International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Study of Detection and Prevention Techniques for Flooding attack on AODV in MANET

Shruti Bhalodiya[1], Krunal Vaghela[2]

[1]PG Scholar, Computer Engineering, RK University, Rajkot, Gujarat, India

[2]Dy. Director, School of Computer Science, RK University, Rajkot, Gujarat, India

Abstract: ***Mobile means moving and ad hoc means temporary without any fixed infrastructure. Hence, mobile ad hoc network is a temporary network in which nodes are moving without any fixed infrastructure or centralized administration. MANETs are vulnerable to security attacks because of the decentralized authentication. Black hole, gray hole, worm hole, flooding are such type of security threats that affects the network. This paper presents a review on MANET, AODV routing protocol, flooding attack and comparison of various detection and prevention techniques of flooding attack. Among all this techniques, RFAP technique can easily find the attacker node and protect the network from RREQ flooding attack.***

Keywords: MANET, AODV routing protocol, Security attacks

1. Introduction

Mobile ad hoc networks are self-organizing network of mobile nodes that use wireless links to form a network [1]. This network is a momentarily network that can be destroyed anytime. This network formed dynamically and share common wireless link. As in tradition networks there is not basic fixed structure. Nodes are free to move randomly and can leave or join the network on the fly. In MANET each node works as both host and route. A mobile ad hoc network (MANET) is a group of mobile devise connected by wireless link without the requirement of fixed common infrastructure in place like wireless access point or base station point.

Wireless link in MANET make them more likely to attack. It is easier for hacker to attack this network easily and gain access to private information. They can directly attack the network to delete message, add malicious messages, or masquerade as a node. These violate the network goals of availability, authenticity, authorization, integrity and confidentiality [2].

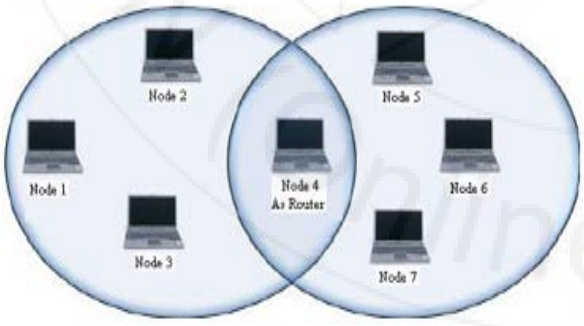

Figure 1: MANET Network

A. Characteristics of MANET[3]:

1. *Dynamic Topology*: Nodes are free to move randomly with different speeds. The nodes in the MANET dynamically establish routing among themselves as they wander, forming their own network.
2. *Infrastructure-Less*: Each node operates in disturbed peer-to-peer scheme, goes as an independent router and produces independent data.
3. *Multi-hop Routing*: No default router existing, each node acts as a router and host.
4. *Limited Bandwidth*: Limited bandwidth available between two intermediate nodes. Node may have limited power and thus computations need to be energy-efficient.
5. *Distributed Nature of Operation*: The operation of the network is distributed amongst the nodes. The nodes should cooperate to implement many functions mainly security and routing.

2. Literature Review

Based on routing information, MANET includes three protocol types:

A. Routing Protocol in MANET:

1) Proactive Routing Protocol [4]

Proactive routing protocol also called table driven protocol. In proactive routing protocols, every node maintains the network topology information in the form of routing tables by intermittently exchanging routing information. Routing information is generally spread in the whole network. Whenever a node wants to a path for destination, it goes an appropriate path-finding algorithm on the routing information. DSDV (Distance Sequence distance Vector), CGSR (Cluster-head Gateway Switch Routing), WRP (Wireless Routing Protocol) protocols are proactive routing protocols.

2) Reactive Routing Protocol [4]

Reactive routing protocols are also recognized as on demand routing protocol. Protocols that fall

under this category do not maintain the routing information. They find the necessary path when it is required and this process complete by using a connection formation process. These protocols do not exchange routing table information periodically like proactive routing protocol. AODV (Ad hoc on-demand distance vector) ,DSR (Dynamic Source Routing) protocols are reactive routing protocols.

3) Hybrid Routing Protocol [4]

Protocols belonging this category combine the best features of the reactive and proactive routing protocols. Nodes within a certain distance from the node disturbed are said to be within the routing area of the given node. For routing within this area, a proactive approach is used. For nodes that are located beyond this area, a reactive approach is used. ZHLS (Zone-based Hierarchical Link State Routing), ZRP (Zone Routing Protocol) protocols are hybrid routing protocols.

B. AODV Routing Protocol

Ad hoc On-Demand Distance Vector (AODV) Routing is a one of the on-demand or reactive routing protocol [5]. It is a reactive routing protocol means it establishes a path when it required. It works destination sequence numbers to identify the most current path. Main variance between AODV and DSR is DSR uses source routing in which a data packet conveys the complete path to be traversed and in AODV the source node and the intermediate node store the the next hop information consistent to each flow for data packet transmission.

In an on-demand routing protocol, the source node overflows the RouteRequest packet in the network when a route is not available for the selected destination [4]. It may increase multiple routes to different destinations from a single RouteRequest. The main difference between AODV and other on demand routing protocols is that it customs a destination sequence Number (DestSeqNum) to define and up-to-date path to the destination. A node updates its routing table information when the DestSeqNum of the present packet received is greater than the last DestSeqNum stored at the node.

A RouteRequest carries the Source ID, Destination ID, Source Sequence No, Destination Sequence No, Broadcast ID, time to live[4]. DestSeqNam indicates the freshness of the route that is accepted by the source. When the intermediate node accepts a RouteRequest, it either one forwards it or conveys a RouteReply if it has a legal route to the destination. If a RouteRequest is acknowledged multiple times, which is specified by the Source ID-Broadcast ID pair, the duplication copies are discarded.

All intermediate nodes having effective route path to the destination, are allowed to send RouteReply packets to the source. The timer is used to delete this entry in case a RouteReply is not received before the timer finishes. When a source node acquires about the path break, it re-establishes route to the destination if required by higher layers. If path break is detected at an intermediate node, the node updates the end nodes by sending an unwanted Route Reply with the hop count set as ∞.

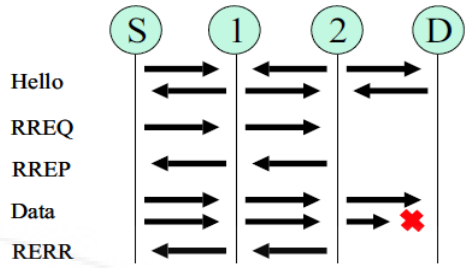

Figure 2: AODV control packets

C. Security Attacks against MANET

1) BlackHole Attack [7]

The black hole attack is an active attack. It has two properties First is attacker sends fake routing information, declaring that it has the valid route from source to the destination, due to which other nodes in the network route the data packets through the malicious node. Second, malicious node targets the routing packets, drops them instead of normally forwarding them.

2) GrayHole Attack [7]:

This attack is also known as routing misbehaviour attack which show the way to dropping of messages. Gray hole attack has two phases .In the first phase the node itself advertise having a valid route to destination while in second phase, nodes drops interrupt packets within a certain probability As soon as it receive the packet from neighbor the attacker drop the packet.

3) Wormhole Attack [7]:

In a wormhole attack, an invader receives packets from one location in the network, "tunnel" them to alternative location in the network, and then repeat them into the network from that location.. This tunnel between two colluding attacks is known as a wormhole In AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormhole are hard to detect because the path that is used is not part of the actual network.

4) Flooding Attack [7]:

Main aim of the flooding attack is to consume the network resources, such as battery power and bandwidth or to interrupt the routing operation to cause severe degradation in network performance.

RREQ Flooding: In RREQ flooding attack, the attacker broadcast several RREQ packets for the node which existing or not existing in the network. To perform RREQ flooding the attacker disable the RREQ rate so it will effect on to consumes network bandwidth.

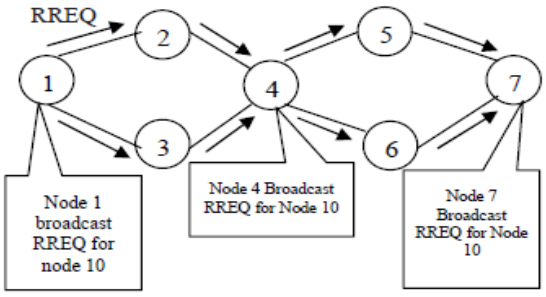

Figure 3: RREQ Flooding Attack [7]

Data Flooding: In Data flooding attack, data packets are used to floods the network. In this flooding malicious node construct a path to all the node then send the large amount of bogus data packet and this bogus data packet fail the network resources so it will hard to detect.

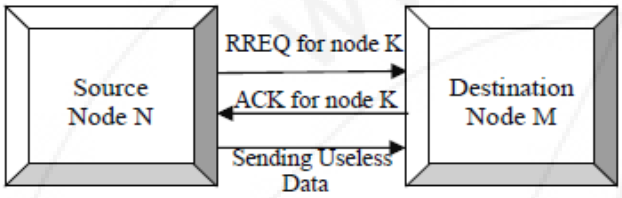

Figure 4: Data flooding attack [7]

SYN Flooding: In sync flooding attack a malicious node sends a enormous number of SYN(Synchronization) packets to a destination node. The destination node sends back SYN+ACK packets and keeps the entry for the unfinished connection request. The attacker never sends ACK(Acknowledgement).Hence a large amount of Memory of target node is consumed for loading Incomplete requests and node may come to a break even.

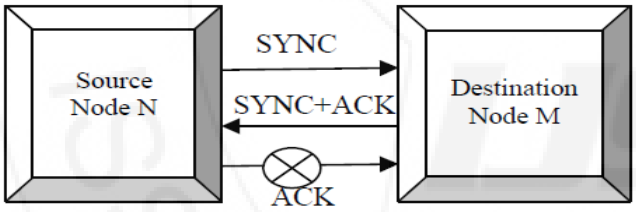

Figure 5: SYN flooding attack [7]

D. Detection and Prevention Techniques of Flooding Attack:

1) Effective Filtering Technique[8]

In this technique author proposed a new mechanism to prevent RREQ flooding attack; this technique can detect the malicious nodes and attacker nodes, which are disturbing the network communication. In this technique there are two thresholds RATE_LIMIT and BLACKLIST_LIMIT, which are used to limit the RREQ message. RATE_LIMIT parameter indicates no. of RREQ that can be known and managed. Here each node monitors the RREQ and maintain a count table for RREQ received. Whenever a RREQ request is received a condition check is performed, if the rate of received RREQ is less than the RATE_LIMIT then received RREQ processed normal otherwise a second condition check is performed, where received RREQ is compared with another threshold BLACKLIST_LIMIT, if the rate of RREQ is greater than the BLACKLIST_LIMIT then it is assume that particular node trying to flood the network with fake RREQ messages otherwise the received RREQ is add to delay queue. After identification of sender node as malicious node it will be blacklisted. The malicious node is blocked for a time period given by BLACKLIST_TIMOUT_LIMIT after if black list time out it will be unblocked. After adding malicious node to blacklist all the neighboring nodes of malicious node now free to divert RREQ from other genuine nodes, if the received RREQ has rate in between RATE_LIMIT and BLACKLIST_LIMIT then this will de add to delay queue by doing so the node which has high attack rate will be delayed.

2) Anonymous Secure Routing protocol Technique[9]:

In this technique presented anonymous communication. In this paper, three main components are used: white listing threshold, blacklist threshold and transmission threshold. This component displays the threshold limit of request packets sent by the neighboring performance analysis of flooding Attack. In RREQ flooding attack the invader selects numerous IP addresses which are not present in the network or choose arbitrary IP addresses dependent on information about range of the IP address in the network. Exhausting neighborhood suppression method, a single threshold is established for all neighboring node. In Data flooding attack the invader node first sets up the path to all the nodes and send useless packet. The given result is that the data packets are recognized in application layer and in future path cutoff is initiated. Effectively identify & eliminate the nodes that are flooding the network. It is not possible to track back the source &destination nodes in an anonymous network.

3) Trust Estimation Technique[10]

A trust estimator is used in every node to estimate the trust level of its neighboring nodes. The trust level is a function of various factors like, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor average time taken to respond to a route request etc. This technique proposed a distributive approach to identified and prevent the flooding attack. The efficiency of the proposed technique depends on the range of threshold value. In an ad hoc network, the relationship of a node i to its neighbor node j can be any of the following types

i. Node p is a stranger (S) to neighbor node q: 0< T <Tacq
ii. Node p is an acquaintance (A) to neighbor node q:
Tacq < =T < Tfri
iii. Node p is a friend (F) to neighbor node q: T > = Tfri

4) Node to Node Authentication using Challenge Response Protocol Technique[12]:

In this paper introduce a node-to-node verification technique using challenge-response protocol and MNT (Malicious Node Table). Challenge- response protocol checks genuine node flooding from malicious node and MNT (Malicious Node Table) used for storage information about malicious node noticed by CRP. AODV routing protocol is used, for packet forwarding and security will be maintained by MNT. The aim of this technique is to provide node accessibility and better security for packet transfer in MANET. It does not provide better packet delivery ratio, throughput and control overhead.

5) RREQ Flooding Attack Prevention (RFAP)Technique[13]:

Route Request Flooding Attack Prevention (RFAP) is a technique for mitigating the RREQ flooding attack in MANET. This technique first finds the flooder node, separates it from the network, gives some punishment and after reasonable punishment re-considers the node as fault nodes. In RFAP if the node breaks the predefine threshold value, it gets punishment. If anyone breaks the law first time the punishment may be less in particular place , in this technique it followed by Custody list. The strictness of punishment increases with the increment in numbers of violating the rule. During Custody List if the node breaks the law, separation time will be increased, in this technique it shown by Jailers List. If the node detained in Custody List starts showing gentle behavior, the node will be free and the RREQ will be interested but it will be under observation for sometime i.e. released on bail. If during observation time, node's RREQs again overtake the threshold value, node will be isolated for a long time, In this technique it shown by Life Imprisonment. After Life Imprisonment time out, all nodes will be free and sent back to a normal life. If in Jailer List node behaves itself before the predefined life imprisonment time, it will be released with observation. Disobedient of node during observation time will send it again in jailer list for life imprisonment. The technique refreshes all nodes after Life Imprisonment time-out because the technique believes that if in MANET a node shows malicious activities it is not necessary it will be doing the same after certain time. Major issue present in majority of solutions is not to recover malicious node after punishment. This technique, RFAP for mitigating the RREQ flooding attack in MANET by utilizing AODV protocol. The result shown that the RFAP technique can easily find the attacker node and protect the network from RREQ flooding attack.The RFAP technique cannot stop the illegal data packets.

3. Discussion

Technique	*Advantages*	*Disadvantages*
Effective Filtering Technique	It Switches the network with high mobility.	This technique does not able to differentiate Between genuine node and fake RREQs from the malicious node.
Anonymous Secure Routing protocol	Effectively identify & eliminate the nodes that are flooding the network.	It is not possible to track back the source &destination nodes in an anonymous network.
Trust Estimation Technique	Nodes are easily recognized based on their relationship i.e friend , acquaintance and stranger.	It get delay to distinguish the Disobedient node by allowing him to sends more packet 'til time out occurs.
Node to node Authentication using challenge response protocol	It provide node accessibility and better security for packet transfer in MANET	It doesn't provide better packet deliver ratio, throughput, control overhead .
RREQ Flooding Attack Prevention (RFAP)Technique	This technique recover malicious node after reasonable punishment.	It cannot stop the illegal data packets.

4. Conclusion

Security attacks like blackhole, grayhole, wormhole and flooding attacks are analyzed. Flooding attack in MANET results in exhaustion of battery power, degradation of throughput and wastage of bandwidth. In this paper, we have analyzed different techniques to detect and prevent flooding attack on AODV routing protocol in MANET. Main issue present in majority of proposed solutions is not to recover malicious node after punishment. RFAP is a technique for mitigating the RREQ flooding attack, which can recover the malicious node after the reasonable punishment and protect the network against attacker. It has ability to stop and isolate flooding attack with no extra burden on the network resources. Discussion of techniques presented in this paper is helpful to design secure techniques for flooding attack.

References

[1] Pradip M. Jawandhiya and Mangesh M. Ghonge, "A Survey of Mobile Adhoc Network Attacks", *International Journal of Engineering Science and Technology*, Vol. 2(9), pp.- 4063-4071, 2010.

[2] A. Mishra and K..M.Nadkarni, *Security in Wireless Ad -hoc Network, in Book*. "The Hand Book of Ad Hoc Wireless Networks" (chapter 30) , 2003.

[3] Robinpreet Kaur & Mritunjay Kumar Rai, " A Novel Review on Routing Protocols in MANETs", *Undergraduate Academic Research Journal (UARJ)*, Volume-1, Issue-1, pp. 103-108, 2012

[4] Siva Ram Murthy and B.S.Manoj, "Ad hoc Wireless Networks"(Chapter 7),2014.

[5] E.M.Royer and C.E.Perkins "Adhoc On-Demand Distance Vector Routing", *IEEE*, February 1999.

[6] Datuk Prof Ir Ishak Ismail and Mohd Hairil Fitri Ja'afar," Mobile Ad Hoc Network Overview", *IEEE*, December 2007.

[7] Ruchita Meher and Seema Ladhe," Review Paper on Flooding Attack in MANET", *International Journal of Engineering Research and Applications*, pp. 39-46,January 2014.

[8] Jian-Hua Song, Fan Hong and Yu Zhang, "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", *IEEE*, 2006.

[9] Venkat Balakrishnan, Vijay Varadharajan ,and Uday Tupakula" Mitigating Flooding attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications", *IEEE*, 2007.

[10] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs", *International Scholarly and Scientific Research and Innovation*, pp. 421-424, 2009.

[11] Ms. Neetu Singh Chouhan and Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET", in *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, pp. 68-72, November 2011.

[12] Komal Joshi Veena Lomte, " Preventing Flooding Attack in MANET Using Node-to-Node Authentication", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 11, pp. 136-140, November 2013.

[13] Kashif Laeeq ,"RFAP, A Preventive Measure against Route Request Flooding Attack in MANETS", *IEEE*,2012.

[14] Neha K. Holey , Sonal S. Honale, "Various Methods for Preventing Flooding Attack in MANET –A Comparative Analysis", *International Journal of Computing and Technology*, Volume 1, Issue 3, pp. 120-122,April 2014.