© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 04 | October - December 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in
Peer Reviewed and Refereed Journal

BLACK HOLE ATTACK IN NETWORK USING AODV ROUTING PROTOCOL ON NS2: A REVIEW

Shivneet Singh
Email id :- redhu.shivneet3@gmail.com

ABSTRACT: In recent years, wired and wireless networks have become more popular. These days, the Internet is required to run any modern device. It has been noted that owing to their intrinsic features and system limits, wireless ad hoc networks are thought to be more susceptible to security risks than wired networks. This research article discusses assaults caused by malicious nodes. This paper will look at the effects of the Black Hole attack on AODV routing. This several studies also explore the method of detection. Numerous papers have addressed the challenges of simulating these assaults and determining their impact on network performance across a variety of network scenarios. Researchers have developed and deployed a wide variety of detection algorithms that may pinpoint a single rogue node in a network. Existing research undertaken to replicate AODV protocol has been the topic of this work.

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

[1] INTRODUCTION TO NETWORK SIMULATION

NS is the brand name for a family of discrete event network simulators that includes ns-1, ns-2, ns-3, and ns-4. They are all computer network simulators that employ discrete events for testing and education. NS2 is a free and open-source Linux-based simulation program. It is a discrete event simulator designed for use in networking research, and it has extensive support for simulating routing, multicast protocols, and Internet Protocol (IP) protocols including UDP, TCP, RTP, and SRM over wired and wireless (local and satellite) networks. Both simplex and duplex connections were available between nodes in ns2. You can only send information in one direction with a simplex connection, but two-way conversations are possible with a duplex one. Bandwidth, latency, and queue type must be configured differently for each kind. The Queues in ns2 come in a variety of forms, including DropTail, RED, CBQ, FQ, SFQ, and DRR.

[2] LITERATURE REVIEW

In [1] Rutvij H. Jhaveri route detection process of default AODV in occurrence of an attacker. Source node S Wishes to send data to target D broadcast RREQ; A malicious node MN replies back with RREP enclosing abnormally 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] Geng Peng, Zou Chaanyun 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 to network. The mechanism could react quickly and effectively protect network from kinds of attacks when some malicious nodes occur in Ad hoc network. Once route is destroyed by malicious node, common neighbor will search another route to destination during a route discovery phase. The mechanism could reinforce security 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 introduced route confirmation request and route confirmation reply to avoid black hole attack. In this approach, intermediate node not only sends RREPs to source node but also sends CREQs to its next-hop node toward destination node. After receiving a CREQ, next-hop node looks up its cache for a route to destination. If it has route, it sends CREP to source node. Upon receiving CREP, source node could confirm validity of path by comparing path in RREP and one in CREP. If both are matched, source node judges that route is correct. One drawback of this approach is that it cannot avoid black hole attack in which two consecutive nodes work in collusion, that is, when next-hop node is a colluding attacker sending CREPs that support incorrect path.

In [5], authors Satoshi Kurosawa et.al. have introduced an anomaly detection scheme to detect black hole attack using dynamic training method in which training data is updated at regular time intervals to express state of network. In this scheme, average of difference between Dst_Seq in RREQ packet and one held in list 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 as feature. 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 by Yibeltal Fantahum Alem & Zhao Hheng Xaun 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 Georgios Skourletopoulos[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. Akshai Aggarwal [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.

[3] AODV ROUTING PROTOCOL

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 04 | October - December 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in
Peer Reviewed and Refereed Journal

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 out new route.
2. Broadcast ID. If sequence number of requested route packet is larger than sequence 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: A source node broadcasts a message to an intermediate node, which then broadcasts the message to the destination node. The RREQ acronym stands for "Route Request" in this context. The components of an RREQ packet are a sequence number, a broadcast identifier, an address pair (source and destination), and an address pair (source and destination). When a source node transmits a new RREQ, the Request id is incremented by 1. Consequently, it aids in the unambiguous identification of RREQ by combining the source address with the broadcast id. The potential rebroadcastings for a given RREQ are stored as numbers.
RREP : Destination node sends Route Reply (RREP) packet to destination 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 caches route back to source.
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.

WORKING OF AODV
To figure out how to get data from a source node to its final destination, AODV sends out HELLO messages to the intermediate nodes along the way. At regular intervals, any mobile node that is actively communicating with others will send out such signals to determine whether a route exists. Unless an intermediary node is receiving repeated HELLO signals from its neighbors at predetermined intervals, there is no route. After determining the best route, the sending node will send a barrage of RREQ packets in the direction of the receiver. As soon as an intermediate node receives an RREQ packet, it does a duplicate-packet check. When checking for duplicates, this RREQ packet is dropped; otherwise, it is sent on to its intended recipient. If the packet successfully reaches its final destination, the receiving node will generate a route reply packet and transmit it back over the same path it took to get there. The node that received the RREP packet will then

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 04 | October - December 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in
Peer Reviewed and Refereed Journal

save the route to the target and initiate communication. Any time a source node gets more than one RREP packet, it will choose the one that takes the shortest route. When an intermediate node detects a failure along the path to the destination, it will create a Route Error packet and transmit it on to the sending node. The route will be removed and the route discovery process will begin again at the source node [9].

[4] BLACK HOLE ATTACK

This is a DOS assault known as a Black Hole Attack. Since this is generated using a sequence number, it has another name: Sequence Number Attack (SNA). The network node that initiates an RREQ or RREP message keeps track of the sequence number, which increases monotonically [8]. The RREQ and RREP messages (for route discovery), the RERR and HELLO messages (for route maintenance), the sequence number, and the hop count are all essential components of the AODV routing protocol. Each route entry in the routing table used by the AODV routing protocol is numbered based on the order in which the destinations are reached. A number of fields may be found in RREQ and RREP messages. With the use of sequence numbers, Black Hole attackers may send a reply message to the source node after receiving an RREQ message from a nearby node, which then increases the value of the destination sequence number. A greater sequence number indicates more recently acquired network data. Because of this, the source node will accept the route reply message from the malicious node and will disregard the route reply message with the lower destination sequence number. Network traffic redirects via rogue node.

WORKING OF BLACK HOLE ATTACK

A RREQ message with a destination sequence number of 7, for example, is sent from a source node S to its surrounding nodes A, B, C, and F in order to initiate a route discovery procedure that would ultimately lead to the successful transmission of a data packet to a destination node D. After receiving an RREQ message from node S, the surrounding node adjusts its routing table and broadcasts the change to its neighbors. It is the combination of the RREQ-Id and the Source IP address that ensures no two RREQ messages will ever be received with the same contents. Any intermediate node that has up-to-date route information to the destination, or the final destination itself, may send a route reply message (RREP).

[5] 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 isolate Attacker nodes in MANET. In this approach Source node identifies Attacker nodes in MANET with help of much more Differences of Sequence number of Source node and Destination nodes.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 12 Issue: 04 | October - December 2021
Paper is available at http://www.jrps.in | Email : info@jrps.in
Peer Reviewed and Refereed Journal

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
Start Route 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 by DSN
Step 5: Calling normal process of Aodv routing
Called RecvReply 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 than threshold value, node is suspected to be attacker node and it adds node to black list. The source node shares this information with neighboring nodes by attacker node identification. So that neighboring nodes know that RREP packet from attacker node is to be discarded. Further, if any node receives RREP packet, it looks over list, if reply is from blacklisted node; no processing is done for same. It RREP packet, it looks over list, if reply is from blacklisted node; no processing is done for same. It simply ignores node and does not receive reply from that node again.

[6] CONCLUSTION AND SCOPE OF RESEARCH

The threat posed by a Black Hole attack on a network is substantial and widespread. When there is a rise in the number of malicious nodes in a network, the performance of the network suffers. The packet delivery ratio has been shown to drop under certain circumstances. Using NS2 simulators, many researchers examined the routing protocol's behavior and calculated the impact of Black Hole attack on AODV routing and its detection method.

It has been projected that Fuzzy logic-based networks would show the impact of Black Hole attacks on AODV protocols in the future. Nodes in such a network would transmit data using fuzzy logic. Fuzzy logic would use a range from 0 to 1 for input and use randomness rather than order to determine the next node.

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] Geng Peng, Zou Chaanyun "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 Yibeltal Fantahum Alem & Zhao Hheng Xaun 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 Georgios Skourletopoulos", 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, Mubashir Yaqoob Mantoo Mahnaz Chishti and Neha Chaudhary, 2014 5th International Conference-IEEE.

[12] A Simulation Study of Malicious Activities under Various Scenarios in Mobile Ad hoc Networks (MANETs) by Akshai Aggarwal, Nirbhay Chaubey 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.