Various Attacks in MANET and its Counter Measures

Manjeet Singh
Department of Computer Science
Guru Nanak Dev University
Amritsar, India

Kamaljit Kaur
Department of Computer Science
Guru Nanak Dev University
Amritsar, India

ABSTRACT
In present years, Security is important concern in Mobile ad hoc Network. MANET is self organized network which contains mobile nodes communicate with each other using wireless links. Nodes in the network are free to move in and out of the network. Due to its unique characteristics like Dynamic topology, Lack of central management, Limited resources, they are vulnerable to various types of attacks .In this paper we will present survey of various attacks like Black hole, Gray hole and worm hole attack in MANET. We will also discuss various proposed solutions to prevent and elimination of these attacks.

General Terms
Detection or Prevention of Various attacks in MANET.

Keywords
MANET, Blackhole, Grayhole, Wormhole;

1. INTRODUCTION
MANET consists of mobile nodes which communicate with each other through wireless medium [1]. The range of mobile nodes is limited. So each node acts as router to communicate with other nodes which are not within its range. The topology of MANET rapidly changes due to which various issues occurs in MANET.

2. MANET ROUTING
Routing is bigger challenge in MANET because of the frequently change in network topology. The main objective of routing protocol is to provide the optimal route with minimal bandwidth and overhead [12]. So the types of protocol in MANET are

Table 1. Routing Protocols

TYPE	WORKING	EXAMPLE	LIMITATION
Proactive Routing	Maintain routing tables of destinations prior to requirement. Nodes periodically send update messages to neighbors.	DSDV, OLSR, WRP, GSR, FSR, STAR, DREAM, HSR	Routing tables must be updated with each topology change. Nodes periodically send update messages even when no traffic is present.
Reactive Routing	On demand route discovery process to flood the network with route query requests. Nodes have information of their active routes only.	AODV, DSR, TORA, LAR, ROAM, CBRP, ARA	Cause delays in packet transmission as routes are calculated.
Hybrid Routing	Combine features from both reactive and Proactive routing protocols to exploit efficient communication in MANET.	ZRP, SHARP, ZHLS, DST, DDR	When the scale of the network changes, sometime overhead or other delay occurs.

3. VUNERABILITIES IN MANET

3.1 Dynamic Topology
Nodes in the network are free to move in and out which leads to the unpredictable topology changes [14]. Because of the change in network topology, it is necessary that nodes incorporate with each other to prevent any kind of security disturbance in the network.

3.2 No Clear Line of Defence
There is lack of secure boundary in MANET which makes it venerable. Attackers can attack the network either internally or externally [13]. The attacks mainly include passive eavesdropping, leakage of secret information, data tampering, message replay and denial of service.

3.3 Wireless Links
As the communication between various nodes is not through physical medium and attackers do not need physical access to the network for various attacks [13]. The bandwidth of wireless medium is less as compared to wired.

3.4 Lack of Centralized Management
There is absence of centralized management which affects the security in MANET because it is difficult to monitor nodes in highly dynamic and large scale network [14]. Due to lack of centralized management various problems of detection of attacks, path breakage, packet dropping occurs.

3.5 Limited Energy Resources
Due to mobility of nodes in MANET, they have limited energy resources as they rely on battery. Since the attackers knows that the nodes have restricted power supply, various attacks like DOS or trapped can be occurred [13]. A node in

the MANET behaves in selfish manner if it finds that there is limited battery.

3.6 Scalability

Scale of MANET keeps changing because the nodes in MANET are mobile and in future it is difficult to predict the number of nodes in network [13]. So the routing protocol should be compatible to the changing scale of the network.

4. VARIOUS SECURITY ATTACKS

We will discuss Black hole, gray hole and Wormhole attack in this section.

4.1 Blackhole Attack

The black hole problem occurs when a malicious node claims shortest path to the destination through it for the purpose of dropping packets coming from source node [15]. An example of black hole attack is shown as Figure 1 in which node 1 is source and node 4 is destination. Node M is malicious node which sends fake RREP after receiving RREQ from source node claiming the shortest path with minimum hop count to destination. After receiving RREP from node M and other node, source node calculate shortest path and start sending packets through node M. Node M drops all the packets coming from source node and creates the problem of blackhole in the network.

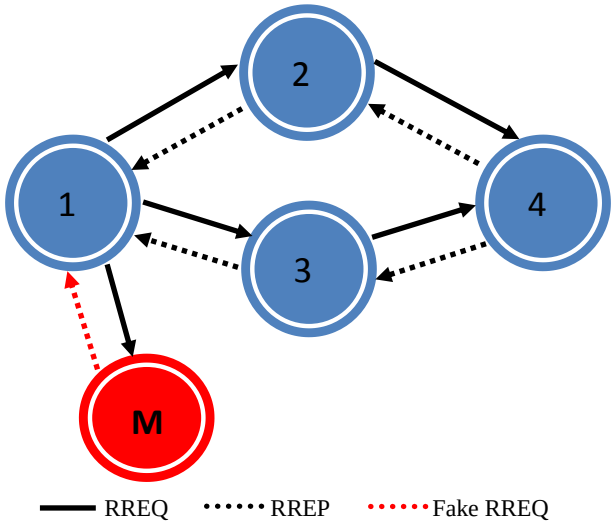

Fig1: Black Hole Problem

In this example node 1 is source node and node 4 is destination node. Node M is malicious node which sends Fake RREP after receiving RREQ from node 1. Node 1 start sending data packets to node M and it drops all the packets. So node M misroute packets and network suffers from blackhole problem.

4.2 Grayhole Attack

It is another form of black hole attack in which malicious node drops packets selectively [15]. The Grayhole attack has two phases.

Phase 1: Malicious node advertise itself by claiming shortest path to destination by sending RREP to source node.

Phase 2: Node selectively drops packet with certain probability and then behaves like normal node. Due to this behaviour it is very hard to detect this kind of attack in the network.

4.3 Wormhole Attack

In Wormhole attack, two colluding nodes creates illusion of having neighbours but actually distant from one another [15]. Two attackers nodes in MANET are connected through high speed-off channel placed at different end in network. The attacker node receives message from any node passes it to the colluding nodes through tunnel and advertise shortest path through them. Due to this false topology information is spread throughout the network. For delivering faster messages, other nodes send their messages through them. Thus it prevents other genuine nodes to establish connection between source and destination. An example of Wormhole attack is shown in Figure 2 in which X and Y are malicious node are connected through out-of-band channel. Node 1 is source node and send RREQ to node X and 2 and X passes it to Y and then to destination 5 and source selects the path 1-X-Y-B as its hop count is lesser. Attackers use this worm hole for various attacks like data tampering and other DOS attacks.

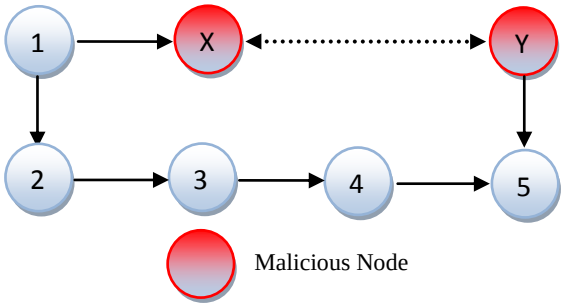

Fig 2: Wormhole attack

X and Y is malicious node in the network. Node 1 and node 5 are source and destination. X and Y are connected through high speed off-channel and create an illusion of neighbours at short distance but actually located at distant. Node 1 selects 1-X-Y-5 path as its hop count is minimum and attacker can use this tunnel to create problems in the network.

5. DETECTION/PREVENTION OF SECURITY ATTACKS

In this section literature is reviewed for prevention or detection of various security attacks like Blackhole attack, Grayhole attack and Wormhole attack.

5.1 Detection/Prevention Methods of Blackhole Attack

Latha Tamilselvan et.al [2] has presented a solution to Black hole(SAODV) in which TimerExpiredTable and Collect Route Reply Table(CRRT). After the expired time all the entries in the CRRT table are checked. The RREP in which there is repeated next hop nodes are selected. It assumes the path is correct or chance of malicious node is less. This solution is good only in those cases when more RREP packets arrive at source to select a secure path. The limitation of this solution is that sometimes a secure and shortest path gets eliminated at source.

Pramod Kumar Singh et.al [3] proposed method used promiscuous mode to detect blackhole and propagates the information of malicious node to all the other nodes in the network. In Proposed approach when the RREP packet is received from an intermediate node, a node preceding to the node which sent RREP packet switches on its promiscuous

mode and sends a *hello* message to the destination node through this node. If the hello message is forwarded by this node to the destination, the node and the route are safe. Otherwise, the node was a malicious node and the preceding node floods an alarm message to the network about the malicious node to isolate it. This method does not require any database, extra memory and more processing power.

Songbai et.al [4] has proposed and implemented a secure and efficient MANET routing protocol, the SAODV protocol. A secure routing protocol SAODV directly verifies the destination node by using the exchange of random numbers. SAODV can effectively prevent black hole attack in MANET and also maintain a high routing efficiency. It brings some burden to the network such as the source node needs to storage received RREP and SRREP in each routing discovery phase and to do relevant calculation. The destination node also needs to storage received SRREQ in each routing discovery phase and to do relevant calculation.

Mehdi et.al [5] has proposed to detect the blackhole in AODV using wait and check the replies from all the neighboring nodes to find a safe route. The judgment process was based on opinion of network's nodes about replier of RREP. The activities of a node were logged by its neighbors. These neighbors are requested to send their opinion about a node. When a source node collects all opinions of neighbors, it decides if the replier is a malicious node. The proposed protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes.

Ankur mishra et.al [6] has presented an approach for detection and elimination of black hole attack by improving AODV by using DRI table with additional check bit. The security mechanism consists of four security procedures. (A). DRI table was used to store neighbour data collection and local malicious node detection using 'from' and 'through' entry for the node. Local anomaly has been detected using Check Bit entry in the modified DRI table. By sending the probe messages two times an Initiator node able to identify the behaviour of the neighbour nodes and stores the check bit value accordingly. (B). Source node stores the RREP requests and check bit in the RREP_tab and demand their respective DRI table with check bit and find one trusted node to destination. (C). The path from source is established using check bit and all the black hole nodes removed. (D). The nodes which marks 0 under check bit column are stored as black hole nodes in MALI_node variable so that in future this node cannot participate in communication.

Table 2. Techniques of Blackhole Detection/Prevention

Method	Description	Limitations
Wait and check replies [2]	Without sending data to the first reply waits for the other reply and choose the path having repeated node; if not then select random path	Average end-end delay is more than the normal AODV.
Promiscuous mode [3]	Node proceeding to the node which sends RREP sends hello packet through this node to detect safe route.	Average end-end delay is much more than normal AODV in presence of black hole attack
SAODV [4]	Source node sends SRREQ which contains secret number to destination after receiving RREP and destination sends SRREP after receiving at least two such SRREQ. Source selects shortest path after receiving at least two SRREP.	The throughput of the network decreases and in presence of black hole attack, nodes are not able to communicate in some cases.
Opinion of network nodes [5]	After receiving RREP source node takes the opinion of various nodes replier of RREP and selects the secured path	Network overhead and delay increases
DRI table with Check bit [6]	Local anomaly is detected using DRI table and check bit is used to find secured path to destination	Overhead of DRI table and check bit entry

5.2 Detection/Prevention of Grayhole Attack

Rutvij H. Jhaveri et.al [7] has presented a R-AODV to detect the malicious node and to improve the performance of MANET. It uses number of sent out RREQs, number of received RREPs and routing table sequence number to dynamically calculate a PEAK value after every received RREPs. The PEAK value was calculated by adding these three parameters to the previous PEAK value. Destination sequence number of received RREP was compared with this PEAK value to detect existence of a malicious node. When a malicious node was detected by an intermediate node after receiving RREP, R-AODV marks the RREP as DO_NOT_CONSIDER and marks the node sending RREP as MALICIOUS_ NODE in the routing table. This technique further reduces normalized routing overhead by decreasing number of forwarded reply packets sent by adversaries.

Khattak et.al [8] has proposed an method for detection of gray hole attack in AODV. The malicious node always tries to reply RREP immediately without having route to destination with minimum hop count. In the proposed method, source node discards the first RREP and selects the second shortest path to destination. So it becomes harder for malicious node to know where to place itself in network to exploit it.

Meenakshi et.al [9] has presented Support Vector Machine (SVM) to defense against malicious attack occurring in AODV. Proposed method uses machine learning to categorize nodes as malicious. A system gather the behaviors of each node in the network and then check behavior of each node and compare it with the threshold values T and validate by the SVM. SVM based system used PDER (Packet Delivery Ratio), PMOR (Packet Modification Rate) and PMISR (Packet Misroute Rate) to analyze the performance.

Table 3. Techniques of Grayhole Detection/Prevention

Method	Description	Limitation
PEAK value [7]	Dynamically calculate PEAK value and compared with destination sequence number to detect the existence of grayhole attack.	Routing overhead involved with effect of mobility
Second shortest path [8]	Source node discard first shortest path and selects the second one.	Perform better only when malicious node is present in network
SVM [9]	Machine learning based method by gathering the behavior of nodes to check whether they are forwarding packets or not in the network	Extra hardware is required

5.3 Detection/Prevention of Wormhole Attack

Yudhvir Singh et.al [10] has proposed a technique for avoidance of worm hole attack which avoids the route having worm hole nodes without affecting network performance. As the misbehaving node advertise itself having shortest path, so alternative path is selected by again doing the route discovery by modifying the working DSR protocol. It detects the routes having wormhole nodes and the routes are not added in DSR routing table.

Prateek Thakral et.al [11] has presented a technique for prevention of wormhole attack using clustering with digital signature. In this technique, a network was divided into various clusters each having its cluster head (CH) and contains Gateway for communication with other clusters. Each cluster head broadcast its public key and gateway exchanges public keys of their CH. This prevented the routing data to be communicated through the wormhole path as the communication takes place through Cluster heads and gateways.

Table 4. Techniques of Wormhole Detection/Prevention

Method	Description	Limitation
Avoiding route [10]	Avoiding the shortest path and again route discovery to avoid worm hole attack	Performance decreases when no malicious node is present
Clustering [11]	Divides network into clusters and communicate using gateways using public keys to prevent worm hole attack	Not work when worm hole nodes are in adjacent clusters

6. CONCLUSION AND FUTURE WORK

Security is important concern in MANET as it is vulnerable to various security attacks. In this paper, we have discussed various vulnerabilities in MANET and various attacks like Black hole, Gray hole and Wormhole attack. Various methods for their prevention and detection are reviewed and some are still not perfect in terms of effectiveness while other are expensive in resource constrained MANET. Some solutions work only in presence of one malicious node and not applicable for multiple malicious nodes.

Future research should be focused on making the methods effective for detection of attacks and also the cost should be minimized to make these methods suitable for resource-constrained MANET.

7. REFERENCES

[1] Ramanathan, Ram, and Jason Redi. "A brief overview of ad hoc networks: challenges and directions." *IEEE communications Magazine* 40, no. 5 (2002): 20-22.

[2] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of blackhole attack in MANET." In *Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on*, pp. 21-21. IEEE, 2007.

[3] Singh, Pramod Kumar, and Govind Sharma. "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET." In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pp. 902-906. IEEE, 2012.

[4] Lu, Songbai, Longxuan Li, Kwok-Yan Lam, and Lingyan Jia. "SAODV: a MANET routing protocol- that can withstand black hole attack." In*Computational Intelligence and Security, 2009. CIS'09. International Conference on*, vol. 2, pp. 421-425. IEEE, 2009.

[5] Medadian, Mehdi, Ahmad Mebadi, and Elham Shahri. "Combat with Black Hole attack in AODV routing protocol." In *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on*, pp. 530-535. IEEE, 2009.

[6] Jaiswal, Ranjeet, and Sanjay Sharma. "A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network." In *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, pp. 499-504. IEEE, 2013.

[7] Jhaveri, Rutvij. "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs." In *Accepted and To be published In: Proceeding of International Conference on Advanced Computing & Communication Technologies (ACCT 2013), CPS (IEEE Computer Society)*. 2013.

[8] Khattak, Hizbullah, N. Nizamuddin, and F. Khurshid. "Preventing black and gray hole attacks in AODV using optimal path routing and hash." In *Networking, Sensing and Control (ICNSC), 2013 10th IEEE International Conference on*, pp. 645-648. IEEE, 2013.

[9] Patel, Meenakshi, and Sanjay Kumar Sharma. "Detection and prevention of Routing Attacks in MANET using AODV." *International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE)* 1, no. 1 (2012): pp-39.

[10] Yudhvir,Avni,Prabha,Deepika and Dheer " Wormhole Attack Avoidance Technique in Mobile Adhoc Networks." In *3rd International Conference on Advanced Computing & Communication Technologies*, pp 283-287. IEEE, 2013.

[11] Dabas, Poonam, and Prateek Thakral. "A Novel Technique for the Prevention of Wormhole Attack." *International Journal* 3, no. 6 (2013).

[12] Hinds, Alex, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi. "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)." *International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.*

[13] Sheikh, Rashid, M. Singh Chande, and D. Kumar Mishra. "Security issues in MANET: A review." In *Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On*, pp. 1-4. IEEE, 2010.

[14] Zaiba Ishrat. "Security issues, challenges & solution in MANET." *IJCST Vol. 2*, Issue 4, Oct - Dec. 2011.

[15] Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. "Dos attacks in mobile ad hoc networks: A survey." In *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on*, pp. 535-541. IEEE, 2012.