TECH-CHRONICLE
AN INTERNATIONAL E-JOURNAL ON
EMERGING TRENDS IN SCIENCE, TECHNOLOGY AND MANAGEMENT

Prevention and Detection of Black hole attack in Manet: A survey

Tripti Sharma
Department of formation hnology, Maharaja Surajmal Instituteof echnology, New Delhi, India-10058
triptionline@yahoo.com

Kiratdeep Singh
Department of Information technology, Maharaja Surajmal Institute of Technology, New Delhi, India-110058
kiratdeep5@gmail.com

Dhruv Sharma
Department of Information Technology, Maharaja Surajmal Institute of Technology, New Delhi, India-110058
dhruvsharma360@gmail.com

HarshitAilawadi
Department of Information Technology, Maharaja Surajmal Institute of Technology, New Delhi, India-110058
ailawadiharshit@gmail.com

Abstract—A prominent security threat in wireless mobile adhoc network is blackhole attack. Since, in AODV, route to destination is looked for adaptively, this loophole is used to carry out malicious hacking practices. A lot of work has been done to overcome the above stated problem. In this paper,the already present solutions have been analysed, comparisons has been done on the basis of various parameters.

Keywords— AODV, SAODV, Blackhole tack and MANET

1. INTRODUCTION

MANET- Mobile Adhoc Network dynamically constructs the network, which comprises of several mobile user devices. These devices inter-communicate with each other without any pre-established infrastructure. Rather, all the transmission links are established through connectionless medium.In spite of such technique for communication, many problems are still faced
about MANETs, namely Security issues, Finite transmission bandwidth etc. Some of the attacks are wormhole attack, black hole attack and denial of service (DoS). Out of the above mentioned security issues in MANET, this paper focuses on Blackhole attack in MANET.In the section 2routing protocols are discussed, in section3 discussion on security threats in MANET is done, in section 4 paper looks into the Black hole attack in MANET. Section 5and 6 have discussion about the attacks in AODV and SAODV, Finally section 6 concludes the papers.

2. BACKGROUND

There are many routing protocols in MANET. In this section we discuss some recognized protocols in MANET. Since, in MANET the network is unfamiliar with the current routing information, so while communicating with the destination node,
the source node should broadcast its present status to all the neighbours.

A. Proactive Routing Protocol

In this routing protocol, the nodes regularly send out their routing information to the adjacent nodes. Routing table is maintained by each and every node. The routing table of a particular node, in addition to the adjacent and reachable node also record the number of hops. The disadvantage of this protocol lies within, being, it increases the overhead when the network size increases. However, if a malicious attacker joins, the network status is immediately reflected. DSDV is the most familiar proactive type routing protocol.

B. Reactive Routing Protocol

Unlike proactive protocols, it is started when nodes wants to send packets. The plus point of reactive routing protocol is that the bandwidth required to periodically send out information is saved. We consider one reactive protocol here, namely AODV.
In AODV, each node has the information about next hop in its routing table. If there is any discrepancy and destination node is not reached from source, immediately route delivery process will be executed. Following procedure is followed for route discovery process:
The source node sends out RREQ packet, then all the neighbouring nodes receive the same, but only a few send back the RREP packet to the source node if information about destination node occurs in their routing table. Where process of route

maintenancetakes place when connection has failed or there is a failure in network topology. RERR is sent to the source node in such a case. Then routing information so present is used to decide a new routing path.

C. Hybrid Protocol

It combines the best of both worlds. In beginning, proactive protocol is used to get all the routing information, subsequently, when the network topology changes, reactive routing protocol is employed. Known protocols are TORA and ZRP.

3. SECURITY THREATS IN MANET

The attacks can be broadly divided into two categories:

A. Passive Attacks

Passive attacks are the attacks in which attacker does not directly participate in bringing the network down. In this attacker simply looks on the network and observers the traffic of the network that which node is trying to routes to which node. And which node is vulnerable and a good candidate for the Denial of service (Dos) attack. The attacker can then give this information to a partner which can use this information to bring the network down.

B. Active Attacks

In Active attacks and attacker actively participates in inhibiting the normal operation of the network. The attacker can drop some packets, can modify the packets or can even fabricates the message. And in this the attacker can even tunnel them over a high-speed private network to a partner in other part of the network. Black hole attack is active in nature.

4. BLACK HOLE ATTACK

In networking Black hole are those points or the nodes where either the incoming traffic or the outgoing traffic is silently discarded and the source is not informed about the lost traffic. Black holes or so called the malicious node can only be detected by only monitoring the data traffic.These malicious nodes can also be working in groups and can do very serious damage to the information and can compromise very important data. Such a type is called as Cooperative Blackhole attack.

The malicious nodes initially must be a part of the data route which is connecting the source and destination nodes. After that it can start its work that is to absorb the data into or data/packet dropping.

Blackhole attacks are of two types:

a. Internal Blackhole Attack

In this attack the malicious node is already a part of the network and does not seek to fit in an active route between the source and the destination. But as soon as it becomes the part of the active route it can start conducting its attack.

b. External Blackhole Attack

In this attack the malicious node is not a part of the route and is an external node. It violates the network in the following way:

1) The malicious node continuously looks for an active route as soon as it detects a route it notes down the destination address.
2) The malicious node prepares a Route Reply Packet (RREP) with destination address set to the new spoofed destination address. The sequence number is set to the highest and hop count is set to lowest.
3) The malicious node sends this packet (RREP) to the nearby nodes of the active route. This packet can also be sent directly to the source node if available. This packet which is sent to intermediate node can now be sent via the backward route path to the data source node.
4) The source node updates its routing table with the new information received in the Route Reply Packet (RREP).
5) The source node the sends the data packet through the new route.
6) The malicious node starts dropping the data of the active route to which it belongs.

5. AODV

AODV isAd Hoc On-Demand Distance Vector which is a protocol used for routing purposes in ad hoc mobile networks having nodes in large numbers. This protocol's algorithm creates routes only when the routes are requested by the source nodes between them which gives flexibility to the network which allow nodes to enter and leave the network at their will. Routes will remain active only as long as the data packets are travelling along them from the source to the destination. The route will automatically get closed when the source stops sending packets to the destination. AODV supports both unicast and multicast.

The Ad hoc On-Demand Distance Vector (AODV) algorithm creates dynamic, self-starting and multi-hop routing between participating mobile nodes to establish and maintain the network. AODV allows mobile nodes to obtain the routes for new destinations immediately, which does not require nodes for the maintenance of routes to destinations which are not active in the communication. AODV also allows mobile nodes to respond to the breakages in link, if any and starts changing in network topology in time. When links break, AODV causes the affected set of nodes to get notification so that they can invalidate the routes which are using the lost link.

6. SAODV

Secure AODV (SAODV) is extension of AODV routing protocol. There are two mechanisms which are used to secure the messages in AODV. One of them is hash chains for securing the information about hop count which is the one and only mutable information in the messages; and the other is digital signatures which are used for authentication of the non-mutable fields of the messages. The information about the hash chains and the signatures is transmitted along with the AODV message as an extension message. SAODV uses hash chains to authenticate the hop count of RREQ and RREP messages in such a way that allows every destination node to verify that the hop count has not been decremented by an hacker. A hash chain is formed by applying a one-way hash function again and again. Digital signatures are used in SAODV to protect the integrity of the non-mutable data in RREQ and RREP messages which means that everything is signed by them but the Hop Count of the AODV message and the Hash from the SAODV.

7. CONCLUSIONS

SAODV can prevent black hole attack in MANET effectively, and also maintain a high routing efficiency. So SAODV is more secure and efficient routing protocol in MANET than AODV. Its security is better than AODV's, and its routing efficiency is not worse than AODV's.

Although SAODV can increase MANET's security, it brings some burden to the network, such as the source node needs to store the received RREP in each routing discovery phase, and to do relevant calculation. The destination node also needs to store received RREQ in each routing discovery phase, and to do relevant calculation. The future research should have better balance in safety and efficiency, to achieve a more secure routing protocol, in which efficiency is better, and at the same time, the network performance of MANET is also better.

8. REFERENCES

[1] SatyabrataChakarbarti and Amitabh Mishra "Quality of service in mobile and adhoc networks". The Electrical Engineering Handbook Series. 2013

[2] Bangnan Xu, Hischke, S. and Walke, B. "The role of Ad hoc networking in future wireless communications". In Proceedings of ICCT Communication Technology. 2003.

[3] Roberto Beraldi and Roberto Baldoni. "Unicast Routing Techniques for mobile Ad hoc networks". The Electrical Engineering Handbook Series. 2003.

[4] Luo Junhai, Xue Liu and Ye Danxia. "Research on multicast routing protocols for mobile ad-hoc networks". Computer Networks: The International Journal of Computer and Telecommunications Networking. 2008.

[5]Perkins C.E., Belding-Royer E. and Das S. "Ad hoc On Demand Distance Vector (AODV) Routing". 2003.

[6] Weerasinghe, H. and Huirong Fu. "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Network: Simulation Implementation and Evaluation". In: Future generation communication and networking(fgcn 2007). Jeju: 2007.

[7] Songbai Lu[1], Longxuan Li Kwok-Yan Lam[1], Lingyan Jia[21], "SAODV: A MANET Routing Protocol that can withstand Black Hole Attack" International Conference on Computational Intelligence and Security. 2009.

[8] E.M. Royer and C-K Toh, "A Review Of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks," IEEE Person. Commun., Vol. 6, no. 2, Apr. 1999.

[9] M. Khalini shoji, H. Taheri*, and S. Vakilinia**, "Preventing Black Hole Attack in AODV through Use of Hash Chain", 2010.*

[10] M. Zapata and N. Ashokan, "Securing Ad-Hoc Routing Protocols" in proc. Of ACM Workshop on Wireless Security(WiSe), Atlanta, GA, Sept.2002.

[11] M. F. Juwad, H. S. Al-Raweshidy, "Experimantal Performance Comparisons between SAODV and AODV", Second Asia International Conference on Modelling &Simulation, 2008:249.