ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

REVIEW OF REMOVAL OF BLACK-HOLE ATTACK IN AODV ROUTING PROTOCOL OF MANET USING BHR

Sumit Purba*, Kantveer Singh
* M.Tech, Department of Computer Science & Engineering, G.I.M.E.T, Amritsar, India
Asst. prof., Department of Computer Science & Engineering, G.I.M.E.T, Amritsar, India

ABSTRACT

A Mobile Ad-Hoc Network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on continual basis. Due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack. In this paper, we give an algorithmic approach to focus on analysing and improving the security of AODV, which is one of the popular routing protocols for MANET. Our aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting & removing Black hole node(s) in the MANET at the beginning. Also the objective of this paper is to provide a simulation study that illustrates the effects of Black hole attack on network performance.

KEYWORDS: Mobile Ad-Hoc Network, routing protocol, Black Hole Attack, AODV, MANET

INTRODUCTION

Nowadays, wireless networks are used increasingly, because they may be utilized by everyone, everywhere, every time, they could be organized dynamically, everywhere, and every time without any network infrastructure. Majority of them are both router and node simultaneously. The feature has enabled the networks to be organized within a predefined constant structure for military and flooding utilization. The nodes are linked through radio frequencies, available node to the radio frequency is supposed to be neighbour or else, other nodes are utilized, hence, the nodes are linked to the network based on dependability and common participation. Mobility of the nodes, wireless communication, dynamic change of network structure, lack of behaviour and functions centralized management lack of definite defending lines, as well as limited usage power of the nodes have created an adequate domain for different attacks to the networks. Ad hoc networks route based on dependable links, so they facilitate well the attacking opportunity by the attackers, and participation in routing process disturbs routing process finally. AODV protocol is the most famous router of the specific networks [4,5] and many studies analyse different attacks to it. AODV develops routes through a query cycle of route order and the reply. When the source node enquires a destination route, the node that lacking a path to destination distributes public route request pack. Receiving nodes, update their information based on source node, and they create an entrance for the reverse path on route tables. Also, the directed node to destination route informs the source node to send concerning data to the destination through this node; Or else, it distributes request order in network. Ray hole is the most important ad hoc attack. It is includes two phases, the first phase process is so malicious that cooperative of AODV protocol informs that it has a path towards destination node by transmitting RREP package. But the malicious cooperative may have two types of attack in the second phase, firstly it transmits the received packs through a specific node or throws them away, also, the malicious cooperative may sometimes throw away all packs all along its lifetime and it may sometimes behave flawlessly. The two moods make hard attack recognition if they are combined [6]. The decision method is based on the behaviours of the nodes so as know whether the node is malicious or not.

TYPES OF ROUTING

In Ad-hoc networks require multi-hop routing and all nodes can potentially contribute in the routing protocols. Routing is the moving information from a source to a destination in an in network. At least one intermediate node within the internetwork is encountered during the transfer of information. Mainly two activities are involved in this concept: determining optimal routing paths and transferring the packets through an internetwork. The transferring of packets

throughout an internetwork is called as packet switching which is straight forward, and the path determination might be very complex. Routing is mainly classified into static routing and dynamic routing. Static routing is the routing strategy being stated manually or statically, in the router. Static routing continues a routing table usually written by a networks administrator. And dynamic routing is that routing strategy that is being learnt by an interior or exterior routing protocol. This routing depends on the state of the network i.e., the routing table is affected with the activeness of the destination. Routing protocols are organized as:

- Reactive Routing Protocol (AODV)
- Proactive Routing protocol (OLSR)

Hybrid routing protocol (ZRP)

AODV

AODV perform both unicast and multicast routing and it preserve a path since needed for communication [4].It used route finding procedure and routing tables for maintaining route information [8]. AODV used HELLO, REEQ AND RREP for communication.

Source_ Address	Source_ Sequence	Broadcast_ Id	Destination_ Address	Destination_ sequence	Hop_ Count

AODV RREQ field

Source_ Address	Destination_ Address	Destination_ Sequence	Hop_ Count	Lifetime	

AODV RREP field

OLSR

Being a proactive protocol, routes to all destinations within the network are known and maintain before using it. Having the routes available within the standard routing table can be useful for some systems and network applications as there is no route discovery delay associated with finding a new route. The routing operating cost generates, although commonly greater than that of a reactive protocol and does not increase with the number of routes being created. Being a link-state protocol, OLSR requires a reasonably large amount of bandwidth and CPU power to compute optimal paths inside the network. OLSR is a hop by hop table driven or proactive routing protocol. The routes are always all the time at once presented when required suitable to its proactive nature [10]. OLSR used multipoint relay (MPR). MPR are responsible for generating and forwarding topology information. OLSR always need to maintain routing tables. OLSR have three types of control messages, Hello, Topology Control (TC), and Multiple Interface Declaration (MID) [11].

ZRP

ZRP based on the Zone. ZRP was planned to decrease the control overhead of proactive routing protocols and discovery in reactive routing protocols and also decrease the latency caused by route. ZRP is adaptive in nature and it depends on the present organization of network. As the name infer ZRP is based on idea of the zone. A routing zone is different for all nodes, and the zones of closest nodes partially cover one by one [12]. ZRP can be considered like a flat protocol. Zone Routing Protocol consists of various components, which simply jointly offer the full routing advantage of ZRP is that each component work by itself. Components of ZRP are IARP Intra zone Routing Protocol; IERP Inter zone Routing Protocol and BRP Border casts Resolution Protocols.

BLACKHOLE ATTACK

Black hole attack is denial of service (DOS) attack in which malicious node send fake information by claiming that it has a fresh or shortest route to destination node and hence source nodes select this shortest path and go through this malicious node and result data misuse or discarded [8]. Once the route is set up, at the moment it's up to the node whether to drop all the packet or familiar it to the nameless address. This special node, which disappears the data

packet, is named as malicious nodes. Black hole attack be an active insider attack. Black hole has two main properties. First the node announces itself when having a suitable route to a destination node and second one the node consumes the intercepted packets.

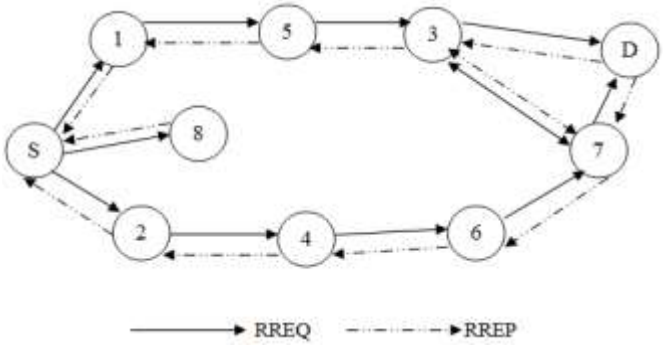

Fig 1. Flow of control message

PROPOSED WORK

Proposed method is implemented in NS2 in which firstly nodes are deployed, and then form the clusters of the various nodes and communication between cluster heads and its members. Normal communication between source and destination is done. After this, some nodes are changed to black hole nodes randomly and then communication between source and destination is done under black hole. After detection of black hole nodes, communication is done between source and destination. AWK files are used along with TCL scripts are used to implement proposed work.

METHODOLOGY

Performance Metrics

To evaluate the performance of proposed technique, it is need to calculate various performance metrics. Various Performance metrics are:

- **Packet Delivery Ratio (PDR) -** It is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. It represents the maximum throughput that the network can achieve. A high packet delivery ratio is desired in a network.
- **Average End-to-End Delay**: The packet end-to-end delay is the average time that packets take to traverse the network. This is the time from the generation of the packet by the sender up to their reception at the destination's application layer and is expressed in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities. Various applications require different levels of packet delay. The end-to-end delay is therefore a measure of the how well a routing protocol adapts to the various constraints in the network and represents the reliability the routing protocol.

- **Throughput:** Ratio of the total amount of data received by nodes in the network to the time of communication is referred to as throughput. It is expressed in bits per second or packets per second. Factors that affect throughput in MANETs include frequent topology changes, unreliable communication, limited bandwidth and limited energy. A high throughput network is desirable.

- **Packet lost:** It gives number of packet lost in the network while communication. Packets lost will be calculated under normal communication, under black hole attack and after detection of black hole attack and proposed technique will be compared on this basis.

- **Detection Rate:** It is number of black hole nodes detected to total number of black hole nodes. It is desirable to get good detection rate to show efficiency to detect attack by proposed method.

REFRENCES

[1] Pradish Dadhania, Sachin Patel "Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks" in International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 1, pp.1487-1491, January February 2013.
[2] Arunima Patel, Sharda Patel, Ashok Verma "A Review of performance Evaluation of AODV Protocol in Manet With and Without Black Hole Attack" International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 11, November 2012.
[3] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols" Chapter 19, pp. 219229.
[4] Prem Chand and MK Soni "Performance Comparison of AODV and DSR on-Demand Routing Protocols for Mobile Ad-Hoc Networks" International Journal of Computer Applications ISSN 0975 – 8887 Volume 49– No.18, July 2012.
[5] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala "DoS Attacks in Mobile Ad-hoc Networks: A Survey" 2012 Second International Conference on Advanced Computing & Communication Technologies.
[6] Harmandeep Singh, Gurpreet Singh and Manpreet Singh "Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack" International Journal of Computer Applications ISSN 0975 – 8887 Volume 42– No.18, March 2012.
[7] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad "Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc Networks" Emerging technology Trends in Electronics, communication and networking, © IEEE 2012 First international Conference ISBN 978-1-4673-1628-6.
[8] VinayP.Virada "Securing And Preventing Aodv Routing Protocol From Black Hole Attack Using Counter Algorithm" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October - 2012 ISSN: 2278-0181.
[9] Ashish Bagwari, Raman Jee, Pankaj Joshi and Sourabh Bisht " Performance of AODV Routing Protocol with increasing the MANET Nodes and its effects on QoS of Mobile Ad hoc Networks " 2012 International Conference on Communication Systems and Network Technologies 978-0-7695-4692-6/12 © 2012 IEEE.
[10] Naveen Bilandi, Harsh K Verma "Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET" International Journal of Electronics and Computer Science Engineering 1660 ISSN-2277-1956.
[11] Irshad Ullah and Shoaib Ur Rehman "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols" Master Thesis Electrical Engineering June, 2010 Thesis no: MEE 10:62.
[12] Himani Yadav and Rakesh Kumar "Identification and Removal of Black Hole Attack for Secure Communication in MANETs" International Journal of Computer Science and Telecommunications [Volume 3, Issue 9, September 2012] ISSN 2047-3338".
[13] Scalable Network Technologies (SNT). Qual Net. http://www.qualnet.com