ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

Review on Black hole Attack Detection in Wireless MANET

[1] Kishor A. Dongarwar, [2] Mr. Nitesh Ghodichor,
[1][2] Assistant Professor, Department of Computer Technology
Priyadarshani College of Engineering and Research,
Nagpur University, Maharashtra, India

Abstract - **In wireless mobile ad-hoc network nodes are communicating with each other with the help of wireless link. In MANET (Mobile Ad-hoc Network) due the absence of centralize monitoring the network is vulnerable by various types of attacks. In this type of network a node establishes communication is on trust base. As due to their feature of open medium, dynamically changing topology of network, absence of central monitoring security is the significant challenge for these networks. In MANET an intermediate node involved for promoting a packet to the destination node, this intermediate node may act in malicious manner and drops all the packets instead of forwarding to an appropriate node. Such a malicious behavior of a node is called as black hole attack. In this paper we study one routing protocol i.e. Ad-hoc On-demand Distance Vector(AODV) protocol and analyze in detail one type of attack the "black hole" attack and discuss different solutions for the black hole problem in wireless mobile ad-hoc network.**

Keywords:--- **wireless mobile ad-hoc network, AODV routing protocol, black hole attack.**

I. INTRODUCTION

Since the beginning of wireless communication, man has always been motivated to make progress and better the existing technology. Wireless communication is one of the significant development in 21st century. The advantage of wireless network is that wireless nodes communicate with the nodes into the network while being mobile. A wireless ad-hoc network is a group of nodes communicate by wireless links. In wireless mobile ad-hoc network there is no use of any access point or centralized administration for the control on the network. So that every node acts as a router to establish a route. When source establish connection with destination, packet are forwarded through an intermediate nodes, thus searching a fastest route from source to the destination is an important issue in MANET. There are different routing protocols are available, which are categorized into proactive and reactive routing protocols. In proactive routing protocol, every mobile node maintains routing table with entries for each and every possible destination node, and periodically exchanges routing messages, in order to ensure that the information in the routing table is up to date and true, such as DSDV (Destination Sequence Distance Vector).Each node in MANET is limited to battery power and bandwidth, so continuous transmission of routing messages would lead to congestion of the network. In reactive routing protocol, the route is establish when source node wanted to communicate with destination, such as AODV and DSR (Dynamic Source Routing). The AODV [1] is the most popular routing protocol and has extensively discussed in many research papers. In this paper we discuss about AODV protocol and what are the vulnerabilities in AODV protocol.

The technology of MANET is also called infrastructureless networking. MANET technology can provide an extremely flexible method of establishing communications in situations where geographical or terrestrial constraints demand totally distributed network system without any fixed base station, such as battlefields, other emergency and disaster situations. As ad-hoc network can be used for military purposes or in some common security purposes like for online transaction, so main requirement is to make it secure or attack free so that malicious node cannot enter into this network and cannot be able access the secure information. People with intelligence and having bad intention are misusing the aspect of wireless communication. Various attacks against wireless mobile ad-hoc network can be conducted by an intruder. The main aim of an attacker is the violation and disturbance of the correct network operation. An intermediate node constitute a behavioural deviation, whose consequence is the violation of the objective for which the network is deployed. Such malicious behaviour is called the black hole attack.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

The rest of the paper is structured as follows: section II describes the AODV protocol, what are the vulnerabilities in AODV protocol in section III, in Section IV the black hole attack in AODV protocol, then section V summarizes the related work and detailed description of the suggested solution. finally conclusion can be achieved.

II. OVERVIEW OF AODV PROTOCOL

The AODV routing protocol is an adaptation of the DSDV protocol for dynamic link condition [1].The AODV Routing protocol uses on-demand mechanism for finding paths from source to the sink node, that is, a route is demanded only by a source node for sending data packets. It uses destination sequence numbers for identifying the most recent path. It is the highly distinctive feature of Ad-hoc on-demand distance vector protocol. Each and every node in an Ad-hoc network maintains routing table, which contains information about the path to particular destination. Whenever a node wants to send packet, it first checks its routing table to check whether a route to the destination is already exist. If so, it uses that path to send the packets to the destination. If a path is not available or the previously entered path is inactivated, then the node starts route discovery process.

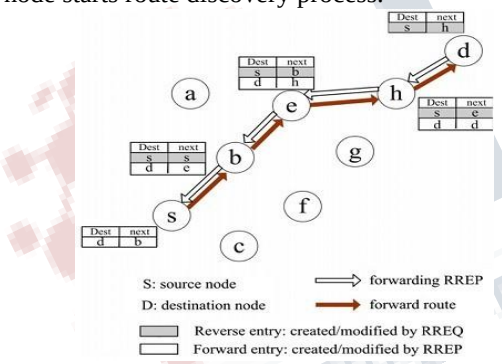

Fig. 1. RREQ message and reverse route [9]

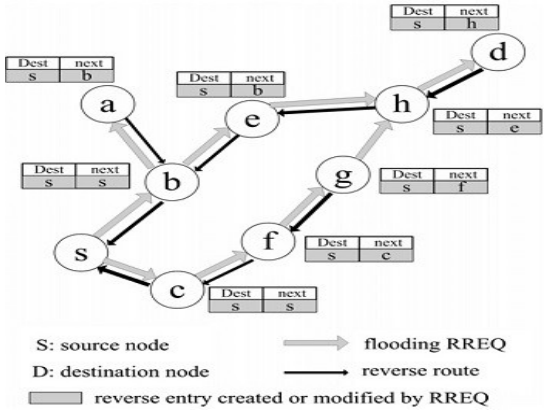

Fig. 2. RREP message and forward route [9]

There are three types of control messages are defined, A RREQ (Route REQuest) packet is broadcasted by the node. The node which receives the RREQ control message checks its routing table if it is destination node that receives the RREQ packet first checks if it is the destination or not if it is destination node, it sends back an RREP (Route REPly) packet. If it is not the destination, then it checks with its routing table to determine if it has fresh route to the destination. If not, it sends the RREQ packet by broadcasting it to its neighbours. If its routing table does contain an entry to the destination, then the comparison of the destination sequence number in its routing table with the destination sequence number present in the RREQ packet is done. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREP packet, then the node update its routing table. If the number in the routing table is higher than the number in the packet, it denotes that the route is a fresh route and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. Every intermediate node that received RREQ message will make entry in its routing table for the node that has forwarded the packet and also for the source node. The RREP packet send back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (RouteERRor) packet to all other nodes that uses this link for their communication to other nodes.

III. VULNERABILITIES IN AODV PROTOCOL

AODV protocol is very efficient as a network service but it has many vulnerabilities, attacker can easily attacked. AODV protocol is designed for an ideal network, for a network having no malicious node AODV protocol is most successful one. But we knows there are some unwanted nodes everywhere which attacks on the network. In AODV protocol what can do during the RREQ and RREP messages is possible can be shown below:

- Sequence number can be changed.
- Hop counts can be modified (main attack is looping in the network).
- Modification of source route to the destination (Black Hole Attack).
- Fabrication of error messages (Error message that Destination is not reachable).
- Fabrication of source routes (cache poisoning).

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

Black hole attack is the serious one. In this attack the malicious node gets whole of the data that source node sending and after that it drops the data. So in this paper we will discuss the black hole attack under AODV protocol.

IV. BLACK HOLE ATTACK

According to the AODV protocol, the network is infrastructureless so any intermediate node into the network may reply to the RREQ received during a route establishment by checking it routing table and send RREP if it is having a fresh enough route to the destination node. This destination is checked by using destination sequence number that is present in the RREQ control message. This techniques used for decreasing routing delay but it makes system vulnerable to a malicious. A Black Hole attack [2] is a kind of denial of service attack where a malicious node gives false information of having shortest route to the destination in order to get all the data packets and drop it. Imagine a malicious node N4. When node N1 broadcasts a RREQ packet, other neighbour node receives it. Node N4, is a malicious node, so that node N4 does not check its routing table for the requested route to node N6. Hence, it immediately sends back a RREP packet to node N1, claiming that it has afresh route to the destination node N6. Node N1 receives the RREP from N4 immediately and discard all the RREP comes later and assumes that the route through N4 is the shortest route and sends packet to the destination through it. When the node N1 sends data to N4, it absorbs all the data and drops all the packets and behaving like a Black hole.

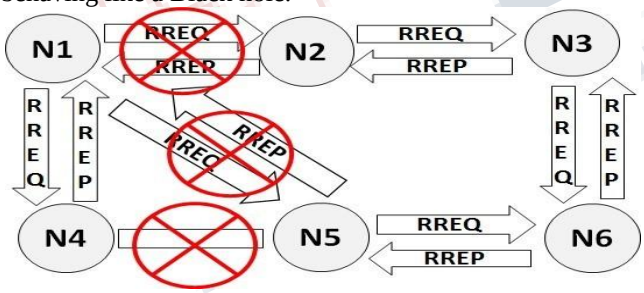

Fig. 3. Black Hole Attack

Deng [2] used On-Demand Distance Vector (AODV) and proposed a solution, in this each intermediate node to send back the nexthop information when it sends back an RREP message packet to source node. When source node receives the reply message from an intermediate node, it does not send the data packets right away, but extracts the nexthop information from the reply packet and then sends a FurtherRequest to the nexthop to verify that it has a route to the intermediate node who sends back the reply message, and that it has a route to the destination node. To avoid the problem of recursiveness, only the requested nexthop can send back a FurtherReply message, which includes the check result. The inquired intermediate node may also send back the FurtherReply message when it receives the FurtherRequest. In this method we ignore the FurtherReply message from the inquired intermediate node. Thus, we avoid the situation of the intermediate node taking further action such as fabricating the reply message on behalf of the nexthop node. When the source node receives the FurtherReply from the nexthop, it extracts the check result from the reply packets. If the nexthop has no route to the requested intermediate node, and it also has no route to the destination node, the source node initiates another routing discovery process, and also sends out an alarm message to isolate the malicious node.This approach could be used for individual attacks but cannot avoid cooperative attacks. For instance, if the next hop also cooperate with the replied node, which will be replied for both question and the source node will trust on next hop and send data within the replied node that may be a black hole node.

Sun Guan and Chen [3] used On-Demand Distance Vector (AODV) as their routing protocol. The detection scheme utilized neighbourhood-based method. In this, once the normal path discovery procedure in a routing protocol is finished, the source node sends a special control packet to request the destination to send its current neighbour set. By comparing the received neighbour sets, the source node can determine whether there is a black hole attack in the network. To mitigate the impact of the black hole attack, author design a routing recovery protocol to establish the path to the correct destination. This scheme will be failed to detect black hole attack when that attacker decides to force the fake reply packets selectively and detection of cooperative black hole attack was the next problem of their solution.

Latha Tamilselvan [4], proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies with next hop details from the other neighbouring nodes. After receiving the first request it sets timer in the 'TimerExpiredTable', for collecting the further requests from different nodes. It will store the 'sequence number', and the time at which the packet arrives, in a 'Collect Route Reply Table' (CRRT). The time for which every node will wait is proportional to its distance from the source. It calculates the 'timeout' value based on arriving time of the first route request. After the timeout value, it first checks in CRRT whether there is any repeated next

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

hop node. If any repeated next hop node is present in the reply paths it assumes the paths are correct. Then it chooses any one of the paths with the repeated node to transmit the DATA packets. If there is no repetition select random route from CRRT. Here again the chance of malicious route selected is reduced. The author simulated this solution by (GloMoSim) and results indicate that packet delivery ratio was improved with low delay and overhead.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto [5] propose a new anomaly detection scheme based on a dynamic learning method. The MANET hosts are mobile on their own so that the MANET environment is dynamically changing. In this author use dynamic learning method which is based on a statistical decision theory that calculates the multidimensional projection distance between the current and normal states of the targeted host. Author proposes to use weighted coefficients with a forgetting curve as its mathematical property has been proved to suit a requirements. They concerns one of the most popular MANET routing protocols, i.e., the ad hoc on-demand distance vector (AODV).This approach is not able to isolate the black hole nodes due to absence of detection mode such as revising the AODV protocol. Moreover, this comes with bigger processing overhead and the determination of optimal threshold values remains unresolved.

Payal , Swadas [6] used AODV as their routing protocol by proposing a dynamic learning system to detect black hole attack by notifying the other nodes in the network. In network a node receives RREP packet and it checks first the value of sequence number in its routing table. If the sequence number is higher than the threshold value, it will be considered as malicious node. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The authors used of advantage of AODV protocol that the source node alarmed the black hole to its neighbour's in order to be refused and removed. Also, deploying the dynamic learning system improved the average end-to-end delay and normalized routing overhead. However, if a cooperative attack occurs in MANET, detecting process will be too complex so, this solution cannot be used for cooperative attacks.

Hesiri Weerasinghe [7] used a methodology to detect multiple black hole nodes that working collaboratively as a collection to begin cooperative black hole attacks. Author used Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP) to produce a slightly modified version of ADOV protocol. This solution has been compared with the currently available solution proposed by Deng [2] and also the performance of both solutions compared with original AODV by QualNet simulator in term of throughput, packet loss rate, and end-to-end delay and control packet overhead. The author confirmed that original AODV and solution proposed by Deng [2] deeply suffer from multiple black hole attacks and this new solution can present better performance in compare to the previous solutions in term of throughput rate and minimum packet loss.

Rutvij, Sankita and Devesh [8] investigated on some of the existing approaches for black hole and grayhole attack and presented solution against these attacks which is able to find effectively short and secure routes to destination. Their theoretical analysis approach can increase packet delivery ratio (PDR) with negligible difference in routing overhead. Nodes receiving RREP from an intermediate nodes confirm the truth of routing information; source node broadcasts a list of malicious nodes when sending RREQ. Nodes update route tables when they get any information of malicious nodes from received routing packets. No extra control packet can be mentioned as benefit of this algorithm and there is minute difference in routing overhead which is the ratio of the number of routing related transmissions to the number of data related transmissions. And in this malicious nodes would be isolated and packet delivery ratio (PDR) will greatly be improved.

V. CONCLUSIONS

The MANET is an emerging research area with practical applications. However, a wireless MANET presents a greater security problem than conventional wired and wireless net-works due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability. In this we study the routing security issues of MANET, analyse one type of attack, the black hole, Also we discuss some solutions provided for avoiding black hole attack. Extensive research solutions ought to be carried out for efficient detection and prevention of these DoS attacks, especially, blackhole attacks and grayhole attacks.

Acknowledgment
I would like to thanks my guide Dr. G. V. Chowdhary for his support, encouragement and valuable advices on this paper.

REFERENCES

[1] C. Perkins, E. Belding-Royer, and S. Das, "Ad-hoc on-demand distance vector (AODV)
routing", Internet Draft, RFC 3561, July 2003.

[2] Deng H, Li W, Agrawal DP, "Routing Security in Wireless Ad-hoc Networks", IEEE Communications Magazine
40(10):70.75.doi:10.1109/MCOM.2002.1039859, (2002).

[3] Bo Sun,Yong Guan,Jian Chen,Udo W.Pooch, "Detecting Black-hole Attack in Mobile Ad Hoc Network",5th European Personal Mobile Communications Conference, Glasgow, Volume 492, Issue, 22-25 pp.490 . 495, April 2003.

[4] Latha Tamilselvan and Sankaranarayanan, V., "Prevention of Black hole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)Pages 21-27,2007.

[5] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour,and Yoshiaki Nemoto, "Detecting Black hole 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.

[6] Payal N. Raj, Prashant B. Swadas ,"DPRAODV: A Dynamic Learning System against Black hole Attack in Aodv Based Manet",IJCSIInternational Journal of Computer Science Issues, Vol. 2, pp 54-59,2009.

[7] Hesiri Weerasinghe , "On Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc
Networks", Proceedings of the IEEE International Conference on Communications, Jun. 24-
28,2011.

[8] Rutvij H. Jhaveri , Sankita J. Patel,"DoS Attacks in Mobile Ad-hoc Networks: A Survey", Second International Conference on Advanced Computing and Communication Technologies.
2 (2), p535-540, 2012.

[9] Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications 34 (2011) 107–117.

[10] "An Unobservable Secure Routing Protocol with Wormhole Attack Prevention for
Mobile Ad-Hoc Network", V Patil, P Fulare, N Ghodichor – (2014) 1930-1932