International Journal of Scientific & Engineering Research, Volume 7, Issue 12, December-2016
ISSN 2229-5518

BLACKHOLE ATTACK DETECTION IN AODV ROUTING PROTOCOL

Monika
M.tech Scholar
Department of Computer Science & Applications, Kurukshetra University, Kurukshetra
monikapunia56@gmail.com

Abstract:-Mobile Ad-hoc networks are collection of mobile hosts that communicate with each other without any infrastructure, hence are also termed as infrastructureless. One of the major area of concern in mobile ad-hoc networks is the security and because of the security attacks in its routing protocol, the networks are left unprotected against the attack of the malicious nodes. One of the major attack in mobile ad-hoc networks is the black hole attack. In this attack all the data packets processed by the source node are taken up by the malicious node and hence does not reach to the destination node. Therefore the data packets are dropped by the malicious nodes. This results in data loss. This paper is focused on detection of the black hole attacks in AODV. AODV is a reactive routing protocol for MANETS.

Keywords:-Ad hoc Network, black hole, AODV, MANET, RREQ, RREP

1. Introduction:-

An Ad-hoc network is a cooperative engagement of collection of mobile hosts without the need of centralized access point. Mobile Ad-hoc Networks (MANETS) are wireless networks, characterized by dynamic topologies and no fixed infrastructure. A MANET is an autonomous collection of mobile users that communicate over the network having bandwidth constrained wireless links. Since the nodes are mobile, the network topology might change rapidly and unpredictably over time. It is widely being used in many applications namely military battlefield, sensor networks, telemedicine and many more where each node act as a router. These nodes have the ability to configure themselves because of their self configuration ability, can be deployed urgently without the need of any infrastructure.

MANETS should have a secure way for transmission and communication and hence this is quite challenging issue as there is increasing threat of attack on mobile networks. In order to provide secure communication and transmission, we must understand different types of attacks and their effects on MANETS namely wormhole attack, Denial of service attack, routing table overflow attack etc. Out of all these attacks there is one major attack i.e. Black Hole Attack.

In this paper focus is on Black Hole Attack in AODV Routing Protocol. The Route discovery process is initiated when a source needs a route to a destination and it does not have a source in its routing table. To initiate route discovery, the source floods the network with a RREQ packet specifying the destination, the route is requested for, when a node receives an RREQ packet, it checks to see whether it has route to the destination. If either case is TRUE, the node generates an RREP packet, which is sent back to the source along the reverse path. Each node along the reverse path sets up a forward pointer to the node it received the RREP from. If the

node is not the destination and does not have route to the destination, it broadcast the RREQ packet. When the source node receives the first RREP, it begins sending data to the destination .To determine the relative degree of routes, each entry in the routing table and all RREQ and RREP packets are tagged with a destination sequence number. Large destination sequence number indicates more current route.

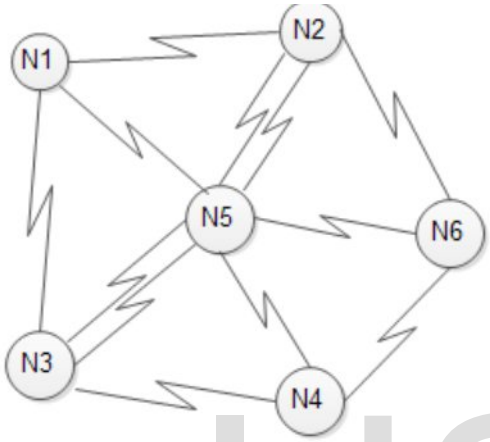

Fig.1. Mobile Ad-hoc Network Architecture

2. AODV Routing Protocol (AODV):

AODV is a reactive routing protocol for ad hoc and mobile networks that maintains routes only between nodes which needs to communicate. The AODV routing protocol is build on DSDV algorithm. AODV is an improvement on DSDV because it typically reduces the number of required broadcasts by creating routes on an on demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The routing messages in AODV do not contain information about the whole path, but only about the source and the destination. Therefore, routing messages does not have an increasing size. It uses destination sequence numbers to specify how fresh a route is in relation to another, which is used to grant loop freedom. [1]

2.1 Control Messages in AODV:-

There are four control messages in AODV which are described as follows:-
Routing Request (RREQ):-
When a route is not available for destination, a route request packet (RREQ) is flooded through the network which contains the following format shown below([2]).

RREQ:

Type	Flag	Reserved	Hop count
RREQ(Broadcast Id)			
Destination IP Address			
Destination Sequence Number			
Source IP Address			
Source Sequence Number			

Fig.2: RREQ

Routing Reply (RREP):-
If a node is the destination, or has a valid route to the destination, it unicasts route reply message (RREP) back to the source. This message has the following command [3]:-

RREP:

Type	A	Reserved	Hop Count
Destination IP Address			
Destination Sequence Number			
Source IP Address			
Source Sequence Number			

Fig.3: RREP

Route Error Message (RRER):-
All nodes monitor their own neighborhood and broadcast message when:-

- A node detects that the link with adjacent neighbor is broken (destination no longer reachable).
- If it gets a data packet destined to a node for which it does not had an active route and is not repairing.
- If it receives a RERR from a neighbor for one or more than one active routes, to notify the other nodes on both sides of the link about loss of this link.

HELLO Messages:-
Each node gets to know its neighborhood by using local broadcasts, so-called HELLO messages.. Although AODV is a reactive protocol and uses these periodic HELLO messages to inform the neighbors' that the link is still alive. The HELLO messages can never be forwarded because they are broadcasted with TTL = 1. When a node receives a HELLO message, it refreshes corresponding lifetime of the neighbor information in the routing table.

2.2 Working of AODV:-

(Ad hoc On-Demand Distance Vector) is basically a reactive routing protocol and it consists of two modules:-
When a node sends a packet to some destination, it checks its routing table to determine if it has a current route to destination.
If Yes, forward the packet to next hope.
If No, it initiates a route discovery process [4].

2.2.1 Route discovery module:- To send data to the given destination D, the source Node S consults in routing table. If it finds a valid entry (a route) towards destination D, it uses it immediately, else it launches a route discovery procedure which consists in broadcasting, by the source node S, a route request (RREQ) message towards neighbors. When RREQ is received by an intermediate node, this consults routing table to find a fresh route towards the requested destination in RREQ. If such a route is found, a RREP message is sent through the pre-established reverse route towards the source S. If the intermediate node does not find a fresh route, it updated its routing table and sends RREQ to these neighbors. This process is reiterated until RREQ reaches destination node D. The destination node D sends RREP to S by using the pre-established reverse route. It should be noted that source S can receive several RREP, it will choose that whose destination's sequence number is larger, if destination's sequence number of several RREP are equal, that of which the smallest hope counter will be selected.

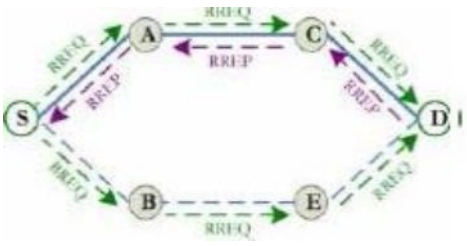

Fig.4:- Route Discovery Process of AODV

2.2.2 Route Maintenance Module:- AODV uses Hello messages to maintain the connectivity between nodes. Each node periodically sends a Hello message to neighbors and awaits Hello messages on behalf of these neighbors. If Hello messages are exchanged in two directions, a symmetrical link between nodes is always maintained if no link interrupt occurs. The broken link is repaired locally by the node upstream, else a route error (RERR) message is sent to the source S. This can launch again the route discovery procedure. It should be noted that the link interrupt is the consequence of the mobility or breakdown of nodes. [5]

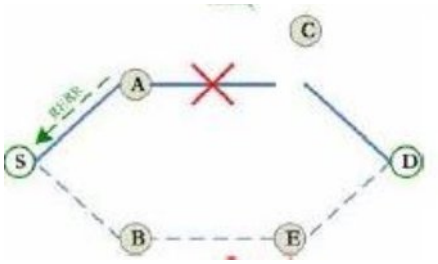

Fig.5:- Route Maintenance Process of AODV

3. Related Work

In this section, the previous work done on different kinds of attacks and the detection methods on
various routing protocol in MANETS is being stated. In related research Vipin Khandelwal has described that AODV routing protocol uses sequence number to determine the current network topology information. In AODV malicious node takes the advantage of this sequence number and hence attack is created in our network by increasing higher value. The technique discussed is pre-process. But this preprocess introduced additional delay due to pre-process only. In related research k.konate [6] has described various attacks against MANETs. In related research Meenakshi Patel [7] has described techniques detection and prevention attack against routing in MANET. Bansal and Baker [8] had proposed a scheme that relies on first-hand observations. Sen et. al had presented a scheme for detection of malicious packet dropping nodes in MANET [9]. The mechanism is based on local misbehavior detection and flodding of detection information. Deng, Li and Aggarwal [10] have suggested a mechanism of defence against black-hole in ad-hoc networks, in this proposed scheme as soon as the route reply packet is received from one of the intermediate nodes, another route request was sent from the source node to a neighbour node of the intermediate node in the path.

This is to ensure that such a path existed from the intermediate node to the destination node.

3.1 DPRAODV Scheme [11]:-

In this scheme, the authors had set up a threshold value for the sequence number. If the received sequence number was higher than the threshold value, then the sender node was regarded as black-hole node and then a blacklist was constructed with the attacker node. This scheme used a control packet called "ALARM" message to tell the neighboring nodes about this malicious node.

Discussion-This scheme increases the packet delivery ratio with nominal increase in routing overhead. This method cannot detect the cooperative black-hole attack. Also the false detection ratio of this scheme is high. The control packet overhead is also present .

3.2 Distributed Cooperative Mechanism [12]:-

In DCM method, the authors had detected and alleviated the black-hole node through four step procedure. In the first phase, each node maintained an additional table named as estimation table which constitutes the evaluation of credibility of each node based on the overhearing of packets. If a suspicion was found then the node enters the second phase of local detection in which it checks with the partner cooperative node. If the inspection value was found to be negative then the node enters third phase in which all one-hop neighbors were involved in broadcasting about the credibility of that suspicious node. Finally, in global reaction phase, the information was shared with all the nodes of the network and thus the blackhole node is detached.

Discussion:-The distributed and cooperative mechanism provides higher values of packet delivery ratio. But routing control overhead was very high because multiple control packets are shared among nodes during phase second and third.

3.3 Neighborhood Based Method [13]:-

The basic approach depends upon the difference between the neighbor sets. The source compared the received neighbor sets and if the difference between them is found to be greater than threshold value the corresponding node is assumed to be blackhole node.

Discussion:-This scheme is highly efficient as it improves the throughput by 15% but it adds to the routing control overhead by the introduction of two additional control packets. But this scheme cannot detect the cooperative blackhole attacks. This method fails in the scenario where the malicious nodes can forge fake RREPs.

3.4 Time-Based Threshold Detection Scheme [14]:-

In this scheme, the basic idea is to check the time of receiving first route request with the timer threshold value. Every node after receiving first request sets timer in "Timer Expired Table" and the subsequent requests will be received until the timer expires. It will store the sequence number and the time at which route request arrives in "Collect Route Reply Table". After timeout, it first checks its CRRT whether there is any same next hop node. If the next hop is repeated then it assumes that the path is safe i.e. does not contain any malicious node .

Discussion:- Time-based mechanism delivers high packet delivery ratio with nominal routing overhead. The scheme is limited in use because if there is no repetition of next hop node then it selects random route from CRTT and there can be chances of black-hole node being present over there. Also end-to-end delay may be raised when malicious node is away from source.

4. Proposed Work:

The approach that is discussed here is based on the Backbone network discussed by Rubin et. al. A backbone network is maintained which operates at a level above the ad-hoc network. This idea is basically used to control the traffic flow.

In this algorithm nodes are divided into three parts :-

I. Regular Node(RN):- low power and low transmission range, not trustworthy.
II. Backbone Node(BN):- have high transmission range and form a core that monitors the nodes.
III. Backbone core Node(BCN):- similar power as BN, these nodes can be elevated to BN nodes for increasing connectivity and coverage of the network.

Algorithm:-

This algorithm is mainly having two parts:-

- Core formation and maintenance.
- Detection of malicious node.

Core Formation and maintenance:

- Source node broadcasts RREQ message.
- Source node receives RREP message and check if it is reachable in specified number of hop.
  If, yes add in associated node list
  Else, in unassociated node list.
- If no other request go to the grid.
- If backbone core node does not detect any backbone node in its neighbor then this node sends a coordination message to backbone node and waits for reply.

- Backbone Core node on receiving reply to coordination reply to coordination message, it executes action which is specified in the reply.

Black-hole Attack:-

The key idea is that the source node, after every block of data packets asks the backbone network and perform end-to-end check with the destination, whether the packets have reached it. If destination does not receive a block of data packets, then backbone network initiates the detection of the chain of malicious nodes.

Assumptions:

N1: Backbone node, to which source node is associated.

N2: Backbone node, to which destination node is associated.

Nr: is the node to which send RREP to source(for the RREQ for source to destination route)

Steps:-

i. Firstly divide the data into k equal parts i.e.[1….k].

ii. Then send an introductory message to destination node with a symmetric key K.

iii. Now send the data to destination and after that send a message check having Nr, to N1.
If an "OK" is received from N1 then send a timer for malicious removal.
If a "NOT OK" is received from N! then set a timer for malicious removal and if before timeout receive the "REMOVED OK" from N1 then go to Step second. Else terminate .

iv. Action of N1:On receiving introductory message from source, send monitor message to all neighbors of source asking them to monitor data sent by source.

v. On receiving "CHECK" from source send query to all neighbors of source and waits for results message and on receiving this set its max counter value. If it receives "Destination Malicious" then repeat the steps and if not receive any message then terminate. In the same way N2 also does the same.

vi. Regular node on receiving monitor check if source is its neighbor then start counting the number of packets source to destination and also on receiving query message send result message to the source of the query message. Once the BN say N1 finds that acknowledgement message not received until a predefined timeout. Then Black Hole removal process get initiated by N1.

5. Conclusion:-

In this paper focus is on different control messages of AODV and working of AODV. In the proposed methodology In the proposed methodology how can black hole attacks in AODV be detected is discussed. Using this proposed algorithm, the Simple Black Hole attack and Cooperative Black hole attack and to some extent Gray hole attack can be removed. Through this algorithm we can get to know how black hole attacks in AODV can be detected through Backbone network concept. The proposed solution here does not increase the overhead of routes. Future work in this direction is in progress.

References:-

[1] D. S. P. D. P. D. Rajib Das, "Security Measures for Black Hole Attack in MANET:An Appraoch," p. 2.

[2] A. K. M. S. a. G. B. Samyak Shah, "Performance Evaluation of Ad Hoc Routing Protocols Using NS2 Simulation," in *Mobile and Pervasive Computing*, 2008.

[3] &. H. G. Rajan Bansal, "Analytical Study the performance Evaluation of Mobile Adhoc Network using AODV Protocol," *International Journal of Computer Application,* Jan 2011.

[4] R. C. &. R. K. R. Preeti Bhati, "An efficient Agent based AODV Routing Protocol in MANET," *International Journal on Computer Science & Engineering Vol No 7,* July 2007.

[5] P. B. R. Monika Roopak, "Blackhole attack implementation in AODV routing Protocol," *International Journal of Scientific & Engineering Research, Volume 4, Issue 5.*

[6] G. A. K. Konate, "Attack Analysis in mobile ad hoc net-works: Modeling and

Simulation," in *Second Internal Conference on Intelligent System, Modeling and Simulation*, 2011.

[7] S. S. Meenakshi Patel, "Detection and prevention of Routing Attacks in MANET using AODV," *International Journal of Advanced Research in Computer Science and Electronics Engineering,* 2012.

[8] A. B. Satyanarayan Vuppala, "A Simulation Anal-ysis of Node Selfishness in MANET using NS-3," *Int. J. of Recent Trends in Engineering and Technology,* Nov,2011.

[9] D. A. S. Bhargava, "Security Enhancements in AODV protocol for Wireless Ad Hoc Networks," *IEEE,* 2001.

[10] A.Boukerche, "Performance Evaluation of routing Protocol for AdHoc Wireless Network," in *Mobile Network and Application*.

[11] P. B. S. Payal N. Raj, ""DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Bodv," *International Journal of Computer Science Issues,* pp. 54-59, 2009.

[12] W. T.-K. C. R. S. c. c. Chang Wu Yu, "A Distributed and Cooperative Black Hole Node Detection," *Emerging Technologies in knowledge Discovery and Data,* pp. 538-549, 2007.

[13] Y. G. J. C. a. U. P. B. Sun, "Detecting blackhole attack in mobile ad hoc networks," in *Proc. 5th European Personal Mobile Communications Conference*, Apr. 2003.

[14] S. V. Tamilselvan L, "Prevention of Blackhole Attack in MANET," in *2nd International Conference on Wireless Broadband and Ultra Wideband Communications,*, Sydney, Australia,, August,2007.