreet Singh, Gurleen Kaur Walia[5]

Has the performance analysis of aodv, and has the traffic attack in manet and uses the opnet simulator

Simulator Parameter	Value
Simulator	OPNET 14.5
Simulation time	300 ms
Traffic type	HTTP, FTP, VIDEO CONFERENCING

6) S.Kurosawa, H.Nakayama and N.Kato[6]

the regular time intervals has been updated by using dynamic leaning method the no of node used here was 30 and Average detection has been analysed

Simulation Time	Nodes	Detection Rate	False Rate
1000	30	8% INCREASED	6% DECREASED

7) Pooja Jaiswal, Rakesh Kumar[7]

it is done by destination sequence number sent by the replying node and the difference between the source node and the intermediate node

Simulation Time	No Of Nodes	Pdr	End To End

1000	30-70	INCREASES	DECREASES
------	-------	-----------	-----------

8) M.Medadian, K.Fardad[8]

They proposed the solution of co-operative black hole attack by waiting for the node and for the safe delivery the node

Simulation Time	No of Nodes	PDR	End To End
0	30-50	INCREASES	DECREASES

9) M.Uma Parvathy, D.K Varughese[9]

Has found the black hole attack in route discovery mechanism by the extension of aodv protocol. The simulation results show the proposed protocol.

Simulation Time	No Of Nodes	PDR	Throughput
500	50	INCREASES	BETTER AVERAGE THROUGHPUT

10) N.Mistry, Dc Jinwala[10]

The black hole attack can be analyzed by using AODV protocol by packet delivery ratio here he used 25 nodes which is increased by 90%

Simulation Time	No Of Nodes	PDR	End-To-End Delay
300 sec	25	INCREASES by 90%	BETTER AVERAGE THROUGHPUT

V. COMPARATIVE TABLE OF BLACK HOLE ATTACK DETECTIONS

Title Of The Paper	Routing Protocol	Tools Used	Detection Type	Year	Results
Irshad Ullah, Shoib ur Rehman	OLSR, AODV	OPNET	HTTP, FTP	2010	Throughput of aodv is effected of twice compare of olsr
Suranta k.A, Rathi S.B, Thosar T.P And snehal Mehatre	AODV	Dynamic Leaning Metho D	Single Detection	2012	It initiates single route discovery process

E.A Mary Anita, v.vasudevan	PDR	Odmrp	Co-Operative Detection	2007	Increased The Mobility Of Nodes
Shyamala Ramachandran, Villi Shanmugam	NS2	Leach	Co-Operative Detection	2013	Resist The Attack And Enhance Its Performance
Ekta Barchodia, Parul Preet Singh, Gurleen Kaur Walia.	DSR	Opnet	Http,Ftp	2012	Throughput Is High In Video Conferencing
S.Kurosawa, H.Nakayama and N.Kato	AODV	Ns2	Single Detecton	2007	Shows Effect In Detecting Black Hole Attack
Pooja Jaiswal, Rakesh Kumar	AODV	Ns2	Single Detection	2012	Decreases Pdr End To End Delay
M.Medadian, K.Fardad	AODV	Glomosim	Co-Operative Detection	2012	Additional Delay Over Head
M.Umaparvathi, D.K Varughese	AODV	Ns2 Co-Operative Detection	Co-Operative Detection	2012	Bette Performance In Terms Of Pdr & Throughput
Mstry.N, Jinwala Dc, Iaeng, Zaveri.M	AODV	Ns2	Single Detection	2010	Pdr Is Improved By Approximately 80%.

VI. SUMMARY

Thus from this comparative study the opnet simulator gives the most effectiveness.

REFERENCES

- [1] IRSHAD ULLAH ,SHOAIB UR REHMAN
Analysis of Black Hole Attack on MANETs

Using Different MANET Routing Protocols
School of Computing
Blekinge Institute of Technology
Thesis no: MEE 10:62
june, 2010

- [2] Suranta k .A, Rathi S.B, Thosar T.P And Snehal Mehatre
“securing black hole attack in routing protocol aAODV in manet with watch dog mechanisum”

World research journal of computer architecture
ISSN:2278-8514&ISSN :2278-8522

Volume 1, issue 1,2012,pp[19-20]

- [3] E.A Mary Anitha,V.Vasudevan
Performance Evaluation and Comparison of On Demand Multicast Reactive Routing Protocols under Black Hole Attack in MANET
International Journal of Security, (IJS) Volume(3), Issue(4)
- [4] Shyamala Ramachandran,Villi Shanmugam.
“performance comparison of routing attack in manet &wsn”
International journal of ad-hoc sensor & ubiquitous computing(IJASUC)
Vol 3,no 4 august 2012.
- [5] Ekta Barchodia,Parul Preet Singh,Gurleen Kaur Walia.
international Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2012
DOI : 10.5121/ijdps.2012.3308 75
Evaluation of various Traffic loads in MANET with DSR routing protocol through use of OPNET Simulator
- [6] S. Kurosawa, H. Nakayama, and N. Kato,
“Detecting black hole attack on AODV based mobile ad-hoc networks by dynamic learning method,”
International Journal of Network Security”, pp. 338–346, 2007.
- [7] Pooja Jaiswal, Rakesh Kumar,” International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No5, October 2012, “Prevention of Black Hole Attack in MANET”.
- [8] M. Medadian, K. Fardad, “European Journal of Scientific Research, Vol. 69 No. 1 (2012),“Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol”.
- [9] M. Umaparvathi, D.K. Varughese, “European Journal of Scientific Research, Vol. 72 No. 3” (2012), “Two Tier Secure AODV against Black Hole Attack in MANETs”.
- [10] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) “Improving AODV Protocol Against Blackhole Attacks”, Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010.