A Study of Black Hole Attack and its Recent Prevention Techniques in MANET

Pandi Selvam Raman
Assistant Professor & Head
Department of CS & IT
Ananda College, Devakottai

ABSTRACT

A mobile ad hoc network (MANETs) is a self-organizing system of mobile nodes that communicate with each other via wireless links with no fixed infrastructure or centralized administration such as base station or access points. MANETs nodes can communicate directly if they are in each other transmission range; else the relay nodes are forwarding the packets to neighbors or receivers. This connectivity between multiple nodes is furnished by network layer. Due to the MANETs open wireless medium security is one of the indispensable roles to resist attacks such as Rushing, Black Hole, and Worm Hole etc. Among these Black Hole attack is one of the major attack and this detection and prevention is still considered as a challenging task in ad hoc networks. Therefore this paper exposes a study of Black Hole attack and its various prevention techniques that are explored recently.

Keywords

MANETs, Routing, Security, Attacks strategies, Black hole attack.

1. INTRODUCTION

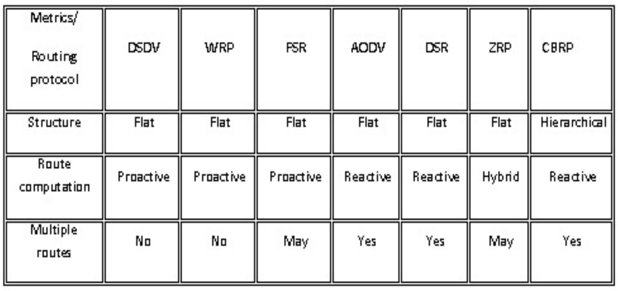
A MANET is a self-configuring (autonomous) system of mobile hosts connected by wireless links. The nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably [1]. An ad hoc network can be set up anywhere without any assistance of external infrastructure like wires or base stations. Networks are formed on-the-fly i.e. devices can leave and join the network during its lifetime. In general, MANET can operate in two modes namely peer-to-peer (communicate directly within their radio range) and multi-hop (communicate via intermediate nodes outside their radio range) [2]. MANETs are used at business meetings and conferences to confidentially exchange data, at the library to access the Internet with a laptop, and at hospitals to transfer confidential data from a medical device to a doctor's PDA etc.

Routing is the process of exchanging information from one station to the other stations of the network [3]. It may divide into different aspects. Route construction (topology) based it further divided into three types namely i. Tree based ii. Mesh based and iii. Hybrid. The tree based routing scheme has single path between the source and receiver. In the mesh based approach multiple redundant paths connect the source and the destination. The hybrid approach attempt has been made to combine both the mesh-based and the tree-based approaches.

Based on routing update mechanism protocols are classified as table driven (proactive or pre-computed routing), on-demand (reactive routing) or hybrid. In proactive routing, nodes are continuously evaluate the routes to all reachable nodes and attempts to maintain up-to-date routing information. In reactive nodes do not maintain routing information if there is no communication. In hybrid, the nodes are balanced which delay and overhead of both proactive and reactive [4].

The structure based routing protocols are classified as flat and hierarchical. In a flat structure, all nodes in a network are at the same level and have the same routing functionality. In hierarchical, nodes are dynamically organized into partitions called clusters [5].

Table 1. Types of Routing Protocols



Metrics/ Routing protocol	DSDV	WRP	FSR	AODV	DSR	ZRP	CBRP
Structure	Flat	Flat	Flat	Flat	Flat	Flat	Hierarchical
Route computation	Proactive	Proactive	Proactive	Reactive	Reactive	Hybrid	Reactive
Multiple routes	No	No	May	Yes	Yes	May	Yes

Security is an essential service for wired and wireless network communications. However, MANETs are much more vulnerable to attack because of its non-trivial challenges such as lack of fixed infrastructure, dynamic topology, link variation and energy constraints. So, each and every node in the network has to prepare for attacks at any point of time. And also as there is no central based controlling identity for the participating nodes; the attacks are much easier to launch in MANET.

Black Hole Attacks are a kind of serious security service where a malicious node advertise itself a shortest path during routing discovery and redirect the data towards malicious node. Malicious node dropped the data or its desired destination instead of original destination.

This paper organized as follows: Section 2 exposes MANETs weaknesses in security system. Section 3 explains about common security principles for MANETs. Section 4 describes attacks classification on different ISO/OSI layers. Section 5 depicts different possible attacks on network layer. Section 6 discusses how the Black Hole attacks have an effect on ad hoc network. A number of recent prevention techniques against black hole attacks are presented in Section 7 followed by conclusions is Section 8.

2. MANET VULNERABILITIES

Generally, Mobile ad hoc network is more vulnerable than wired network. Some of the vulnerabilities of MANET are as follows [6].

- **Open Medium:** Eavesdropping is easier than in wired network.
- **Lack of centralized management:** MANET does not have any centralized infrastructure. This absence makes the sensing of attacks very difficult in highly dynamic mobility.
- **Resource availability:** Resource availability is big issue in MANET. Due to dynamic environment providing security is considerable issue in MANET security system.
- **Scalability:** Due to mobility of nodes, scale of ad-hoc network varying all the time. Hence scalability is a major issue concerning security.
- **Dynamic topology:** Unpredictable changes (nodes enter and leave) of nodes may disturb the trust relationship among nodes. This dynamic behavior could be better protected with adaptive and distributed security mechanisms.
- **Limited power supply:** The MANET stations require considering limited power supply that will be the source of several threats. A station for example can behave in a selfish way and does not forward packets.
- **Cooperative Algorithms:** The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.

These vulnerabilities makes in MANET very difficult to identifying, monitoring and mitigating the different network threats.

3. SECURITY CRITERIA FOR MANET

Communication between nodes takes place over open wireless medium such networks are more prone to attacks and have security threats. Therefore it is important to resist them by preserving the following security principles in MANETs [7].

- **Availability**: All the nodes in the network should be available to perform the services assigned to them. Any kind of attack on this principle resists the legitimate node to perform its operation.
- **Integrity**: This principle maintains the actual data from getting tampered by an intruder. It prevents any kind of modification in the actual data.
- **Confidentiality:** It ensures that the data transferred from source node to destination node should not be disclosed to other nodes.
- **Authentication:** It means that any new node should be authenticated first before entering in the network to ensure its legitimacy.
- **Non-Repudiation:** Any node cannot deny for having sent the data to other nodes.

4. ATTACKS IN MANET

A variety of attacks are possible in MANET. These security attacks can be roughly classified by the following criteria: passive or active, internal or external and different protocol layer related [8].

- **Internal Vs External attacks:** Internal attacks (sometimes called Interior attacks) are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes. External attacks (sometimes called Exterior attacks) are carried out by nodes that do not belong to the network. It causes congestion sends false routing information or causes unavailability of services. External attacks can classify into two categories like active and passive attacks.
- **Passive Vs Active attack:** Passive attacks obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET
- **Attacks in Different Protocol Layer:** The attacks may classify on the basis of different protocol layer. On network layer the attackers can absorb network traffic, inject themselves into the path between the source and destination, and thus control the network traffic flow. Such kind of multicast attacks are Rushing attack, Black hole attack, Neighbour attack and Jellyfish attack.

5. NETWORK LAYER ATTACKS ON MANET

In MANETs the different active attacks disrupt the network or gaining the data by attacker. Some of these are [8]:

5.1 Black Hole Attack

An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order reducing the quantity of routing information available to the other nodes. This attacks effects the packet delivery ratio and to reduce the routing information available to the other nodes.

5.2 Rushing Attack

The meaning of Rushing is Sudden. Rushing attack is also called Novel attack or Denial of Service attack. A rushing attacker exploits this duplicate suppression mechanism by quickly forwarding route discovery packets in order to gain access to the forwarding group.

5.3 Neighbour Attack

An attacker, simply forwards the packet without recording its Id in the packet to make two nodes that are not within the communication range of each other believe that they are neighbors (i.e., one-hop away from each other), resulting in a disrupted route.

5.4 Jelly Fish Attack

A jellyfish attacker first needs to intrude into the multicast forwarding group. It then delays data packets unnecessarily for some amount of time before forwarding them. This results in significantly high end-to-end delay and thus degrades the performance of real applications.

6. BLACK HOLE ATTACK

Black hole Attack is a type of Denial of Service Attack. Black hole Attack is a malicious node uses its routing protocol to advertise itself having the shortest path towards destination node. When route is established, then malicious node drops the packets or forwards it to the attacker desired address [9].

In the Black Hole Attack the attacker must create a RREP with Destination sequence greater than the destination sequence of the receiver node. The sender node believes that black hole node and further communicates with this black hole node instead of original destination node. This misbehaving mostly damage nodes interface and hence wasting all resource utilization in addition to losing packets.

Black hole Attacks are classified into two categories [10].

- **Single Black Hole Attack:**

Single Black Hole attack uses only single node acts as malicious node within a zone.

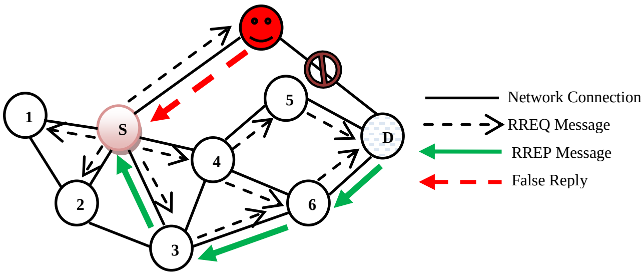


Fig 1: Single Black hole attack

- **Cooperative Black Hole Attack:** Collaborative Black Hole Attack uses multiple nodes in a group act as malicious node to drop all the data packets.

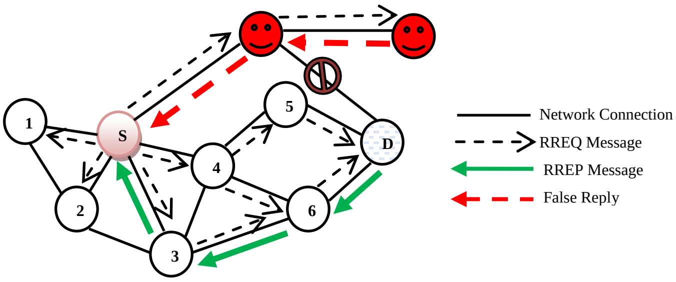


Fig 2: Cooperative Black hole attack

7. RECENT PREVENTION & DETECTION TECHNIQUES

Various researchers have presented various tremendous solutions to prevent and detect the black hole attack in MANET.Here we have discussing some of them.

Ayesha Siddiqua et. al. [11] proposed an algorithm called ***secure knowledge algorithm*** to detect and prevent the black hole attack. In which they have mainly consider to ensure data delivery to receiver node and finds packet drop reasons before declaring node as a black hole node. For this AODV routing protocol is modified to detect and prevent the black hole attack. Black hole nodes are created and analyzed via NS2 and result of simulation shows that the proposed algorithm's delivery ratio with respect to number of malicious node with simulation time.

Miss Bhandare A.S. et. al. [12] proposed an approach against Co-operative Black hole attack in which ***detection and defense mechanism*** is proposed to remove the intruder that bring out black hole attack by taking decision about safe route on basis of Normal V/S Abnormal activity. This anti-prevention system called as Malicious Node Detection for AODV (MDSAODV) and it checks route reply against fake reply. The significant advantage of this method is that decision about unsafe route is taken independently by source and no any additional overhead required. The performance of MANET without and with Black hole, under MDS system is analyzed through NS2 to catch abnormal behavior of malicious node in the network.

Nidhi Choudhary et. al. [13] proposed a new approach called ***timer based detection approach*** to identify and remove the black hole node. In this method each node defines a trust value for its neighbor node and inserts a timer with each data packet, if the trust value decreases below a threshold value for any node then all other nodes put that node in their blacklist table. This is implemented in EXata-cyber and the performance is evaluated in terms of packet delivery ratio while increasing number of nodes and attackers in the network.

Ali Dorri et. al. [14] proposed solution for detection and elimination of cooperative Black hole Attack based on AODV routing protocol. In this approach the source node checks the Next_Hop_Node and Previous_Hop_Node of the RREP in order to check the malicious nodes in the path. By using a ***Data Routing Information table*** the source node can detect malicious nodes and eliminate them from the network. Opnet 14.5 simulator is used for evaluation and results were proven that the proposed approach achievement (malicious node detection) in all situations. Ultimately, this approach decreased the packet overhead and processing time of other nodes by eliminating malicious nodes in the network.

Pooja et. al. [15] proposed solution for Black hole attack detection. ***Hint-based Probabilistic routing protocol*** is used to detect Black hole nodes. Each node hint value computed and to store value at each node's buffer. For simulation, windows based simulator ONE is used with java. The network performance is analyzed under packet delivered, packets dropped, throughput and overhead ratio.

Ashish Kumar Jain et. al. [16] proposed solution for Black hole Attack detection using ***RREP caching Mechanism***. In this method modified the AODV routing protocol by ignoring the first RREP packet reaching the source node. Simulation is done by NS2 and that results shows that this method modified AODV protocol works very well under number of black hole nodes.

Anand A. Aware et. al. [17] proposed solution for Black hole attack prevention/detection using ***hash function*** where first RREP reject from its neighbor and will select the second optimal path. This method continuously monitors the network to identify the malicious node like Black hole, Gray hole, Co-operative black hole Attack.

Kriti Patidar et. al. [18] proposed ***specification based intrusion detection*** technique to detect and prevent black hole attack on AODV. AODV routing behavior and individual nodes monitor the routing behavior of their neighbors for detecting run-time violation of the specifications. The proposed work is simulated by NS2 to show better performance as PDR, throughput and average end-to-end delay.

Vishvas Kshirsagar et. al. [19] proposed method finds the un-trusted (packet dropper) node from the network, if any un-trusted node found, the performance of the network can be improved by eliminate that node using ***Bayes' Theorem and Prior probability.*** This mathematical model secure routing in an independent environment because of it uses heuristic rather than deterministic model.

Gayatri Wahane et. al. [20] proposed Detection of Cooperative Black Hole Attack using ***Crosschecking with TrueLink*** (timing based countermeasure) in AODV. The simulation is conducted to prove the minimum routing overhead, delay and maximum throughput when number of nodes and pause time more.

Ruo Jun Cai et. al.[21] proposed ***Neighborhood Connectivity Based Trust Scheme(NCPTS)*** on Dynamic Source Routing(DSR) to prevent different forms of black hole attack. In which each periodically broadcast Hello message to include two hops topology instead of only direct neighbors. Now when source node receives a route reply from three hops, then it updates its Neighborhood Connectivity Information Table (NCIT) to verify whether the intermediate node1 and it's another intermediate node2 as a direct neighbor and whether node destination can be reached via intermediate node2. If the replied path is not consistent with the NCIT, node Source node will drop this RREP and down the trust level of node intermediate node1. During this way, it can identify both single and colluded active black hole attackers. NS2 is used to simulate the protocol and two types of attacks are studied i) Single Active Black Hole (ABH) and ii) Colluded Active Black Hole (Colluded ABH). Results are proven that the protocol Packet Delivery Ratio while increasing attackers.

Harsh Pratap Singh et. al. [22] proposed a Mechanism for Discovery and Prevention of Co-operative Black hole attack in AODV using ***Broadcast Synchronization***. In this method the First step of solution is to compare the internal clock time with external clock time sequence. The time sequence of internal and external clock if compared with standard threshold time clock, the clock time of normal mobile node is greater than the threshold time initialization time duration and other nodes are blacklisted. Proposed scheme for detection process is sometime failed in the clock synchronization.

Seryvuth Tan et. al. [23] proposed ***Secure Route Discovery*** for the AODV protocol(SRD-AODV). This method requires the source node and the destination node to verify the sequence numbers in the RREQ and RREP messages, respectively, based on defined thresholds same as before establishing a connection with a destination node for sending the data. The improved model simulation results using the Network Simulator 2 (NS2) demonstrate an improvement in the ratio of packet delivery with respect to node mobility on three different environments (small, medium and large) compared to the standard AODV protocol.

Durgesh Kshirsagar et. al. [24] proposed a method to detect and prevent Black hole Attack using by real time monitoring intermediate node by its neighbor node. When a source node transmits some data it will broadcast RREQ message. As soon as the intermediate node receives this packet it will check whether it has a route to the destination or not. If yes generate RREP message towards the source node else, forward the RREQ to its neighbor nodes. Neighbors node maintains two counters Forward count-fcount and Receive Count-rcount used for counting number of forwarded packets and number of received packets respectively. For simulation, NS2 is used and two scenarios (number of nodes and mobility of nodes) are considered to prove the packet delivery ratio and routing overhead.

8. CONCLUSION

Security plays a vital role in every field so as in MANETs. Due to the dynamic nature MANETs are so susceptible to attacks. Active Black hole attack is serious attack where attacker creates a forged route between source and destination to forward or drop the packet. In this paper we have described various network layer attacks like black hole, rushing, neighbor and jelly fish attacks also surveyed some of the existing solutions to black hole attack that have been proposed by various researchers. The survey also gives up-to-date information of all the works that have been done recently.

9. REFERENCES

[1] Ram Ramanathan and Jason Redi, "A Brief Overview of Ad hoc Networks: Challenges and Directions," *IEEE Computer Magazine*, pp.20-22, 2002.

[2] Sheltami, Tarek, "Ad hoc Network Overview," http://www.ccse.kfupm.edu.sa/~tarek, Ad hoc network Technology, 2003.

[3] Changling Liu and Jorg Kaiser, "A Survey of Mobile Ad hoc Network Routing Protocols," Univ. of Ulm, *Tech. Rep.Series*, 2005.

[4] Krishna Gorantala, "Routing Protocols in Mobile Ad hoc Networks," *Master Thesis in Computing Science*, Umea University, Sweden, 2006.

[5] Geetha Jayakumar, and G. Gopinath, "Ad Hoc Mobile Wireless Networks Routing Protocols – A Review," *Journal of Computer Science* 3 (8), pp.574-582, 2007.

[6] Djenouri D., Khelladi L., and Badache N., " A survey of security issues in Mobile Adhoc and Sensor Networks," *IEEE Communications survey and tutorials*, Vol.7, No.4, pp.1-27, 2005.

[7] Umesh Kumar Singh and Shivlal Mewada "An Overview and Study of Security Issues & Challenges in Mobile Ad-hoc Networks (MANET)*" International Journal of Computer Science and Information Security*, Vol. 9, No. 4, April 2011.

[8] Rajinder Singh, Parvinder Singh and Manoj Duhan "An effective implementation of security based algorithmic approach in mobile adhoc networks" *Human-centric Computing and Information Sciences*, Springer 2014.

[9] Ranjan, Rakesh, Nirnemesh Kumar Singh, and Ajay Singh. "Security issues of black hole attacks in MANET." *Computing, Communication & Automation (ICCCA), International Conference on*. IEEE, 2015.

[10] Kishor Jyoti Sarma, Rupam Sharma, Rajdeep Das, "A Survey of Black Hole Attack Detection in Manet." IEEE, 2014

[11] Ayesha Siddiqua, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." *Signal Processing and Communication Engineering Systems (SPACES), 2015 International Conference on*. IEEE, 2015.

[12] Miss Bhandare A. S., and S. B. Patil. "Securing MANET against Co-operative Black Hole Attack and Its Performance Analysis-A Case Study." *Computing Communication Control and Automation (ICCUBEA), International Conference on*. IEEE, 2015.

[13] Nidhi Choudhary, and Lokesh Tharani. "Preventing black hole attack in AODV using timer-based detection mechanism." *Signal processing and communication engineering systems (SPACES), International conference on*. IEEE, 2015.

[14] Ali Dorri and Hamed Nikdel. "A new approach for detecting and eliminating cooperative black hole nodes in MANET." *Information and Knowledge Technology (IKT), 2015 7th Conference on*. IEEE, 2015.

[15] Pooja and Chauhan, R. K. "An assessment based approach to detect black hole attack in MANET." *Computing, Communication & Automation (ICCCA), 2015 International Conference on*. IEEE, 2015.

[16] Ashish Kumar Jain and Vrinda Tokekar. "Mitigating the effects of Black hole attacks on AODV routing protocol in Mobile Ad hoc Networks." *Pervasive computing (ICPC), 2015 international conference on*. IEEE, 2015.

[17] Anand A.Aware and Kiran Bhandari. "Prevention of Black hole Attack on AODV in MANET using hash function." *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on*. IEEE, 2014.

[18] Kriti Patidar and Vandana Dubey. "Modification in routing mechanism of AODV for defending blackhole and wormhole attacks." *IT in Business, Industry and Government (CSIBIG), 2014 Conference on*. IEEE, 2014.

[19] Vishvas Kshirsagar, Ashok M. Kanthe, and Dina Simunic. "Analytical approach towards packet drop attacks in mobile ad-hoc networks." *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*. IEEE, 2014.

[20] Gayatri Wahane, Ashok M. Kanthe, and Dina Simunic. "Detection of cooperative black hole attack using crosschecking with truelink in MANET." *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*. IEEE, 2014.

[21] Ruo Cai Jun, Peter Han Joo Chong, and Cherry Ye Aung. "Poster: Trust-based routing with neighborhood connectivity to prevent single and colluded active black hole." *Communications and Networking in China (CHINACOM), 2014 9th International Conference on*. IEEE, 2014.

[22] Harsh Pratap Singh and Rashmi Singh. "A mechanism for discovery and prevention of coopeartive black hole attack in mobile ad hoc network using AODV protocol." *Electronics and Communication Systems (ICECS), 2014 International Conference on*. IEEE, 2014.

[23] Seryvuth Tan and Keecheon Kim. "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs." *High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on*. IEEE, 2013.

[24] Durgesh Kshirsagar and Abhijit Patil. "Blackhole attack detection and prevention by real time monitoring." *Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on*. IEEE, 2013.