UACEE International Journal of Advances in Computer Networks and its Security – IJCNS
Volume 3 : Issue 2 [ISSN 2250 – 3757]
Publication Date : 05 June 2013

Preventing Black hole Attacks in Mobile adhoc Networks: A Review

Preeti Kamra
Amritsar College of Engineering & Technology, India
mongapreeti@yahoo.com

Tanu Preet Singh
PhD Research Scholar,
Uttarakhand Technical University, Dehradun, India
tanupreet.singh@gmail.com

Dr. R.K Singh
Prof. & OSD,
Uttarakhand Technical University, Dehradun, India
rksinghkec12@rediffmail.com

***Abstract* - Wireless networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic position. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET). Black hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network. MANETs must have a secure way for transmission and communication which is quite challenging and vital issue. In this paper, a brief overview is given about the black hole attack on MANETs and various kind of routing protocols which get affected by the Black Hole attack along with an overview about the countermeasures to avoid it.**

Keywords: MANETs, AODV, Routing protocol, black hole attack.

I. Introduction

In a wireless mobile ad hoc network (MANET), there are no basic network devices, such as routers or access points; data transfer among nodes is realized by means of multiple hops, and rather than just serving as a single terminal, every mobile node acts as a router to establish a route. When a source node intends to transfer data to a destination node, packets are transferred through the intermediate nodes, thus, searching for and quickly establishing a route from a source to a destination node is an important issue for MANETs. Mobile nodes present within the range of wireless link can overhear and even participate in the network. However this lead to security issues because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defence mechanism.

Wireless ad hoc networks are vulnerable to various attacks. These include passive eavesdropping, active interfering, impersonation, and denial-of-service. The scope of this paper is to study the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad-Hoc on Demand Distance Vector (AODV). Comparative analysis of Black Hole attack for both protocols is taken into account. The impact of Black Hole attack on the performance of MANET is evaluated finding out which protocol is more vulnerable to the attack and how much is the impact of the attack on both protocols. The measurements were taken in the light of throughput, end-to-end delay and network load. Simulation is done in Optimized Network Engineering Tool (OPNET).

II. Classification of MANETs Routing Protocols

Routing protocols in MANETs are classified into three different categories according to their functionality

1. Reactive protocols
2. Proactive protocols
3. Hybrid protocols

The hierarchy of these protocols is shown bellow in the figure 1.

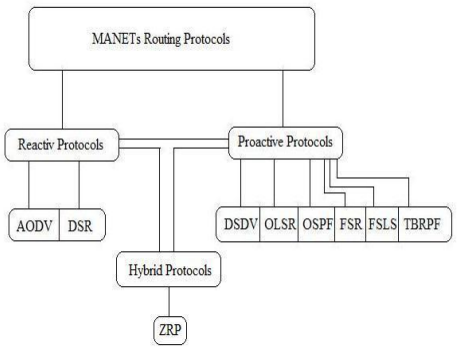

Fig. 1 : Classification of Routing Protocols

1) Reactive Protocols:

Reactive protocols also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route.[3, 4].

2) Proactive Protocols:

Proactive routing protocols work as the other way around as compared to reactive routing protocols. These protocols constantly maintain the updated topology of the network.

3) Hybrid Protocols:

Hybrid protocols exploit the strengths of both reactive and proactive protocols, and combine them together to get better results.

The various Flaws in MANETS which lead to different types of attacks are:-

Non Secure Boundaries: MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Spoofing of node's identity, data tempering, confidential information leakage and impersonating node are the results of such attacks when security is compromised [9].

Compromised Node: Mobile nodes in MANET are free to move, join or leave the network. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity.

No Central Management: MANET is a self-configurable network, which consists of Mobile nodes where the communication among these mobile nodes is done without a central control. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management.

Problem of Scalability: The nodes are free to move in and out of the Ad-Hoc network which makes the Ad-Hoc network very much scalable and shrinkable.

III. Black Hole Attack In MANETs

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address[22].. This attack is called a black hole as it swallows all objects; data packets [15].

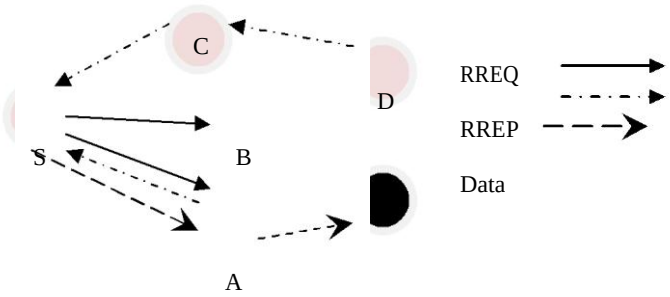

Fig. 2 Black hole attacks in MANETs

In figure 2, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a black hole. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D.

Black hole attack in Ad-Hoc On Demand Distance Vector (AODV).

Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack.

Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route

External Black hole attack

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

Black hole attack in Optimized Link State Routing Protocol (OLSR)

In OLSR black hole attack, a malicious node keeps its willingness field to will always in its HELLO message. So in this case, neighbours of malicious node will always select it as Multiple Point Relay. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack. The effect of this attack is much vulnerable when more than one malicious node is present near the sender and destination nodes.

Iv.Countermeasures

In preventive mechanism, authentications, access controls, and encryption techniques are involved. While in Reactive mechanism, different schemes like intrusion detection systems (IDS) and cooperation mechanisms are used. In case of MANET intrusion is used for detection of misuse.

4.1 Mitigation Techniques against Black Hole Attack

The network layer is far more vulnerable for attacks than any layer in MANET. Numerous security threats are imposed on this layer. One way is to use secure routing protocol. Attack which modifies routing messages can be provoked by the use of source authentication. Digital signature, message authentication code (MAC), hashed MAC (HMAC) can be used. Up to certain level of security can be attained at network layer in internet by the use of IPSec. Authenticated Routing for Ad-Hoc Networks (ARAN) is another routing protocol which provides the protection from Black Hole attack where there is threat to the changes in sequence number, hop count modification, source routing changes and spoofing of destination addresses.

4.2 Mitigation by Confirmation Request Message

It has been proposed route confirmation request message (CREQ) and route confirmation reply (CREP) in order to avoid Black Hole attack. In this proposal when intermediate nodes sends Requests to the source node its send CREQ to its next hop node in direction of destination node. After receiving CREQ, the next hop look for route in its destination in cache.

4.3 Mitigation by SAODV protocol

The Secure Ad-Hoc On-Demand Distance Vector Routing (SAODV) which verify the destination node by exchanging random numbers. SAODV can effectively prevent Black Hole attack in Mobile Ad-hoc network and maintain better routing efficiency. It is better than AODV in terms of security and routing efficiency.

4.4 Mitigation by checking multiple RREP

The solution focus on the requirement of a source node to wait unless the arrival of RREP packet from more than two nodes. When it receives multiple RREPs the source node check that there is any share hops or not. The source node will consider the routed safe if it finds the share hops. Its drawback is the introduction of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of node.

V.Conclusion

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. We discuss the various causes for the black hole attack and the countermeasures to prevent them.

References

[1] http://en.wikipedia.org/wiki/Personal_area_network , last visited 12, Apr, 2010.

[2] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, last visited 12, Apr, 2010. C.E.Perkins and E.M.Royer, "Ad-Hoc On Demand Distance Vector Routing,"

[3] Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.

[4] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.

[5] http://www.faqs.org/rfcs/rfc3561.html M.Abolhasan, T.Wysocki, E.Dutkiewicz, " A Review of Routing Protocols for

[6] Mobile Ad-Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia, June, 2003.

[7] Detection Algorithm for Mobile Ad-Hoc Neworks," International Journal of Network Security and Its Application (IJN SA), Vol. 1, No.1, April, 2009.

[8] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray

[9] Black Hole Attack in Mobile Ad-Hoc Networks," Second International Conference on Communications and Networking in china, pp.366-370, Aug, 2007.