International Journal of Future Generation Communication and Networking
Vol. 8, No. 4 (2015), pp. 287-294
http://dx.doi.org/10.14257/ijfgcn.2015.8.4.28

A Review: Black Hole & Gray Hole Attack in MANET

Sweta Dixit, Krishna Kumar Joshi and Neelam Joshi

Dept. of Computer science & Engg.
Maharana Pratap College of Technology, Gwalior, India
swetadixit64@gmail.com, Krishnakjoshi@gmail.com,
Neelam.khemariya@gmail.com

Abstract

In past few years, mobile ad hoc network has gaining more attention of researchers. Mobile Adhoc Network (MANET) are most widely used all over the world, due to its ability to communicate each other without the use of any fixed network. It applications used in military network, disaster relief operations and also in commercial environments. Due to open, dynamic and infrastructure-less nature, the ad hoc networks are vulnerable to various attacks. The black hole and grayhole attack is one of them in MANET. Security is an necessary requirement in MANET. Without any proper security solution, the malicious node in the network will act as a normal node which causes eaves dropping and selective forwarding attack generally known as Gray Hole attack. In this paper we survey on MANET applications, routing protocols, different types of attacks and also the review of researchers.

Keywords*: Black hole, gray hole, AODV, RREQ, RREP*

1. Introduction

Ad-hoc in Latin means specifically" for this purpose ". Unlike the surviving static infrastructure of mobile devices MANETS (mobile ad-hoc network) is an infrastructure less, autonomous and dynamic in nature. Links are constantly made broken in arbitrarily fashion that means each node or router is generally free to move anywhere independently in the network in any direction and in this ways connects to other devices frequently. Each node must forward traffic unless it is of its own use. The basic difficulty in building a MANET is equipping each device to continuously maintain the information required to properly control congestion. MANET can work by itself or by connecting to Interest. Unlike the mesh network which is a centralized control. MANETS consist of a peer-to-peer, self –healing and self –forming network [1]

2. Manet Routing Protocols

In MANET nodes can move rapidly from one place to another. So the path formed by a source may not exist after a short span of time if any intermediate node moves from one network to another. Routing in MANET has been a very challenging task due to its very rapidly changing topology between nodes. Routing protocols are broadly classified into three categories:

a) ON DEMAND or Reactive Protocols

In this protocol nodes find their routes only when they need. These protocols first initiate route discovery and roué maintenance for discovery route it make use of route request (RREQ) and route reply (RREP) .Some of the on demand routing protocols are DSR, AODV and TORA .

ISSN: 2233-7857 IJFGCN

b) TABLE DRIVEN or Proactive protocols

These protocols constantly maintain the network topology. In a network every node contains the information of the neighbors. Unlike on demand routing in this protocol information is stored in different tables and these tables are updated periodically according to the changes in the network topologies. Some of the table driven routing protocols are DSDV, DBF, GSR, WRP and ZRP.

c) HYBRID protocols

It is the combination of proactive and reactive protocols is a Hybrid protocols. These protocols make use of distance-vector for more precise metrics to establish the best paths to destination networks. The hybrid routing protocol is CBR.[2]

3. Applications of MANET

1) Tactical networks :

It can generally be used in military communication and operations and also in automated battlefields.

2) Education :

In virtual classroom,ad-hoc communication during conferences and lectures, in universities and lecture settings.

3) Emergency services :

In search and rescue operations, disaster discovery, replacement of fixed infrastructure in case of environmental disasters, policing and fire- fighting, to support doctors in the hospitals.

4) *Sensor networks* : home applications ,BAN

5) *Coverage extension*: Extending cellular networks

6) Commercial and civilian environment:

E-commerce, Business, Networks of visitors at airport

7) Home and enterprise networking :

Conferences,meetings ,Personal area networks(PAN),Personal networks (PN)

4. Security Requirements in MANET

a. Availability:

It is important to ensure that the data should be accessible to the authorized user at any time. Some types of attacks makes the authorized users not to use the data.

b. Data confidentiality:

Its means to protest or hide information to the unauthorized users. It is the most important aspect of security but it is the most which is attacked mostly. Cryptography and encryption are the techniques used to ensure confidentiality.

c. Integrity:

It is to ensure that the data is secure and unchanged of the original information.

d. Non-repudiation:

It is to ensure that the one cannot deny the authentication of digital signature to the message or data it has sent or originated.

5. Security Attacks

There are four types of Security attacks :

a) Active attacks
b) Passive attacks
c) External attacks
d) Internal attacks

a) Active attack

In this type of attack an attacker generally tries to break the secured network. It generally uses worms, viruses, stealth, or Trojan horses. Active attack usually tries to break protection features, to introduce bogus code, and to steal or change information.

b) Passive attack

This looks for the unencrypted traffic and deploys for clear-text passwords and important information that can be used in other types of attacks. This type of attack generally includes congestion analysis, monitoring of unprotected sending or receiving of information, decrypting weakly encrypted congestion, and obtaining authentication information such as passwords. It makes the attacker to see the future actions. Passive attacks result in the access of data information or data files to an intruder without the knowledge of the user.

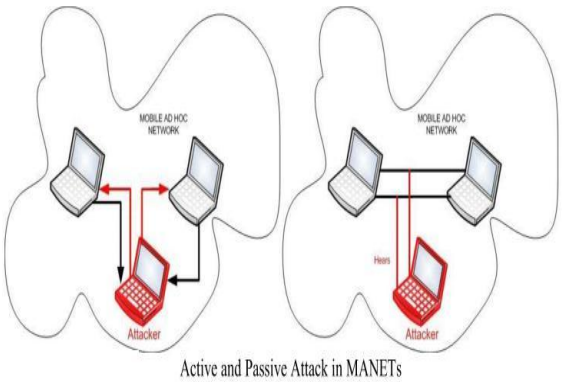

Figure 1. Active and Passive Attack

c) External attack

Generally external attacks are done by outsider without taking assistance from the insider or authorized user. Anyone in experienced attacker, a malicious and experienced user, a group of malicious organization can do such attacks .Their is generally a specific plan or tools for attacking .The most important way involved in such techniques is to scan and gather information.

d) *Internal attacks*

An insider attack or internal attack involves someone from the inside, such as a disaffected employee, attacking the network. Internal attacks can be malicious or non-malicious. Malicious insiders purposely eavesdrop, steal, or damage the data information or data files; use information in a fraudulent manner; or deny access to other valid users. No malicious attack generally comes from the lack of knowledge, carelessness.

6. Types of Attacks

A. Black hole attack:

[3]In the black hole attack in MANET mainly the routing protocol is used to advertise itself to the other intermediate nodes as it is having the shortest route as having the destination whose packets it want to intercept by the attacker. An attacker constantly monitors the request for route in a flooding based network. And when it receives the request from the node who it wants to intercept it pretends and reply itself as having the shortest route to the destination. And when the reply of the malicious node reaches to the initiating node before the actual node would reply, a fake route is already created by the malicious node. And from the time the malicious node able to put itself in between the source and destination node it can do anything with the arriving packets from either side. Either it can drop packets to do a denial-of –service attack or it put its place to first step in the man-in the-middle attack.

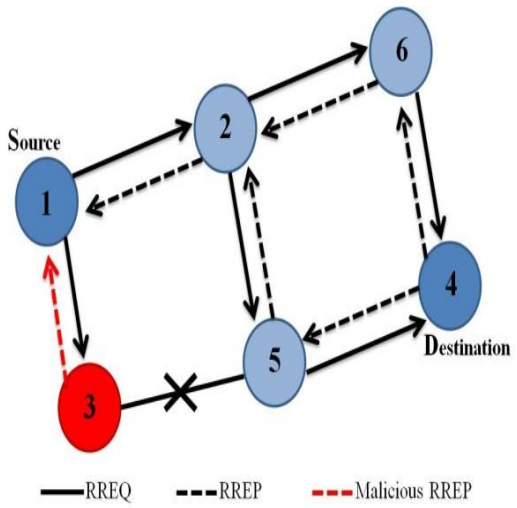

Figure 2. Black Hole Attack

For example in the Fig:2 node
(1) i.e the source node wants to send packets to the node
(2) .i.e the destination node but the node
(3) In between the route is the malicious node will advertise itself as having the shortest route to node
(4) When once it is able to insert in between source and destination it can do anything with the packets.

a. AODV (Ad Hoc Distance Vector) Routing Protocol

AODV is generally an ad-hoc on demand or reactive distance vector routing protocol that establishes route to the destination when it is desired by the source node. It maintains this route as and when needed by the source node. It provides quick adaptation to dynamic link conditions, less processing, memory overhead, less network utilization, and determines unicast routes to destinations within the ad hoc network. In order to communicate among the mobile nodes, Route Discovery is used. [4]

b. Route Discovery-

[3]When any node in network send a packet to destination and that particular path does not find in its routing table for the same destination, then that source will initiate route discovery process. Source now broadcast its RRRQ (route request) packet to neighbors .In

this technique source node searches the destination by a TTL (time to live) value. if any reply do not come in TTL time then it incremented by a value .It will be repeated continuously until the threshold value is reached .If any intermediate node forwards the RREQ ,so the address of the node from which first packet of the broadcast is received, thereby it establishes a reverse path. RREP is unicast to the route towards the source from which it came.In this way when the RREP reaches to the source node, a secure path is established between source and destination node.

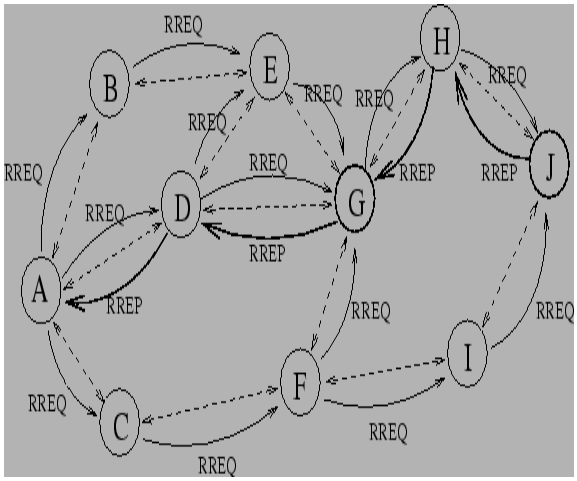

Figure 3. AODV Algorithm

B. Gray Hole attack :

A special case [5] in the black hole attack is the grey hole attack .It can be seen as the variation in the basic black hole attack in which the packets are dropped selectively. Generally these selectively forward attacks are mainly of two kinds

- Forwarding all TCP packets but dropping all UDP packets.
- But when 50% of the packets are dropped or dropping them with a probabilistic distribution then it seem to disrupt the network and the security measures are unable to detect it.

In the gray -hole [5] attack an attack can ignore packets from a single source or IP address or from a range of IP addresses and forwards the remaining data packets.

The nodes in the grey hole are very effective. In grey hole each node in the network records the activities in the routing table and maintain a table about all the neighbor nodes to route a data packet to the final or desired node, and when source node wants to route a packet to the destination node, it checks for the routing table if a specific route is present in it or not. Otherwise it uses route discovery.

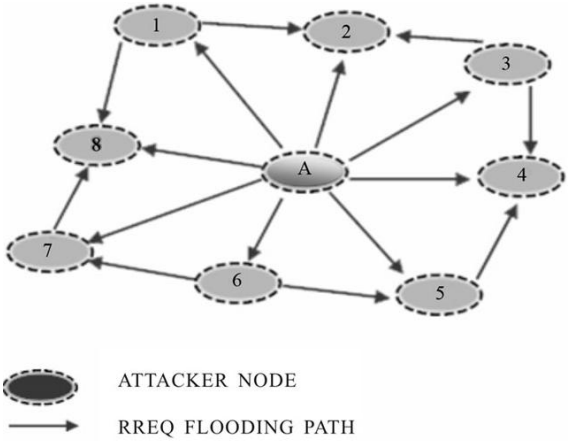

Figure 4. Gray Hole

C. Worm Hole attack:

Basically in the wormhole attack in MANET two attackers are connected by a high speed off-channel link which is known as the wormhole link. And this link can be of any form, it can be "wired" link or it can be a wireless transmission. Once the link is established of wormhole then the data is recorded by the adversary and then it forward the data to each other and then by using this wormhole link it replays the data packets to the other end .It then replays with the valid network messages at improper places, this worm hole attacker make the far away nodes believe that it is the nearest neighbor and forcefully come in between the communication process of all the affected nodes.[6]

D. Byzantine attack:

A compromised intermediate node may works alone, or can work in a group of compromised intermediate nodes works in collusion and results into the byzantine attack. In this the attacker node creates routing loops , forwards packets by using paths which are non-optimal or may selectively dropping of the data packets which results in the degradation of the performance of the network.[7]

E. Flooding attack:

In some cases it is possible that the nodes of the network are not present and is having either very low or no protection against tampering .And thus in this case ad-hoc have no choice but have to compromise. The most common attack in this case is of denial of service (DOS) attack mainly introduced by the intruders or the compromised nodes.[5]

7. Types of Attacks

A. Time-based Threshold Detection Scheme

In this paper author uses a timer to set in the" Rimer Expired Table". When it receives the first request after that it sends request to the other nodes in the network, a timer is used to collect remaining request from the other nodes. This Rimer table will store the sequence number of packets and the receiving time in a Collect Route Reply Table (CRRT), counting the timeout value based on the arriving time of the first RREQ, analyze the route offers is valid or malicious based on the above threshold value.[11]

Honey-pot based detection scheme:

In this paper author detected a strategy by applying mobile identifying anomaly activities of an attacker, it is possible to detect a possible honey-pot agents which utilize their topological knowledge and detect such malicious node advertises themselves as having the shortest route to the destination route. They are implemented as roaming software agents that keeps on travelling in the network and attract attackers by sending route request advertisements. We get valuable information about the attacker on attacker's strategy from the intrusion logs gathered at a given honey-pot. The drawbacks of the proposed algorithm is for WMN not for mobile ad-hoc network as it is proactive mechanism, it will generate lots of congestion in the network as the honey-pot lacks from the centralized control of authority.[10]

Detection Using Promiscuous Mode

In this paper author proposed a method which uses promiscuous mode of the node. This promiscuous mode allows and in the network to intercept and read each network packet that arrives. Promiscuous mode generally means that if a node A is within the range of node B, even if it is not involve directly ,it can overhear the communication by and through B .An alarm message is sent to the network about the malicious node to isolate it. In this the simulation results shows that approach is able to secure the AODV protocol from black hole and is successful in achieving the increased throughput and on the other head routing overhead to the minimal. [9]

Prevention of Black Hole Attack in MANET Network using Anomaly Detection:

In this paper author proposed techniques in uses host-based IDS scheme. It is generally assumed that all activities of a system can be monitored and anomaly activities of an intruder or attacker can be identified from trusted or valid activities. Therefore, by intrusion and isolate the adversary. To do so an anomaly detection system needs to collect or provided with a pre-collected set of anomaly data, called audit data. Once audit data is collected and is given to the anomaly detection system, the anomaly detection system is able to compare every activity of a host with the audit data on a fly. If any of the activity of a host matches with the activities presented in the audit data, the anomaly detection system keeps the other nodes isolated from particular anomaly node by forbidding further interaction. It do not trust on peer nodes. [13]

An Efficient Algorithm for Detection of Black Hole Attack in AODV based MANETs:

In this paper author proposes to give an efficient approach for the detection and removal of black hole attack .This algorithm can detect both single and co-operative black hole. The most attractive thing about this approach is that it not only detects non-idle nodes, but can also detect the idle ones also. By using graphs such as throughput graph, packet delivery ration graph and average end-to –end delay graph are drawn to find the number of attackers present.[12]

Analysis and Prevention of Effects of Gray Hole Attacks on Routing Protocol in Mobile ad-hoc Networks:

In this paper author proposes to use Intrusion detection systems (IDs) to detect malicious nodes or misbehaving node in the network and also the other misbehaving node in the network of misbehaving node. In this paper author analyzed the effect of gray hole in an AODV network in NS-2. In this simulation author analyzed that the normal AODV had very less data loss i.e. only 41.6% but with the gray hole it is increased to 91.04%.

But with the solution given by the author in IDAODV is data loss is again decreased to 85% .And it is also observed that as the speed varied the behavior of AODV remains normal but the malicious node increases the e-delay too much which is controlled in the solution.[11]

8. Conclusion

In this paper, we present a survey on black hole and Grayhole attack in MANET. Black hole and Grayhole attack are the serious attacks in MANET. Black hole is an attack where a malicious node does not forward the data packets to the destination and grayhole attack is a special variation of black hole attack which is difficult to detect. Many researchers proposed various methods and techniques to prevent and detect the black hole and grayhole problem. In this survey paper, present various techniques to resolve attacks in MANET.

References

[1] N. Modi, V. Kumar Gupta, I.Rajput, "A Survey Paper On Detection Of Gray-Hole Attack in MANET", International Journal of Computer Science & CommunicationNetworks,vol.4, no. 1, pp.09-12.
[2] B. Patel, "A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, vol. 5, no. 3, **(2014)**, pp. 2816-2818.
[3] S. Jain, J. Singhai, M. Chawla "A Review Paper on Cooperative Blackhole And Grayhole Attacks in Mobile Ad hoc Networks", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) vol.2, no.3, **(2011)**.
[4] V. Shanmuganathan, T. An and M.E., "A Survey on Gray Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), vol.2, no. 6, **(2012)**.
[5] M. Arya and Y. K. Jain "Gary hole attack and prevention in Mobile Adhoc Network", IJCA vol.27, no.10, **(2011)**.
[6] A. P. Rai, V. Srivastava, R. Bhat", Wormhole Attack Detection in Mobile Ad Hoc Networks", International Journal of Engineering and Innovative Technology (IJEIT), vol. 2, no. 2, **(2012)**.
[7] V. Shrivastava, P. Mishra, "A Novel Protection Scheme against Byzantine Attack in Mobile Ad hoc Network" , International Journal of Innovative Research in Computer and Communication Engineering, vol. 2, no. 4, **(2014)**.
[8] N. S. Chouhan, S. Yadav, "Flooding Attacks Prevention in MANET", International Journal of Computer Technology and Electronics Engineering (IJCTEE), vol. 1, no. 3.
[9] N. P. John , A. Thomas, "Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review", International Journal of Scientific and Research Publications, vol. 2, no. 9, **(2012)**.
[10] L. Tamil Selven and N. Sankara, "Prevention of Black hole Attack in MANET", International Conference on wireless Broadband and Ultra Wideband Communications, **(2007)**.
[11] M.-Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Elsevier, Computer Communications, vol. 34, **(2011)**, pp. 107–117.
[12] P. K. Singh, G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET" IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, **(2012)**.
[13] L. Shrivastava, B.K. Chaurasia, GS Tomar, S.S. Bhadoria, "Secure Congestion Adaptive Routing using Group Signature Scheme", Springer's Trans. on Comput. Sci., vol.17, pp. 101–115, 2013.
[14] L. Shrivastava, G.S. Tomar & Sarita Bhadoria, "Secure and Congestion Adaptive Mechanism with Load Balancing for MANETs", International Journal of Communication Systems and Networks, vol.1 no.1, pp. 41-51, **(2012)**.
[15] Y. F. Alem and Z. C. Xuan, "Preventing Black hole Attack in Mobile Ad-hoc Networks using Anomaly Detection", IEEE International Conference, **(2010)**.

