A Review on Simulation of Black Hole Attack in Network using AODV Routing Protocol on Ns2

Bright Keswani[+], Bijendra Bansal[#], Poonam Keswani[*], Rakhi Purohit[&]

[+]*Professor, Department of Computer Applications, Suresh Gyan Vihar University, Jaipur, India*

[#]*Research Scholar, Suresh Gyan Vihar University, Jaipur, India*

[*]*Assistant Professor, Akashdeep PG College, Jaipur, India*

[&]*Assistant Professor, Poornima Institute of Engineering and Technology, Jaipur, India*

Abstract- Wired or wireless networks are becoming famous in recent years. Presently every electronic gadget is operated withhelp of such Network. It has been observed that wireless ad hoc network are suppose to more vulnerable to protection threats as compare to wired network due to inherent characteristics and system constraints. Research paper is addressing attacks due to malicious nodes. Paper is examining influence of Black Hole attack over AODV routing. The detection mechanism is also discussed in this several research. Simulation of such attacks and determination of effect of such attack on network performance by various network scenario has been discussed in several studies. Many researches have implemented detection mechanisms that help to isolates malicious node innetwork. This paper has focused onexisting research performed to simulate AODV protocol.

Keywords- Network simulation, Routing protocol, AODV, Black hole attack, NS2

I. INTRODUCTION TO NETWORK SIMULATION

NS is a name for a series of discrete event network simulators, specifically ns-1, ns-2, ns-3 and ns-4. All are discrete-event computer network simulators, primarily used in research and teaching. NS2 is an open-source simulation tool that runs on Linux. It is a discreet event simulator targeted at networking research and provides substantial support forsimulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired and wireless (local and satellite) networks.In ns2 nodes could be connected in two ways, simplex and duplex. Simplex connection enables one-way communication and duplex connection enables two-way communication. Each type require bandwidth, delay and type of queue for configuration. Different types of Queue available in ns2 are DropTail, RED, CBQ, FQ, SFQ, DRR.

II. LITERATURE REVIEW

In [1] Rutvij H. Jhaveri route detection process of default AODV inoccurrence of an attacker. Source node S Wishes to send data to target D broadcast RREQ; A malicious node MN replies back with RREP enclosingabnormally high destination sequence number misleading S as if it has a fresher route to D; another normal intermediate node IN sends RREP having acceptably higher sequence number.

In [2] GengPeng, ZouChaanyun presented Routing Attack and Solutions in Mobile ad hoc Network" IEEE-2006. A security routing mechanism based on common neighbor listening is proposed. In this mechanism, trust_value and trust_threshold are defined to evaluate a node's credit standing and judge whether a node is a malicious node or not. The common neighbor which holds biggest trust_value is chosen to listen tonetwork. The mechanism could react quickly and effectively protectnetwork from kinds of attacks when some malicious nodes occur inAd hoc network. Onceroute is destroyed by malicious node, common neighbor will search another route todestination during a route discovery phase. The mechanism could reinforcesecurity of on-demand protocols such as Ad hoc On-demand Distance Vector and Dynamic Source Routing. The performance of common neighbor listening mechanism in AODV is justified by computer simulation.performance of common neighbor listening mechanism is evaluated by computer simulation using ns-2. In [3] and [4],author's have introducedroute confirmation request and route confirmation reply to avoidblack hole attack. In this approach,intermediate node not only sends RREPs tosource node but also sends CREQs to its next-hop node towarddestination node. After receiving a CREQ,next-hop node looks up its cache for a route todestination. If it hasroute, it sendsCREP tosource node. Upon receivingCREP,source node could confirmvalidity ofpath by comparingpath in RREP andone in CREP. If both are matched,source node judges thatroute is correct. One drawback of this approach is that it cannot avoidblack hole attack in which two consecutive nodes work in collusion, that is, whennext-hop node is a colluding attacker sending CREPs that supportincorrect path.

In [5], authors Satoshi Kurosawa et.al. have introduced an anomaly detection scheme to detect black hole attack using dynamic training method in whichtraining data is updated at regular time intervals to expressstate ofnetwork. In this scheme,average ofdifference betweenDst_Seq in RREQ packet andone held inlist are calculated and this operation is executed for every received RREP packet. The average of this difference is finally calculated for each timeslot and it taken asfeature. Hence, it consumes considerable amount time to do calculations for every RREP packet.

In [6] C. Perkins introduced Ad hoc On-Demand Distance Vector (AODV) Routing and in [7] Y-C. Hu, A. Perrig, and D. Johnson made research on Wormhole Attacks in Wireless Networks. In [8] Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection was presented byYibeltalFantahumAlem& Zhao HhengXaun from Tainjin.K. Natarajan and Dr. G. Mahadeven[9] presented Succinct Comparative Analysis and Performance Evaluation of MANET Routing Protocols. Michalis Papadopoulos, Constandinos X. Mavromoustakis and GeorgiosSkourletopoulos[10] made Performance Analysis of Reactive Routing Protocols in Mobile Ad hoc Networks.In [11] Performance Measurement in MANET has been made by Sandeep Kumar Arora, Mubashir. AkshaiAggarwal[12] performed Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs). M. Shobana [13] did Performance Analysis and Comparison of various Routing Protocols.

III. AODV ROUTING PROTOCOL

AODV maintains routing information for only active routes. This protocol is based on two mechanisms (1) Route discovery (2) Route maintenance [13]. Each node has two counters.

1. Sequence number which is used to find outnew route.
2. Broadcast ID. If sequence number of requested route packet is larger thansequence number of destination node than this route is a fresh route otherwise intermediate nodes will reply to source node.

There are four types of data packet message:

RREQ: When a packet is to be sent todestination by a source node, than a message is broadcasted todestination node through intermediate node. This message is known as Route Request (RREQ) message. RREQ packet consists of source and destination sequence number, broadcast ID, source address, and destination address. The Request id is increased by one every time when source node sends new RREQ. Thus it helps in identifying RREQ uniquely throughcombination of source address and broadcast id. Each RREQ holds a value that indicatesnumber of times it could be re-broadcasted.

RREP: Destination node sends Route Reply (RREP) packet todestination using reverse path as a reply to RREQ RREP packet contains source address, destination sequence number, and destination address. The reason for unicasting RREP message is that every forwarding node cachesroute back tosource.

RERR: Route Error Message is sent when there is a path failure or link breaks and when RREQ cannot be reached at destination. RERR packet includes unreachable destination sequence number, unreachable destination address and source address [6]**.**

HELLO: It needed for link status monitoring and for broadcasting connectivity information. A node should use this messages only if it is part of an active route.

As source node need to send data to destination than AODV uses HELLO messages to discover path to destination through intermediate nodes. Each active mobile node transmits this messages in particular time interval to check if there is a path or not. If intermediate node does not receives multiple HELLO messages at regular interval from its neighbors than there is a no path. After path confirmation, source node floods RREQ packet towards destination. When an intermediate node receives RREQ packet, it checks its duplicity. If this RREQ packet is duplicate than it ignores it otherwise forward it towards destination. When reached to destination node, destination node will create a route reply packet and send it back tosource node using reverse path. When source node receives RREP packet, it storespath todestination and will startcommunication. Whensource node receives multiple RREP packet, it selectsshortest path. In case of a link break towardsdestination, intermediate node will generate Route Error packet and sends it to source node.Source node will delete that route and restartroute discovery process [9].

IV. BLACK HOLE ATTACK

Black Hole Attack is a type of Denial-of-services (DOS) attack. This is also called Sequence Number Attack(SNA) because it is created by sequence number. Sequence number is monotonically increasing number and maintained by originator node ofRREQ and RREP message innetwork [8]. AODV routing protocol includes key features such as RREQ and RREP (For route discovery), RERR and HELLO message (For route maintenance), sequence number and hop count. AODV routing protocol has every route entry is assigned by destination sequence number inrouting table. RREQ and RREP message contains several of fields. In Black Hole attack a malicious takesadvantage of sequence number and attacker node receivingRREQ message fromneighboring node and more increase value ofdestination sequence number and send reply message tosource node. Higher value of sequence number signifies fresh information of network. So source node accepts route reply message frommalicious node and ignores less destination sequence number route reply message. Network traffic redirects throughmalicious node.

When source node S wants to send data packet to destination node D, It creates route discovery process by using RREQ message having destination sequence number suppose 7 send to neighboring node A, B, C and F. When neighboring node receive RREQ message from source node S it updates routing table and further rebroadcast to their neighboring nodes. Each RREQ message is uniquely identified by using RREQ-Id and Source IP address that eliminate duplicates. Route reply message (RREP) is generated by either any intermediate node having fresh route information todestination or destination node.

V. DETECTION PROCESS FOR BLACK HOLE ATTACK

Detection process is very difficult in Mobile Ad hoc network due to limited resources such as bandwidth, battery life and storage capacity. We should also concern minimum possible rise in routing overhead and delay to implement any detection process.

Algorithm and Flow diagram of Detection process

This Algorithm is designed to identify and isolateAttacker nodes inMANET. In this approach Source node identifiesAttacker nodes inMANET with help of much more Differences of Sequence number of Source node and Destination nodes.

SN : Source Node Id
DN : Destination Node Id
RREQ : Route Request
RREP : Route Reply
DSN : Destination Sequence Number
SSN : Source Sequence Number
AN : Attacker Node

Step 1: Initialization process
StartRoute discovery process with SN and DN by using RREQ and RREP packets

Step 2:Storing process RREP packets
SN created a new routing table name as newm_routingTable to store all RREP packets for preprocessing of all RREP packets

Step 3: Identification and elimination of Attacker Nodes

```
While (newm_routingTable is not Empty)
{
Retrieve first entry from new routing table and determined which DSN is Much more difference with SSN then entry will be added in blacklist and discard them
}
```

Step 4: Route selection process
After step 3 a new route is selected from newm_routingTable byDSN

Step 5: Calling normal process of Aodv routing
Called Recv Reply process of Aodv routing protocol

Step 6: Repeat step 3 to step 5 for each AN in network

Step 7: End

In normal AODV, node that receives RREP packet first checks value of sequence number in its routing table. The RREP packet is accepted if it has RREP_seq_no higher than one in routing table. Our proposed solution provides an addition check to find whether RREP_seq_no is higher than much differences as threshold value. The threshold value is average of difference of dest_seq_no in each time slot between sequence number in routing table and RREP packet. As value of RREP_seq_no is found to be higher thanthreshold value, node is suspected to be attacker node and it addsnode toblack list. The source node shares this information with neighboring nodes byattacker node identification. So that neighboring nodes know that RREP packet fromattacker node is to be discarded. Further, if any node receives RREP packet, it looks overlist, ifreply is fromblacklisted node; no processing is done forsame. ItRREP packet, it looks overlist, ifreply is fromblacklisted node; no processing is done forsame. It simply ignoresnode and does not receive reply from that node again.

VI. CONCLUSTION AND SCOPE OF RESEARCH

Black Hole attack is big serious problem in network. A malicious node reducenetwork performance when number of malicious nodes innetwork increased. It has been observed that packet delivery ratio is decreased in such cases. Several researches analyzed behavior of routing protocol and determinedeffect of Black Hole attack on AODV routing and its detection mechanism using NS2 simulators.

In future it has been determined effect of Black Hole attack over AODV protocol would be observed in Fuzzy logic based network. In such network, nodes would perform transmission onbasis of fuzzy logic. The fuzzy logic would considervalue between 0 and 1 and selectnodes on random basis instead of sequential selection.

REFERENCES

[1]. Rutvij H. Jhaveri,Sankita J. Patel,Devesh C. Jinwala "Improving Route Discovery for AODV to Prevent Black hole and Grayhole Attacks in MANETs", INFOCOMP 2013.

[2]. GengPeng, ZouChaanyun "Routing Attack and Solutions in Mobile ad hoc Network" IEEE-2006.

[3]. Y.Zhang and W.Lee,"Intrusion detection in wireless ad-hoc networks", 6th annual international Mobile computing and networking conference proceedings, 2000.

[4]. Seungjoon Lee, Bohyung Han, Minho Shin; "Robust Routing in Wireless Ad Hoc Networks" 2002, international Conference.

[5]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007, PP:338-346.

[6]. C. Perkins, E. Belding-Royer, S. Das, "RFC-3561 Ad hoc On-Demand Distance Vector (AODV) Routing", pp. 1-32, July 2003.

[7]. Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks", IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[8]. Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection by YibeltalFantahumAlem& Zhao HhengXaun from Tainjin 300222, China 2010, IEEE.

[9]. K. Natarajan and Dr. G. Mahadeven, "A Succinct Comparative Analysis and Performance Evaluation of MANET Routing Protocols", IEEE (ICCCI -2013), Jan. 04 – 06, 2013, Coimbatore, INDIA.

[10]. Michalis Papadopoulos, Constandinos X. Mavromoustakis and GeorgiosSkourletopoulos", Performance Analysis of Reactive Routing Protocols in Mobile Ad hoc Networks", 2014 International Conference on Telecommunications and Multimedia (TEMU),IEEE.

[11]. Performance Measurement in MANET BY Sandeep Kumar Arora, MubashirYaqoobMantooMahnazChishti and NehaChaudhary, 2014 5th International Conference-IEEE.

[12]. A Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs) by AkshaiAggarwal, NirbhayChaubey and Keyurbhai A Jani from Gujrat, India 2013, IEEE.

[13]. A Performance Analysis and Comparison of various Routing Protocols in MANET by M. Shobana and Dr. S. Karthik from Coimbatore-641035, 2013, IEEE.