BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN(Print):2348-0513; ISSN(Online): 2454-471X;
Vol. 3, Issue 9, Sep 2015, 101-108
© BEST Journals

DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN MANETS

A. BALA KISHORE & KAMAKSHI M B

Telecommunication, R.V. College of Engineering, Karnataka, India

ABSTRACT

A Mobile Adhoc network (MANET) is a self-configuring network which consists of mobile nodes connecting each other without any infrastructure. Each node can send packets to other nodes through intermediate nodes and these intermediate nodes acts like router. AODV (Adhoc on demand distance vector) is a loop free reactive routing protocol used in these networks for the routing operation. These MANETs are open to many attacks, of which blackhole attack is one of the passive attack which drops the packets without forwarding them to the neighboring nodes. In this paper, an algorithm is developed to detect and bypass the attacker without disturbing the data packets and thereby create a safe path for the packet to reach the destination.

KEYWORDS: ADHOC Network, AODV, Blackhole Attack, MANET

INTRODUCTION TO MANET

A Mobile Adhoc network (MANET) [1] is a collection of wireless devices or nodes without any pre-established infrastructure which can be created anywhere independent of environment. These MANETs consists of mobile nodes which can move freely in any direction and therefore changes its topology frequently. Each node in this network has information about the next neighbour nodes. Nodes in these networks can communicate to each other by using multihop transmission as shown in figure 1. If a destination node is present within the transmission range of source node, then direct transmission will takes place. If not, a path from source to destination will be created by using neighboring nodes and the packet will be sent in the selected path. Each node in this network acts like host or router.

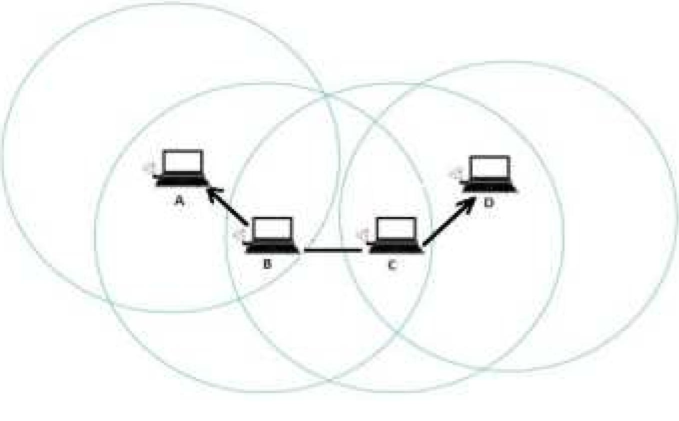

Figure 1: Example of MANET

A routing protocol [2] is needed in MANETs for routing a packet in a path. Reactive (on-demand) and proactive (Table driven) are the two types of routing Protocols in MANETs used for creating and maintaining the paths in MANETs.

Main characteristics of MANETs include operating without any centralized infrastructure, Multihop transmission, recreation of link breakage path, constant resources like power, bandwidth, battery lifetime etc.

MANETs are open to many security issues as any mobile host or node can enter into the network and can either view the information or alter it while passing in the network.

Overview of AODV Protocol

Adhoc on demand distance vector (AODV) [12] is a reactive routing protocol which creates a path on demand using control packets. The main advantage of this routing protocol when compared to other protocols is the usage of destination sequence number for identifying the most recent path. Whenever any node changes its position, it updates its sequence number and broadcast to the network. A node updates its path only when the destination sequence number of the current packet is greater than the destination sequence number for the previous packet.

Whenever a source node wants to send data to a destination node, it will check in its routing table if it has any route to the destination. It sends data packet to the destination node if it has a path. If the source node does not have a path, it will create a RREQ (route request) packet and broadcast it to its neighbours. If any neighbour node is the destination node, it receives RREQ packet sent by the sender. If it is not the destination node, it will again broadcast the RREQ packets to its neighbours and this process continues until the packet reaches the destination.

After receiving RREQ packet, destination node will create a Route reply (RREP) packet and forwards in unidirectional path which contains less number of hops to source node. The source node will now send the data packet in the RREP path. If any link breakage occurs in the path, then the upstream node in the path will create a Route error (RERR) packet and forwards it to the source node. Then the source node creates a new path to destination using the same process as shown in figure 2.

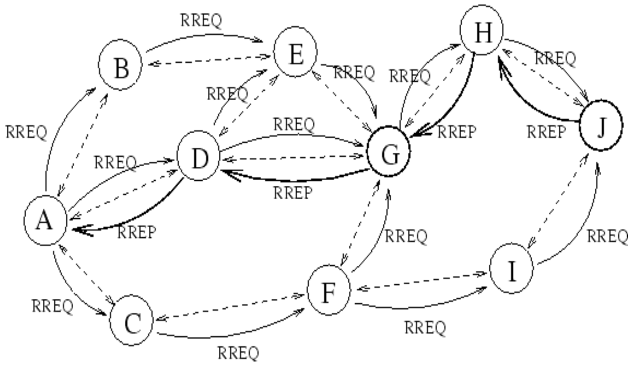

Figure 2: Working of AODV Routing Protocol

Blackhole Attack

Security is the major issue in MANETs where the network is prone to many attacks which are classified into active and passive attacks. Blackhole attack [3] [8] is one such kind of active attack where the attacker node(maliciousnode) advertises itself as having a fresh route to the destination by generating RREP packet with high destination sequence number. Thinking that the path through the attacker node is a fresh route, source node will send data packet in that path. After receiving packet, the malicious node drops the packet instead of forwarding to destination. So the throughput and packet delivery ratio for the network in the presence of blackhole node is zero.

LITERATURE SURVEY

LathaTamilselvan, DR.V. Sankaranarayanan [15] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is given to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide to that node. Any node having 0 value is considered as malicious node and is eliminated.

Hesiri Weerasinghe [17] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the Ramaswamy to improve the accuracy. This algorithm uses a methodology to identify multiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP).

In [21], the authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

Lalit Himral et al [22] have proposed method to find the secured routes and prevent the black hole nodes (malicious node) in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back first RREP or not. Generally, the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely it is from the malicious node. Immediately remove that entry from the RR-Table.

ALGORITHM

Malicious node usually absorbs packets and will not forward it to the next node instead, it will drop the packets. So an algorithm was developed to detect a node which only receives packets but not forwarding it. The algorithm to detect and prevent the malicious node is as explained below.

```
{
IF time is start of simulation THEN
BEGIN
        Initialize quarantine list;
        Initialize activity table of neighbours;
        This table has following fields:
        (Node id, number of received data, number of sent data, number of sent rrep)
```

```
END
IF packet is data THEN
BEGIN
     INCREMENT number of received data for sender of packet
    IF this node isn't destination THEN
    BEGIN
        GET next node which isn't in quarantine list
        IF found next node for forwarding THEN
        BEGIN
            FORWARD packet to next node
            INCREMENT number of sent data to next node
        END
        ELSE
        SEND error packet to source
    END
    ELSE
    RECIEVE packet
END
IF packet is rrep THEN
BEGIN
    INCREMENT number of received rrep for sender of packet
    IF sender isn't in quarantine list THEN
    BEGIN
        CREATE an opinion request packet and broadcast to neighbours of rrep's sender FORWARD packet
    END
    ELSE
    BEGIN
        IGNORE the reply from the blacklisted node
        BUILD the route to destination with latest sequence number and small hop count
    END
```

```
END
IF packet is opinion request THEN
BEGIN
    CHECK if this node has any opinion about requested node
    IF this node has any opinion THEN
    BEGIN
        EXTRACT activities of the requested node from activity table (including number of received data,
        number of sent data, and number of sent rrep)
        CREATE response packet including the required information
        FORWARD response packet
    END
    ELSE
    FORWARD packet
END
IF packet is response packet THEN
BEGIN
    IF this node is sender of the opinion request packet THEN
    BEGIN
        EXTRACT information from packet (including number of received data, number of sent data, and
        number of sent rrep)
        IF ((sum of sent rrep’s is high) and (sum of sent data is low) and (sum of received data is high)) THEN
        BEGIN
            ADD attacker to quarantine list
            REMOVE all routes to this node present in the routing table
        END
    END
    ELSE
    FORWARD packet
END
}
```

Quarantine list table and activity table of neighbours are the two tables which are created in the above algorithm, where Quarantine list table consists of the list of malicious nodes, and the activity table of neighbours consists of the number of packets sent and received for each node which will be updated for every transmission and reception of the packet.

Opinion request packet and response packet are two more packets used to fetch information about the unknown node to decide whether the node is malicious or not.

PERFORMANCE PARAMETERS

Throughput, Packet delivery ratio and packet drop are some of the parameters which are used to find the efficiency of the network. These parameters are calculated for the network before adding malicious node, after adding malicious node, and after bypassing malicious node and are compared. The observed results after bypassing malicious node shows the efficiency. These parameters are explained below.

Throughput defines the rate at which the packets are successfully delivered between source and sink. The value of throughput is more for the network with better performance.

$$\textbf{Throughput}=\frac{\textbf{Total number of packets received}}{\textbf{[Stop time – Start time]}}$$

Packet delivery ratio is defined as the ratio of number of packets delivered to the destination and the number of packets sent by the source. The value of Packet delivery ratio must be high for better network performance. Its higher ratio leads to the reduction in the drop rate of packets.

$$\textbf{Packet delivery ratio}= \frac{\textbf{Number of packets received}}{\textbf{Number of packets sent}}$$

Packet drop is defined as the number of packets dropped due to the breaks in the paths, packet life time, movement of the nodes etc.

$$\textbf{Packet drop = Number of packets dropped}$$

CONCLUSIONS

Black hole attack is a denial of service attack which drops the data packet without reaching destination. The new proposed algorithm detects the black hole at the time of establishment of path. From the results obtained, it is observed that when the malicious node is present in the network:

- It drastically reduces the number of packets delivered to the destination.
- The throughput of the network decreases drastically.
- Number of packets dropped are increasing more.
- After bypassing the blackhole node, route resuming is done. It is observed that:
- Packet delivery ratio is far better than that of blackhole attack.

- Throughput of the network increases and reaches to satisfactory level.
- Number of packet drops in a network is reduced when compared with the network consisting black hole node.

REFERENCES

1. Islam, N. et al "A Novel Approach to Service Discovery in Mobile Adhoc Network," Networking and Communications Conference, 2008. INCC 2008. IEEE International, vol., no., pp.58, 62, 1-3 May 2008.
2. Istikmal; Leanna, et al "Comparison of proactive and reactive routing protocol in mobile adhoc network based on “Ant-algorithm”," Computer, Control, Informatics and Its Applications (IC3INA), 2013 International Conference on , vol., no., pp.153,158, 19-21 Nov. 2013.
3. Mandala, et al"A review of blackhole attack in mobile adhoc network," Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2013 3rd International Conference on, vol., no., pp.339, 344, 7-8 Nov. 2013.
4. Perkins, et al “Ad-hoc on-demand distance vector routing,” Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on, vol., no., pp.90, 100, 25-26 Feb 1999.
5. Medadian, et al “Combat with Black Hole attack in AODV routing protocol”, Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, vol., no., pp.530, 535, 15-17 Dec. 2009.
6. Amol A. Bhosle, et al“Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET”, International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012.
7. Payal N. Raj et al “DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET”, International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.
8. Mohammad Al-shurman, et al “Black Hole Attack in Mobile Ad Hoc Networks”, ACM Southeast Regional Conference, Proceedings of the 42nd annual southeast regional conference, 2004, pp 96-97.
9. LathaTamilselvan et al “Prevention of Black Hole Attack in MANET”, Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.
10. Mehdi Medadian et al “Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol”, European Journal of Scientific Research ISSN 1450-216X Vol.69 No.1 (2012), pp.91-101.
11. Mangesh Ghonge et al“Simulation of AODV under Blackhole Attack in MANET” Volume 2, Issue 2, February 2012 ISSN: 2277 128X, International Journal of Advanced Research in Computer Science and Software Engineering.
12. Monika Roopak et al “Performance Analysis of Aodv Protocol under Black Hole Attack”, International Journal of Scientific & Engineering Research Volume 2, Issue 8, August-2011 ISSN 2229-5518.
13. Savner, J et al "Clustering of mobile ad hoc networks: An approach for black hole prevention," Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on , vol., no., pp.361,365, 7-8 Feb. 2014.

14. Surana K.A et al “Securing Black Hole attack in Routing Protocol AODV in MANET with Watchdog Mechanisms”, World Research Journal of Computer Architecture, Vol. 1 Issue 1, 2012, pp. 19-23.

15. Douglas S. J. De Couto et al“A High-Throughput Path Metric for Multi-Hop Wireless routing”, in ACM Mobicom, 2003.

16. Thachil, F et al"A Trust Based Approach for AODV Protocol to Mitigate Black Hole Attack in MANET," Computing Sciences (ICCS), 2012 International Conference on , vol., no., pp.281,285, 14-15 Sept. 2012.

17. Ms Monika et al “Detecting and Overcoming Blackhole Attack in Aodv Protocol”, International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 2013, pp. 77-82.