Gray Hole Attack on Manet: A Survey

Rohit Katoch, Anuj Gupta
Department of Computer Science Engineering
SRI SAI UNIVERSTY PALAMPUR

***Abstract*-In recent years mobile ad hoc networks have become very popular and lots of research is being done on different aspects of MANET. Mobile Ad Hoc Networks (MANET)-a system of mobile nodes (laptops, sensors, etc.) interfacing without the assistance of infrastructure (access points, bridges, etc.). There are different aspects which are taken for research like routing, synchronization, power consumption, bandwidth considerations etc. This paper concentrates on routing techniques which is the most challenging issue due to the dynamic topology of ad hoc networks. There are different routing protocols proposed for MANETs which makes it quite difficult to determine which protocol is suitable for different network conditions .This paper provides an overview of different attack on routing protocols proposed in literature and also provides a comparison between them.**

***Keywords*-MANETs, Routing Protocol, Performance, Dynamic Topology, Synchronization.**

INTRODUCTION

Wireless networks provide connection flexibility between users in different places. Moreover, the network can be extended to any place or building without the need for a wired connection. Wireless networks are classified into two categories; Infrastructure networks and Ad Hoc networks [2]

1.1. Infrastructure networks

An Access Point (AP) represents a central coordinator for all nodes. Any node can be joining the network through AP. In addition, AP organizes the connection between the Basic Set Services (BSSs) so that the route is ready when it is needed. However, one drawback of using an infrastructure network is the large overhead of maintaining the routing tables. Infrastructure network as shown in Figure 1.

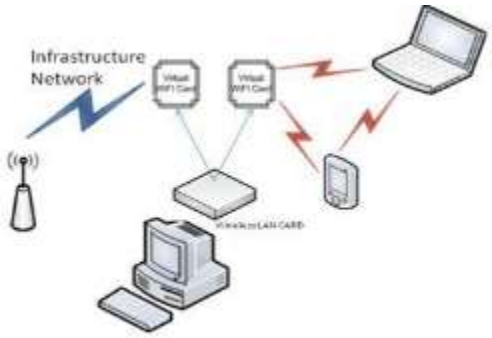

Fig 1: Infrastructure Network

1.2. Ad Hoc networks

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as Routers in wired networks or access points in managed (infrastructure) wireless networks [1]. Ad Hoc networks do not have a certain topology or a central coordination point. Therefore, sending and receiving packets are more complicated than infrastructure networks.

Fig 2: Infrastructure Less Network

2. MANET: Mobile Ad-hoc Network (MANET) is collection of wireless nodes that do not depend on already existing infrastructure so there is no concept of base station or access point. In MANETs, due to availability of mobility in nodes and deficiency of centralized entity, the network topology changes repeatedly and erratically [1]. In MANETs each node works as router for packet forwarding whereas in wired network router performs routing table. It is multi-hop wireless network because different sets of nodes want to establish a network & it is not compulsory that each node is within the transmission range as it might be in out of range, so another set of nodes are used to connect the out of range nodes. Therefore whenever one node sends data to another node, a set of nodes may be used in between, where data is send in different hop that's why they are also called multi-hop, wireless & distributed network [2].

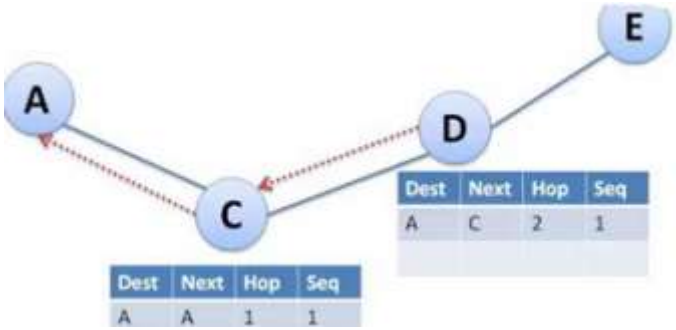

Figure 3. Hop to hop data transfer in MANET

Figure 3 depicts a multi-hop data transfer in a MANET. In the ad-hoc network nodes act as routers as well as hosts therefore node may forward packets as well as run user applications [3, 4].The aim of MANET is to establish an accurate and efficient route between nodes such that any messages are delivered on time [5]. Nowadays, with the immense growth in wireless network applications like PDAs and cell phones, various researches are being done to improve the network services and performance. So there are various challenging design issues in wireless Ad Hoc networks [6].

3. CLASSIFICATION OF ROUTING PROTOCOLS

Routing protocols define a set of rules which helps to transfer data or message packets from source to destination in a network [6]. In MANET, there are different types of routing protocols each of them is applied according to the network situations. Figure 2 shows the classification of the routing protocols according to network structure in MANETs.

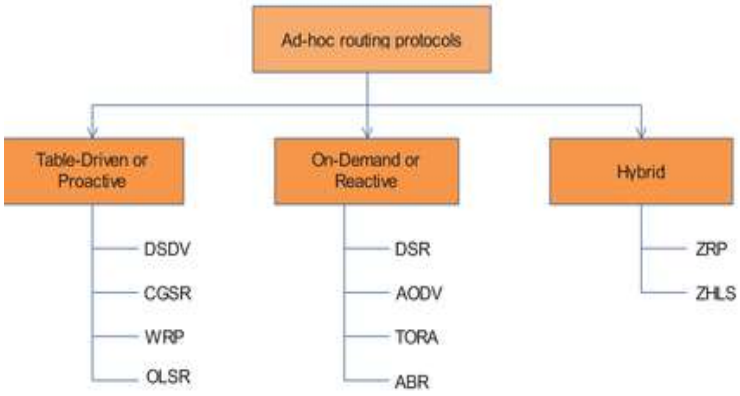

Fig 4: Manet Routing Protocol

3.1. Proactive routing protocols It is also known as Table driven protocols since they maintain the routing information even before it is needed. In proactive routing protocols each and every node maintained a routing table in the network and update this periodic table through periodic exchange of control massage between nodes because every node should have instant information about any topology change in the networks. In proactive routing protocol route to every destination already present so there is no initial delay to start sending data. In table-driven or proactive protocols, the nodes maintain an active list of routes to every other node in the network in a routing table. The tables are periodically updated by broadcasting information to other nodes in the network. Thus, they are an extension to the wired network routing protocols such as the Routing Internet Protocol (RIP). Many proactive routing protocols have been proposed, for e.g. Destination Sequence Distance Vector (DSDV), Optimized Linked State Routing (OLSR).

3.2. Reactive protocols It is also known as On demand routing protocol. In reactive routing protocol routes are developed when it needed so update of routing table in reactive routing protocol is not required so frequently and there is no need of maintain routes for all nodes in the networks. In reactive routing protocol for new destination every node required a route so they have to wait until new root is discovered. Reactive routing protocols take a lazy approach to routing. They do not maintain or constantly update their route tables with the latest route topology. This type of routing creates routes only when desired by the source node. The source node initiates a process called route discovery when it requires a route to the destination. This process is completed when a route is found or when all the possible routes are examined. The process of route maintenance is carried out to maintain the established routes until either the destination becomes unavailable or when the route is no longer required. Several reactive protocols have been proposed such as Dynamic Source Routing Protocol (DSR), Ad hoc On-demand Distance Vector (AODV), Temporary Ordered Routing Algorithm (TORA).

3.3. Hybrid routing protocols This type of protocol is combination of table-driven (Proactive) and on demand (Reactive) routing protocol i.e. it contains features of proactive as well as reactive protocol. It inherits the advantages of proactive and reactive routing protocols. Initially hybrid routing protocol developed the routing through proactive routes and then reactive flooding satisfy the demand of additional activated nodes Several hybrids routing protocols have been proposed such as Zone Routing Protocol (ZRP), Zone-based Hierarchical Link State (ZHLS) and so on, but the most popular protocol is ZRP [3].

4. PROPERTIES OF AD-HOC ROUTING PROTOCOLS

- Distributed Operation: The protocol should of course be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The difference is that nodes in an Ad-hoc network can enter or leave the network very easily and because of mobility the network can be partitioned.
- Loop free: To improve the overall performance, we want the routing protocol to guarantee that the routes supplied are loop free. This avoids any waste of bandwidth or CPU consumption.

- Demand based Operation: To minimize the control overhead in the network and thus not wasting network resources more than necessary, the protocol should be reactive. This means that the protocol should only react when needed and that the protocol should not periodically broadcast control information.
- Unidirectional Link Support: The radio environment can cause the formation of unidirectional links. Utilization of these links and not only bi-directional links improves the routing protocol performance.
- Security: The radio environment is especially vulnerable to impersonation attacks, so to ensure the wanted behavior from the routing protocol, we need some sort of preventive security measures. Authentication and encryption is probably the way to go and the problem here lies within distributing keys among the nodes in the ad-hoc network. This can be uses tunneling to transport all packets.
- Power Conservation: The nodes in an ad-hoc network can be laptops and then clients, such as PDAs that are very limited in battery power and therefore uses some sort of stand- by mode to save power. It is therefore important that the routing protocol has support for that sleep – modes.
- Multiple Routes: To reduce the number of reactions to topological changes and congestion multiple routes could be used .if one route has become invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from insulating another route discovery procedure.
- Quality of Service Support: Some sort of quality of service support is probably necessary to incorporate into the routing protocol. This has a lot to do with what these networks will be used for. It could for instance be real- time traffic support.

5. Security Threats

The attacks can be classified as passive attacks or active attacks

1) Passive attacks: In a passive attack an unauthorized node continuously monitors the network and willing to get the information. In this the communications is not interrupted. There is no direct damage to the network. The attacker can read the information which can be used for future harmful attacks. Examples of passive attacks are eavesdropping and traffic analysis.

- Eavesdropping Attacks: It is also known as disclosure attack. These are passive attacks by external or internal• nodes. The attacker gathers information e.g. Private key, public key or even passwords of the nodes and analyzes broadcast messages to reveal some useful information about the network.
- Traffic Analysis: In this the network traffic and messages are examined to find out information. It can be• performed on encrypted messages. In this the attackers use techniques such as traffic rate analysis, and time correlation monitoring etc.

2) Active Attacks: These attacks cause unauthorized state changes in the network such as denial of service, modification of packets etc. These attacks are generally launched by users or nodes with authorization to operate within the network. The active attacks can be classified into four groups: dropping, modification, fabrication, and timing attacks. An attack can be classified into more than one group.

- Dropping Attacks: It is a kind of denial of service attack and most difficult one to detect and prevent. Malicious or selfish nodes drop all packets that are not destined for them. While malicious nodes aim to disrupt the network connection, selfish nodes aim to preserve their resources. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point. It might also reduce the network performance by causing data packets to be retransmitted, new routes to the destination to be discovered, and the like.
- Modification Attacks: Insider attackers after reading the data in the packet modify it to disrupt the network. For example modifying the hop-count value of a routing packet to a smaller value. By decreasing the hop count value a malicious node can attract more network communication.
- Black Hole Attack: The black hole attack is a kind of denial of service attack. In this attack, the malicious node sends false route replies to the source node claiming to have the shortest path to the destination node. When the source node established the route through the malicious node, the malicious node then misuse or discards any or all of the network traffic being routed through it.
- Gray Hole attack: It is a special type of black hole attack in which the attacking node first agrees to forward packets and then fails to do so.

In this the selected packets are dropped. Gray Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface.

- Wormhole attack: It is also known as tunneling attack. In this an attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

3) Other Attacks:

- Timing Attacks: In this an attacker attracts other nodes by causing itself to appear closer to those nodes than it really is. DoS attacks, rushing attacks, and hello flood attacks use this technique.
- Sleep Deprivation: In sleep deprivation attack, the attacker interacts with the target node in a manner that appears legitimate but the resources of the nodes of the network are consumed by constantly keeping them engaged in routing decisions. The attacker node continually requests for either existing or non-existing destinations, forcing the neighboring nodes to process and forward these packets and therefore consume batteries and network bandwidth obstructing the normal operation of the network.
- Impersonation Attack: These are also called spoofing attacks. The attacker assumes the identity of another node in the network, thus receiving messages directed to the node it fakes. The attacker nodes impersonates a legitimate node and joins the network undetectable, sends false routing information, masked as some other trusted node.
- Routing Table Poisoning Attack: Different routing protocols maintain tables which hold information regarding routes of the network. In poisoning attacks, the attacker node generates and sends fictitious traffic, or mutates legitimate messages from other nodes, in order to create false entries in the tables of the participating nodes. Another possibility is to inject a RREQ packet with a high sequence number. This causes all other legitimate RREQ packets with lower sequence numbers to be deleted. Routing table poisoning attacks can result in selection of non-optimal routes, creation of routing loops, bottlenecks and even partitioning certain parts of the network.
- Location Disclosure Attack: In this attack, the privacy requirements of an ad hoc network are compromised. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, and the structure of the network.
- Rushing Attack: In this attack the attacker (initiator) node initiates a Route Discovery for the target node. If each neighbor of the target node receives these RREQ messages first, then the route discovered by this route discovery process will include a hop through the attacker. Then the neighbor forwards that REQUEST to the target node. When non-attacking REQUESTs arrive later at these nodes, they will discard those legitimate REQUESTs. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

6. GRAY HOLE ATTACK

Since MANET is multihop in nature, it sturdily depends upon the cooperation among the nodes in the network [7]. The guarantee of cooperation among nodes is required. In recent times we have seen a variety of attacks have been identified and detected in the network. To provide a secure communication in the network we need to face the security challenges [9]. There are two major categories where we have to consider always in the security attacks, they are Passive attacks and Active attacks. A passive attack won't interrupt the normal operation of MANET, while data have been exchanged from the network. The solely nature of passive attack is to identify the data exchanged in the network The attacker snoops the data exchanged in the network without altering it. Here the requirements of confidentially gets violated. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, thereby making it impossible for the attacker to get useful information from the data overhead. An Active attack always tries to modify the normal operation of MANET, which means the interruption have been made in the network, such as doing data interruption, modification, deletion and fabrication. Active attacks can be internal or external. The information which is routing through -the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also do the task of route request though it is not authenticated node so the other node rejecting its request due to these route requests the bandwidth is consumed and network is

jammed Some of the security threats in the networks are Interruption, Interception and Modification. In External attacks the attacker aims to cause congestion in the network which can be done by propagating fake routing information or to disturb the nodes from providing services [8]. The attacker always disrupts the nodes to avail the services. In internal attack, the attacker needs to gain the access to participate in the network activities. Here the attacker comes with some malicious impersonation to get access from network as a new node.

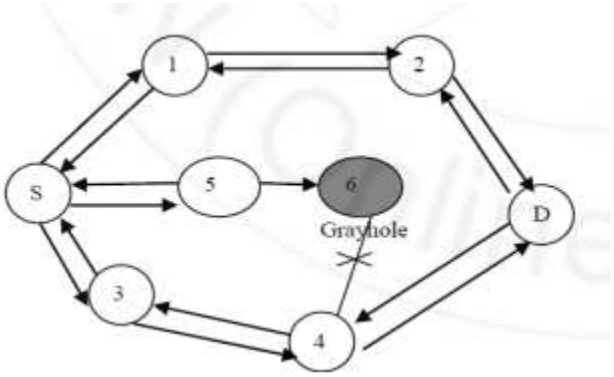

Fig 5: Gray Hole Attack

A variation of black hole attack is the Gray Hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are

(a) Dropping all UDP packets while forwarding TCP packets

(b) Dropping 50% of the packets or dropping them with a probabilistic distribution.

These are the attacks that seek to disrupt the network without being detected by the security measures. Gray Hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node. So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node [11]. If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbour; by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source [12]. A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination. The Gray Hole attack has two phases:

Phase 1: A malicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intention of interrupting packets of spurious route.

Phase 2: In this phase, the nodes has been dropped the interrupted packets with a certain probability and the detection of Gray Hole attack is a difficult process. Normally in the Gray Hole attacks the attacker behaves maliciously for the time until the packets are dropped and then switch to their normal behavior [10]. Both normal node and attacker are same. Due to this behavior it is very hard to find out in the network to figure out such kind of attack. The other name for Gray Hole attack is node misbehaving attack

7. CONCLUSION AND FUTURE WORK

A Gray Hole attack is one of the serious security problems in MANETs. It is an attack where a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. In this paper a survey on gray hole attacks in MANETs is presented. The effects of Gray Holes in ad hoc networks is still considered to be a challenging task.

References

[1] Elizabeth Royer, and Chai-Keong Toh, (1999), "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp 46-55.

[2] Robinpreet Kaur and Mritunjay Kumar Rai, (2012), "A Novel Review on Routing Protocols in MANETs", Undergraduate Academic Research Journal (UARJ), vol. 1, Issue-1, ISSN : 2278 – 1129.

[3] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, M. Degermark, (1999), "Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks", ACM Proceedings of the 5 th annual International Conference on Mobile Computing and Networking, pp.195-206, isbn - 58113-142-9.

[4] Prabhakara Reddy, E. Suresh Babu, and M. L. Ravi Chandra, (2012) "A comprehensive study of Routing protocols in Mobile Ad hoc Networks", Research Survey International Journal of Advanced Information Science and Technology (IJAIST), ISSN: 2319:2682, Vol.7, No.7.

[5] Elizabeth M. Royer and Chai-Keong Toh, (1999) "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, vol. 6, no. 2.

[6] Dr.S.S.Dhenakaran and A.Parvathavarthini, (2013) "An Overview of Routing Protocols in Mobile Ad-Hoc Network", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, " Mitigating Routing Misbehavior in Mobile Ad Hoc Networks." Proceedings of the 6th annual international conference on Mobile Computing and Networking (MOBICOM), Boston, Massachusetts, United States, 2000, 255-265.

[8] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. "Prevention of cooperative black hole attack in wireless ad hoc networks." In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003

[9] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[10] B. Sun; Y. Guan; J. Chen; U.W. Pooch, Detecting Black-hole Attack in Mobile Ad Hoc Networks[C]; 5th European Personal Mobile Communications Conference, 2003, 490-495.

[11] A. Patcha; A. Mishra; Collaborative security architecture for black hole attack prevention in mobile ad hoc networks[C]; Radio and Wireless Conference, 2003, 75-78.

[12] D.M. Shila; T. Anjali; "Defending selective forwarding attacks in WMNs", IEEE International Conference on Electro/InformationTechnology, 2008, 96-101

