A SURVEY PAPER ON DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN AODV PROTOCOL IN MANET

[1]Garima Solanki, [2]Dr. Rashmi Popli
[1] M.tech student, [2]Assistant Professor
[1]Department of Computer Science,
[1]J.C Bose University of Science and Technology, YMCA, Faridabad, India

Abstract: Mobile ad-hoc network is a constantly developing field still there are lots of things that need to be developed and enhanced such as security measures. As manet has self organizing nodes there are lots of ways in which they can communicate with each other, so protocols were developed to establish route between the nodes but all the nodes may not be trustworthy nodes or there can be one or more malicious node which can corrupt the network information may not allow the data packet to follow its original or correct path,the packet can be route request packet or the data packet. Attacks are major issue in routing protocols like Black hole attack which severely disturbs the packet transmission from source to destination attracting the packet to the malicious node telling it has the optimum route for data transmission. It is difficult to identify attacks like Black hole attack in AODV protocol, AODV protocol is one of the reactive protocols .It is initiated on demand from some node in order to find the route from source to destination while travelling the intermediate nodes. In this paper Black hole attack in MANET is discussed and various measures to detect and prevent it are discussed.

In AODV protocol Black hole attack can be launched by either a single malicious node a group of malicious nodes attacking simultaneously called as collaborative attack.

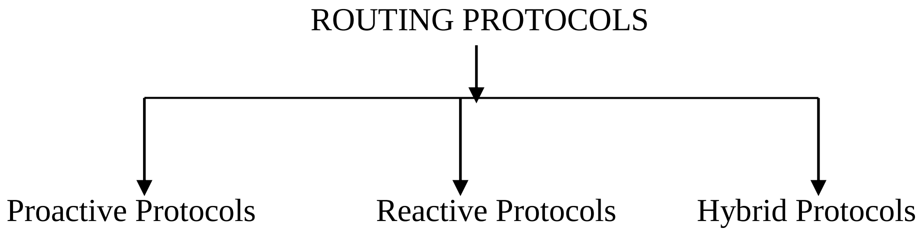
Index terms: **Black hole attack, MANET, Malicious node, collaborative attack, AODV protocol.**

1. Introduction

Mobile ad hoc network has dynamic, self organizing nodes, where each node acts as sender, receiver and router itself. MANET is cost effective, less time consuming and more robust than cellular network but due to its continuously moving nodes, less battery power and security issues it is a great challenge to pass information.

Characteristics of MANET are free movement of nodes, dynamic topology in order to establish communication, any node can connect or leave the network at any point of time whenever required, limited resources and no central point of coordination.

Routing in MANET is classified based on previously stored information and information gathered on demand or both, on basis of that information routing protocols are categorized as follows:



Routing protocols are divided into three major categories that is Proactive, Reactive and Hybrid Protocols which are further having protocols beneath them.

Proactive Protocols are the ones which have the information of neighboring nodes previously stored in routing tables. Destination sequenced Distance vector routing protocol (DSDV), OLSR are examples of proactive protocols.

Reactive Protocols are the ones which don't have any previously stored information the route finding phase is initiated on demand and the information is stored in route cache instead of tables. Ad hoc On Demand Distance Vector routing protocol (AODV), Dynamic Source Routing protocol (DSR) are examples of reactive protocol.

Hybrid routing protocols takes the advantages of both proactive and reactive routing protocols. Zone based routing protocol (ZRP).

2. Ad Hoc On-Demand Distance Vector Routing

AODV establishes routes to destinations on demand of a source node that is why it is called as an on demand routing protocol .It supports both unicast and multicast routing. AODV uses sequence numbers in order to check the most recent route, sequence numbers are increasing numbers. Even if any node relocates from its position the sequence number is changed. Route request packets (RREQ) and Route reply packets (RREP) are used to establish path and if any error occurs while establishing path error message is generated. Network node which needs to communicate broadcast a request for connection by sending RREQ, remaining nodes within the vicinity forward the RREQ packet and record the sequence number, so that they can scale back to the source node once the destination node is found and once the destination node is found number of hops are calculated associated with different routes to send back the reply once the route with minimum hop count is found the reply follows the same path.

But in case if link failure occurs the RERR is passed back to the transmitting nodes and whole of the process needs to be followed again as there is no local repair in this protocol which is the major disadvantage of this protocol.

3. Attacks in MANET

Attacks in Manet are classified as:-

3.1) <u>Active attack</u>: In active attack, attacker attempts to alter or modify the data being exchanged between the sender and receiver on the network. They disrupt the functioning of the network. Black hole attack, Worm hole attack, Man in middle attack are all examples of active attacks.

Active attacks can also be classified as:-

3.1.1) <u>External Attacks</u>: External attacks are launched by the malicious nodes outside, which are not part of the network.

3.1.2) <u>Internal Attacks</u>: Internal attacks are launched by the malicious nodes which are part of network but become compromise nodes in order to save its battery life or some other issue.

3.2) <u>Passive attack</u>: In passive attacks, attacker snoops or silently listens to the information being exchanged between sender and receiver on network without making any changes to it.

Passive attacks are generally used to collect information about the pattern of communication being used in the exchange of data. It targets the confidentiality of data and is very difficult to identify or detect this type of attack as it doesn't make any changes to network or its associated resources. Eavesdropping, spoofing are the examples of passive attacks.

4. Black hole Attack

In Black hole attack in Manet a malicious node attracts all the packets towards itself showcasing that it has optimum route towards the destination and once it gets all the packets, malicious node drops all of them, hence all the information is lost. Black hole attack can be launched by a single node or multiple nodes; the attack launched by multiple nodes simultaneously is called collaborative Black hole attack. Black hole attack is divided into two types:

Single Black hole attack: In this only one malicious node attacks on the network and gathers the whole information about the route or the data packet forwarded on that route.

Co-operative Black hole attack: In this attack number of nodes become malicious nodes and attack simultaneously .It is composite form of attack, it completely disturbs the routing of packets coming from source node and doesn't allow to reach them to destination.

4.1) Various techniques used in detection of Black hole attacks are as follows:

1) **Cross layer Cooperation:** Its speed to detect the malicious node or black hole is good. Less power is utilized as computation level is very low but it cannot work for co-operative Black hole attack.
2) **Trustiness and Neighbors:** Its speed is good for Single Black hole attack but cannot work good for co-operative Black hole attack. Moderate power is utilized in this technique but this too cannot work good for co-operative black hole attack.
3) **Genetic Algorithms:** Its speed becomes moderate when necessary data is presented. It utilizes more amount of power as the output is extensive in these algorithms. Its performance is better in both the types of Black hole attack that is Single Black hole attack and Co-operative Black hole attack.
4) **Route redundancy and message parameters:** Its peed is low as it uses multiple route request packets with sequence numbers at the time of detection of attack. More amount of power is utilized for the processing of controls packets as the overhead is large in this case. This technique has a good performance and it is secure too.
5) **Fuzzy Logic:** It has moderate speed of detection of the attack. A large amount of power is required due to a large amount of computation to be done on data for reducing the degree of attack at each node. It has best performance and can be used in case of co-operative Black hole attack efficiently.
6) **Mobile Agents:** Its speed of detection of attack is moderate and not much amount of power is required for computation and processing of data.
7) **Clustering Algorithms:** Its widely used technique for detecting black hole attack , its only disadvantage is that it requires large amount of power for data processing and securing the network from Black hole attack.
8) **Honeypot Based Detection Scheme:** Mobile honeypot agents are employed which utilize their topological knowledge and detect suspicious route advertisements. Valuable information regarding attacker's strategy is gathered from the intrusion logs stored at the installed Honeypots.

4.2) Prevention of Black hole Attack

For prevention of Black hole Attack all of the following services are required:

1) **Authentication:** In this technique identity of the node is verified so that the network can be protected from impersonation. In case of infrastructure based networks it can easily be done by a central authority but in case of MANET it is difficult to achieve as there is no central point of control and the nodes are continuously moving .In MANET authentication is achieved by using encryption along with cryptographic techniques.
2) **Confidentiality:** In case of confidentiality the data sent over the network can only be accessed by the intended user but in case of MANET there is open medium so all nodes within vicinity so to keep the data secure for the intended receiver directional antennas can be used.

3) **Integrity:** It ensures that the data that is being transmitted over the network is not altered or changed in the process of transmission.
4) **Availability:** It ensures that all the network resources and services that are required by the intended nodes are available whenever required by them. It can be achieved by physical protection and the use of robust protocols.
5) **Non-repudiation:** It ensures that neither the sender nor the receiver can falsely deny of sending or receiving the information or data. It can be achieved using digital signatures and public key cryptography techniques.
6) **Access control:** It ensures that the network services cannot be accessed by the unauthorized user; it is commonly used in network communications and individual computer systems.

5) Conclusion

In this paper many different techniques for detection and prevention of Black hole attack are discussed, all or some of these techniques can be used to avoid Black hole attack in MANET and to transmit data from sender to receiver without any changes. All the discussed techniques are efficiently used by various researchers to increase the throughput and decrease the delay, packet drop ratio and data loss rate.

6) References

1) Vimal Kumar, Rakesh Kumar, “An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network”. In: International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014).
2) Jathe s.r. and Dakhane d.m. , “A review paper on black hole attack and comparison of different black hole attack techniques”. In: International journal of cryptography and security, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-22-26.
3) Praveen Joshi, “Security issues in routing protocols in Manets at network layer”. In: WCIT-2010.
4) Sheenu Sharma, Roopam Gupta, “ Simulation Study of Blackhole Attack in the Mobile Ad Hoc Networks ” .In: Journal of Engineering Science and Technology, 2009, Vol. 4, No. 2, 243 – 250.
5) Ming-Yang Su, Kun-Lin Chiang, Wei-Cheng Liao, “ Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks” .In: Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications, 2010, pp.162-167.
6) Shashi Gurung and Siddhartha Chauhan, “A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET”. In: Wireless Netw DOI 10.1007/s11276-017-1622-y.
7) Sina Shahabi, Mahdieh Ghazvini and Mehdi Bakhtiarian , “A modified algorithm to Improve security and performance of AODV protocol against Black hole attack” .In: Wireless Netw (2016) 22:1505–1511,DOI 10.1007/s11276-015-1032-y.
8) Al-Shurman M., Yoo S. and Park S., "Blackhole Attack in Mobile Ad Hoc Networks" ,In: ACM Southeast Regional Conference, pp. 96-97,2004.
9) Sen, J.; Koilakonda, S.; Ukil, A., "A Mechanism for Detecting of Cooperative Blackhole Attack in Mobile Ad Hoc Networks”, In: Second International Conference on Intelligent Systems, Modelling and Simulation (ISMS), pp.338-343, Jan. 2011.
10) Jaydip Sen, Sripad Koilakonda, Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", In: Second International Conference on Intelligent Systems, Modelling and Simulation. IEEE – 2011.