Engineering Universe for Scientific Research and Management
(International Journal)
Impact Factor: 3.7

A Universe of Research
ISSN(ONLINE) : 2319-3069

Vol. 6 Issue 6
June 2014

A Review - Techniques to Mitigate Black/Gray Hole Attacks in MANET

Mr. Kumar Pradyot Dubey[1], Er. Kuntal Barua[2]
Dept. of Computer Science& Engg.LNCT, Indore,India[1]
Dept. of Computer Science & Engg. LNCT, Indore,India[2]
pradyotdubey@gmail.com[1] , kuntal.barua@gmail.com[2]

Abstract

The Mobile Ad hoc networks are formed dynamically by mobile nodes that are connected via wireless links without using the network infrastructure or centralized administration. In MANETs every node can act as host or router at the same time such that every node can send the packets or receive the packets or re-route the packets if the received packets belongs to some other node Routing protocols, which act as the binding force in these networks, are a common target of these nodes. Ad hoc On-demand Distance Vector routing (AODV) is a widely adopted network routing protocol for Mobile Ad hoc Network (MANET). The security of the AODV protocol is threatened by a particular type of attack called 'Black Hole' attack. In this attack a malicious node advertises itself as having the shortest path to the destination node. In this way network data packets diverted into the wrong path, which causes great data loss in MANET. This paper reviews the latest research activities in Ad-Hoc network field, including a summary of MANET characteristics, capabilities and its applications . Hence, A range of literature relating to the field of MANET routing was identified and reviewed.

Keywords: *AODV, OLSR, DSR, MANET.*

1. Introduction

Mobile Ad-Hoc network is an autonomous system, where nodes/stations are connected with each other through wireless links. There is no restriction on the nodes to join or leave the network, therefore the nodes join or leave freely. Mobile Ad-Hoc network topology is dynamic that can change rapidly because the nodes move freely and can organize themselves randomly. This property of the nodes makes the mobile Ad-Hoc networks unpredictable from the point of view of scalability and topology.

Mobile Ad-hoc Networks (MANETs) are dynamic in nature. Any nodes can join and leave the network at any time. Hence any type of intruders can attack the communication at any time, especially the routing mechanism between the nodes. In this study, we study and understand two types of attacks which cause more damage to the routing performance of MANET; the attacks are Black Hole attacks and Gray Hole attacks.

Mobile Ad Hoc Networks are autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Many routing protocols have been developed for MANETS, i.e. AODV, OLSR, DSR .

Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.

The MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

MANETs must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, the engineers must understand different types of attacks and their effects on the MANETs. Wormhole attack, Black hole attack, Sybil attack, flooding attack, routing table overflow attack, Denial of Service (DoS), selfish node misbehaving, impersonation attack are kind of attacks that a MANET can suffer from. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources.

1.1 AODV Routing Protocol

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. AODV is a reactive protocol i.e the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is upto-date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicast back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors.

2. Related Work

In this section we are going to discuss about the different types of the MANET protocols and their works. Here we will study about the research work of different authors, how they use the protocol to solve the problems and what are their future works.

Fidel Thachil & K.C. Shet[1], Proposed a trust based method for detecting malicious node in the network. Each node monitors its neighbours. For this each node has a cache which keeps the record of forwarded packets to its neighbouring nodes. Now this node starts checking whether the packet which has been forwarded to its neighbours is being further forwarded or not. According to this principle every node calculates trust value of its neighbour. If trust value comes below a predefined threshold value, then the node will be declared as malicious.

Mehdi Medadian et. al, proposed a novel approach based on using negotiations with neighbors for countering the black hole nodes. In this approach, any node uses a set of rules to decide the honesty of the reply's sender. During packet transferring, the activities of a node are logged by its neighbors. These neighbors send their opinion about a node. When a node receives replies from all neighbors, it is able to decide whether the replier is a malicious node or a legitimate node. The opinion send by neighbors is based on the number of packets sent to a particular node and number of packets forwarded by it[2].

Nidhi Sharma & Alok Sharma[3], presented a couple of solutions that can be used as a strategy against the black hole attack in MANET (Mobile Ad hoc Network). First solution is to have multiple routes to destination and unicast ping packet to destination using multiple routes (assigning different packet ID's and sequence number). Upon checking the replies received from different routes, decision is made regarding the selection of a route for communication. In the second approach, sequence number is used for the verification of legitimate node. Two extra tables are maintained to record sequence number of the forwarded packets and sequence number of the received packets. If there is a mismatch between sequence number of received RREP (Route Reply) and the sequence number of the table, the route discovery process is started while alarming the whole network about the node. The scheme does not add overhead as sequence number itself is included in every packet in base protocol.

Kamarularifin Abd Jalil et.al[4],proposed an enhanced protocol ERDA. Which is used to prevent black hole attack problem. Some extra tables are added to AODV for keeping the track of all malicious node and its corresponding sequence numbers. In RREP by destination and malicious node, source has records for this. Now source node analyses the sequence numbers by heuristic method and gets malicious node with extremely high sequence number.

Songbai Lu et.al, proposed a secure AODV (SAODV) protocol. According to this; AODV starts sending SRREQ packet along the reverse of the received RREP paths to the destination, intermediate and malicious nodes. This SRREQ packet has a random number (say 'x') generated by source. After receiving SRREQ packet by destination node and accepting 'x'; it generates another random number (say 'y') and sends back with SRREP packet through different routes to source. Source node matches y from different path; if it matches successfully then network is secure. Malicious node cannot detect 'y' or even if it detects then reaches to the source at late in sequence.[5]Source node finds fault in sequence of receiving RREP & SRREP from malicious node and discards it.

Yibeltal Fantahun Alem et.al[6], Presented and idea of Intrusion detection using anomaly detection (IDAD). This technique is used to overcome the malicious node problem. Intrusion detection is a process of detecting faults and preventing it to occur in subsequent actions. In this system each of the anomaly activities (i.e. possible intrusion) identified and collected as a set of data called "Audit Data". This audit data is given to the source node for matching the RREP packet data. If this data doesn't match, then the existing network is secure otherwise there are malicious nodes in the netwok.

Muhammad Raza & Syed Irfan Hyder,Proposed a special network type in which there are three basic devices are used namely Server, Access Point, Nodes. Here server and access points are connected with each other using "Wi-Max"(IEEE 802.16, 10 to 66 GHz). Here Server connects several Access Points in stable (Infrastructure) mode, while nodes are connected with Access Points in Ad-hoc manner. Whenever any new node comes to participate in communication, it gets two responses, one from AP and other from malicious which fakes itself by highlighting as a genuine server. The mobile node connects itself directly to the malicious node. When, after sometime AP scans the network , it finds the new node victim of Black hole. Now access point hears the communication between these two and gets MAC of malicious node, and warns the whole network with the help of this MAC Address.[7]

Harmandeep sing & Manpreet Singh, discussed various attacks in MANET and also all types of protocols of MANET. The Black hole attack on AODV,OLSR and ZPR have been analyzed with respect to different performance parameters such as average end to end delay, throughput and packet delivery ratio.[8]

Dr. S.S.Dhenakaran & A.Parvathavarthini discussed classifications of MANET routing protocols. Furthermore different protocols of different classification categories are compared under the various parameters and the result of this is summarized into a table. Different advantages & disadvantages of different protocols have also been discussed.[9]

Meenakshi Sharma et.al,[10] published a mechanism to detect the malicious node in MANET. Whenever one or more black hole nodes are present in the network ,we can remove these nodes easily by sending fake RREQ message and receiving a modified RREP packet. Whenever black hole node gets fake RREQ packet, it replies to the source by claiming that 'I'm the actual destination'. In this way source can identify any malicious node easily and broadcasts an alarm message to all the nodes in the network.

Bhaliner Kaur & Sonia have discussed the various MANET routing protocols and their comparison on the basis of the some important parameters like 'Throughput', 'Delay', 'Network Load' over the varying conditions of number of nodes. The Simulator for this purpose used is 'Opnet Modeler 14.5'. [11]

3. Literature extraction

Whenever MANET is attacked by any malicious node; 'Throughput' of the Ad-hoc network reduces while the 'Delay' of packet delivery increases at steady rate. The black hole attack is even worse if multiple black holes exist in the network. Out of all the research works some authors like 'Yibeltal Fantahun Alem et.al', 'Songbai Lu et.al' have proposed methods in which source node is dependent on the adjacent nodes or need feedback information in order to decide acceptability of any node in the network. While some authors like 'Muhammad Raza et.al' have put the concept of partial infrastructure into Ad- hoc network. As a consequence we can say that there are various corrections possible in developing an efficient MANET routing protocol in order to achieve security and performance parameters better .

4. Problem definition

Besides Security ,'Throughput' and 'Time Delay' are two most important features of any routing protocol of MANET. Many authors simulated these features in their work to study comparative performances of various routing protocols. According to Bhalinder Kaur and Sonia's proposal ,the selection of efficient and reliable protocol is a critical issue. The performance of routing protocols vary with network and selection of accurate routing protocols according to the network, ultimately influence the efficiency of that network in magnificent way[11]. But there are many pitfalls and weaknesses (like Black Hole /Gray Hole Attack) present in each of all discussed algorithms in some amount. These can be thought of as imbalance between 'Performance' and 'Security' features of MANET. As a consequence there should be an efficient MANET routing protocol which enhances the performance and security of any Ad hoc network.

5. Problem solution

Though there are many solutions proposed by various authors to deal with black hole attack in MANET, some of them are reviewed in this literature and found to exhibit the effect on performance in terms of increase in delay and overhead. Amongst all of the routing algorithms, AODV is best known algorithm. Therefore many researchers have given their solutions by enhancing features of MANET over AODV protocol.

6. Conclusions

In this paper we have identified and reviewed a range of literature on the topic of MANET routing protocols, Our review focuses upon protocols developed by Perkins, namely the Destination Sequenced Distance Vector (DSDV) and Ad-hoc On-demand Distance Vector (AODV) which researchers claim is the most popular MANET routing protocol. Due to the popularity of the AODV protocol a number of variations and improvements on the core protocol have been proposed by researchers to address specific issues with the protocol. A common theme across many of the papers we have reviewed is the exclusive usage of random waypoint mobility model for simulations despite several researchers identifying limitations with this approach to testing.

References

[1]. Fidel Thachil, K.C. Shet, "A Trust Based Approach for AODV protocol to Mitigate Black hole attack in MANET ," 2012 International conference in Computing Science.,IEEE 2012

[2]. Mehdi Medadian, M.H. Yektaie, A.M Rahmani," Combat with Black Hole Attack in AODV routing protocol in MANET", IEEE 2009.

[3]. Nidhi Sharma & Alok Sharma," The Black-hole node attack in MANET",2012 Second International Conference on Advanced Computing & Communication Technologies.

[4]. Kamarularifin Abd Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan ," Securing Routing Table Update in AODV Routing Protocol", 2011 IEEE Conference on Open Systems (ICOS2011), September 25 - 28, 2011, Langkawi, Malaysia.

[5]. Songbai Lu, Longxuan Li, Kwok-Yan Lam, Lingyan Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack", 2009 International Conference on Computational Intelligence and Security.

[6]. Yibeltal Fantahun, Alem Zhao, Cheng Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2010 IEEE.

[7]. Muhammad Raza & Syed Irfan Hyder," A Forced Routing Information Modification Model for Preventing Black Hole Attacks in Wireless Ad Hoc Network"; Proceedings of 2012 9th International Bhurban Conference on Applied Sciences & Technology (IBCAST) Islamabad, Pakistan, 9th - 12th January, 2012

[8]. Harmandeep singh & Manpreet Singh," Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs"; International Journal of Advanced Trends in Computer Science and Engineering, Volume 2, No.3, May - June 2013.

[9]. Dr. S.S.Dhenakaran & A.Parvathavarthini , "An Overview of Routing Protocols in Mobile Ad-Hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 2, February 2013.

[10]. Meenakshi Sharma and Davinderjeet Singh, "Implementation of a Novel Technique for a Secure Route by Detection of Multiple Blackhole Nodes in Manet", International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 - 5161 ©2014 INPRESSCO

[11]. Bhaliner Kaur & Sonia ,"Performance Evaluation of MANET Routing Protocols with Scalability and Node Density issue for FTP Traffic,"International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013 2013, IJARCSSE

[12]. Chundong She, Ping Yi , Junfeng Wang, Hongshen Yang; "Intrusion Detection for Black Hole and Gray Hole in MANETs", KSII Transactions on Internet and Information Systems vol. 7, no. 7, jul. 2013

[13]. Lalit Himral, Vishal Vig & Nagesh Chand," Preventing AODV Routing Protocol from Black Hole Attack", Lalit Himral et al. / International Journal of Engineering Science and Technology (IJEST), Vol. 3 No. ,5 May 2011.

[14]. Subash Chandra Mandhata , Dr.Surya Narayan Patro," A counter measure to Black hole attack on AODV based Mobile Ad-Hoc Networks", International Journal of Computer & Communication Technology (IJCCT), Volume-2, Issue-VI, 2011.

[15]. Jaspal Kumar, M. Kulkarni, Daya Gupta, " Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, 2013, 5, 64-72.

[16]. Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi ,"A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[17]. Harjeet Kaur , Manju Bala , Varsha Sahni, "Performance Evaluation of AODV, OLSR and ZRP Routing Protocols under the Black Hole Attack in MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 6, June 2013.

[18]. Yash Pal Singh, Dr. P.K Singh, Jay Prakash, "A Survey on Detection and Prevention of Black Hole Attack in AODV- based MANETs", Journal of Information, Knowledge and Research in Computer Engineering.

[19]. Sukhvinder Singh , Renu Dhir ,"Simulation Based Performance Comparison of Proactive and Reactive Routing Protocols in MANET using FTP and HTTP Traffics", IJAIR Vol.