Comparative Analysis of Various Attacks on MANET

Pooja Chahal
Department of Computer Science
Lovely Professional University
Phagwara, India

Gaurav Kumar Tak
Department of Computer Science
Lovely Professional University
Phagwara, India

Anurag Singh Tomar
Department of Computer Science
Lovely Professional University
Phagwara, India

ABSTRACT
Mobile Ad hoc Networks (MANET) is a part of wireless networks. No wires and fixed routers are used in this type of network. It is not everlasting network; it is the short term network. Nodes has the capability to self organize themselves and it follows infrastructure less architecture. Network is formed by number of nodes moving in an inconsistent manner. They do not form any topology. Few examples of Ad hoc wireless network devices are Laptops, palmtops, smart phones etc [6]. And every nodes further acts as routers which transfers packet from one node to another node. Security is one of the main issues in Mobile Ad hoc Network. From last few years security problems in MANETs are gaining much attention. As there are many security vulnerabilities in MANET and which is the reason that it is not safe from attacks. There are many types of MANET like VANET (Vehicular Ad hoc Network), SPANs (Smart Phone Ad hoc Networks), iMANET (Internet based Mobile Ad hoc Network), Tactical MANET. The aim of this paper is to discuss about different types of attacks in Ad hoc network and some of the techniques by which these attacks can be protected.

Keywords
Black hole attacks, jellyfish attack Mobile Ad hoc network, Sybil attack, Sleep deprivation torture attack, Wormhole attacks

1. INTRODUCTION
A mobile ad hoc network is a network that is formed by collection of two or more nodes (devices) that moves in an unpredictable manner. One node can communicate with another that is within its radio range or outside their radio range. It follows an infrastructure less architecture yet has a potential of service discovery, routing and packet forwarding. Communication is possible between two nodes with the help of routing protocols like AODV (Ad hoc On demand Routing Protocol), Link State Routing Protocol, WRP (Wireless Routing Protocol), ZRP (Zone Routing Protocol) etc. In these types of networks nodes can move randomly from one place to another without maintaining any topology, no static topology is there. At any time they can join the network and leave the network. These networks can be easily deployed and also setup time is very less because they do not have fixed infrastructure.

2. ATTACKS CLASSIFICATION
Attacks can be classified in many categories like internal attacks, External attacks, Active Attacks Passive Attacks. Attacker can harm the network as internal, external or active, passive so this classification is very important.

2.1 External Attack
These attacks are basically used by the person who is outside the network and want to get access to the network. And if they get entry to the network then they misuse it, they send spoofed packets and due to which the whole network gets down. In wired network this attack is also there. It can be prevented with the help of firewalls [3].

In figure 1, there are four computers or nodes i.e. A, B, C and D and they belongs to a single network. Every computer is connected to each other. Any external computer say computer E which does not belongs to the same network tries to get access to the network and will do malfunctioning in the network.

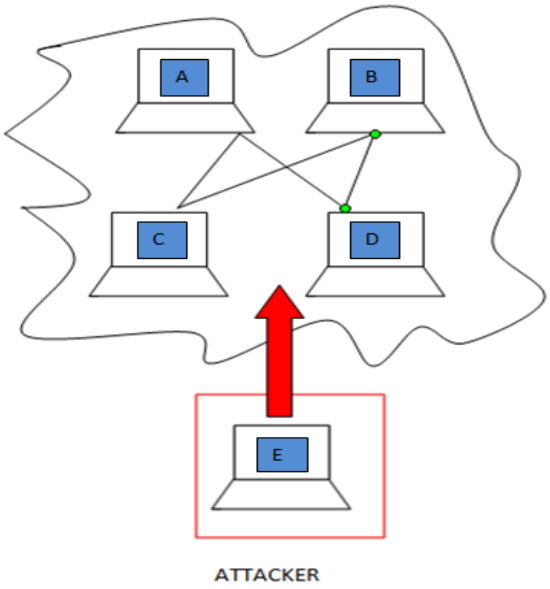

Figure 1: External Attack

2.2 Internal Attack
This attack is usually occurs inside the network. The attacker can normally involve in the communication. A new node that is added to the network can act as an attacker that has gain the access to a network. It has gain access to the network either by making a deal with current node or by impersonation. It is very difficult to predict the internal attacks as compared to external attack [3].

In figure 2, initially there are three nodes A, B and D, they all are connected with each and belongs to the same network. Suppose C node came into existence and join the network and hence can participate in the communication. As C node is malicious one so it can hamper the communication by sending spoofed packets to other nodes or by dropping all the packets.

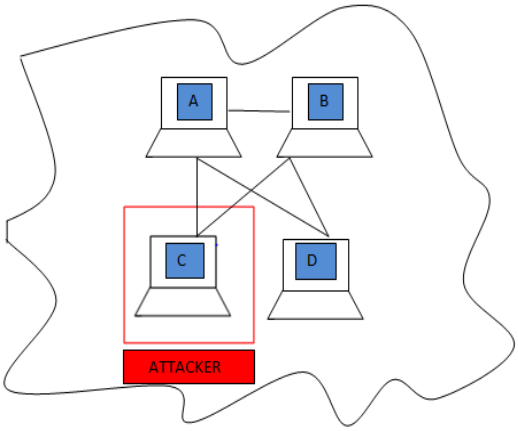

Figure 2: Internal Attack

2.3 Passive Attacks

In this attack, an attacker only listens or keeps track of data or information that is being transferred between two parties. No modification and fabrication is done. Examples of passive attacks are eavesdropping and Traffic Analysis. Attackers can easily get all the information about the network that is useful in hijacking or injecting an attack in the network. It is quite hard to detect passive attacks as compared to active attacks.

In figure 3, there are two computers A and B which are communicating with each other. Suppose they are sharing or transferring some confidential information and while doing so one more computer i.e. computer C comes into play and it will acts as a sniffer and will listen each and every thing that is going on between computer A and computer B. In this type of attack attacker only listens the information and later on display it to others.

2.3.1 Eavesdropping

In this the attacker listen all the information that is being transmitted between the two parties in order to find some useful data like passwords, secret codes, confidential information etc.

2.3.2 Traffic Analysis

In this the attacker keeps track of the traffic flow so that he is able to detect the location of the hosts. By using this method the attacker can determine the patterns, frequency and length of the message.

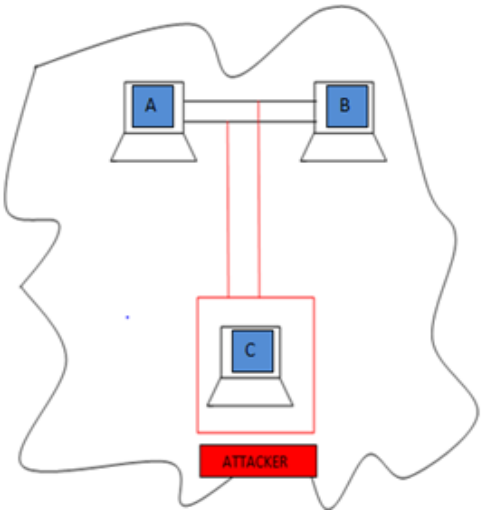

Figure 3: Passive Attack

2.4 Active Attack

In active attack the attackers modify the data. It is basically used to reduce the performance of the network. Some of the examples of active attacks are masquerade attacks, replay attacks, DOS attacks.

In figure 4, there are two computers A and B which are communicating with each other and computer C which acts as an attacker will modify or change all the data coming from computer A and then sent the modified data to computer B.

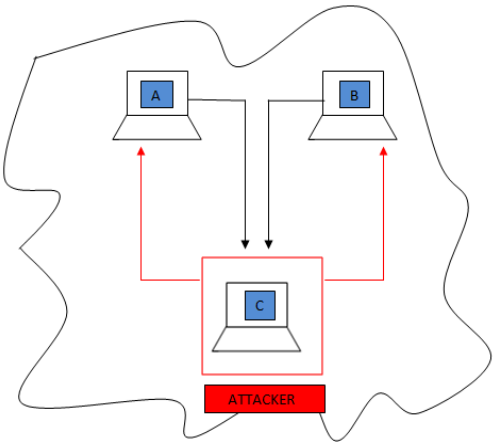

Figure 4: Active Attack

2.4.1 Black hole attack

This attack is network layer attack, all the packets are dropped by the hostile node and fake packets are further send for communication. In this the selfish or hostile node with the help of its routing protocol announces that it has the shortest path to destination. All the nodes in the network get this information then every node will start sending packets to this malicious/hostile node and after receiving all the packets, malicious node will simply drop all the packets and send fake packets [3].

In figure 5, node "X" wants to send packet to node "A". In order to do so node X will send RREQ message to neighboring nodes i.e. node "Y" and node "Z". As "Z" is malicious node it will quickly responds to the RREQ message send by node "X" by sending a false RREP message. Node "X" will think that it is an active route and will send packet to node "Z". After receiving packets from node "X", node "Z" will drop all the packets.

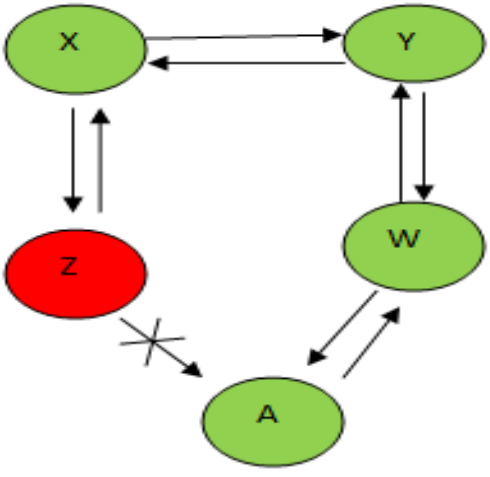

Figure 5: Black hole Attack

2.4.2 Wormhole attack

This attack belongs to network layer and it one of the most dangerous attack. It basically records information or traffic form one point, tunnels it and then broadcast it to other point. Packet Leases is one of the technique by which wormhole attack can be detected, Packet Leases can be geographic or temporal, and the reason of using leases method is that it will put a limit on greatest_amount of transmission distance of a packet. With the help of some of some techniques wormhole techniques can be created for example packet encapsulation, high power transmission capability, packet relay, protocol distortion etc [7].

In figure 6, a malicious node "C" created a extraneous link A-B. And node "C" will wormhole the messages that are transferring between A and B.

There are many techniques proposed to detect and prevent wormhole attacks like Packet leases, SECTOR, these methods needs time synchronization. Hu and Evans proposed a method i.e. use of directional antenna at each node present in the network. This method requires use of some additional hardware. Hu, Perrig, and Johnson introduced a method of using anchor nodes which requires the need to know the exact position of the nodes; it also requires manual setup of the network. Yurong Xu et al. proposed a technique that does not require setting the network manually or any use of hardware and anchor nodes. The above technique is also named as Wormhole geographic distributed detection (WGDD) [8]; this algorithm is able to find out the approximate location of wormhole.

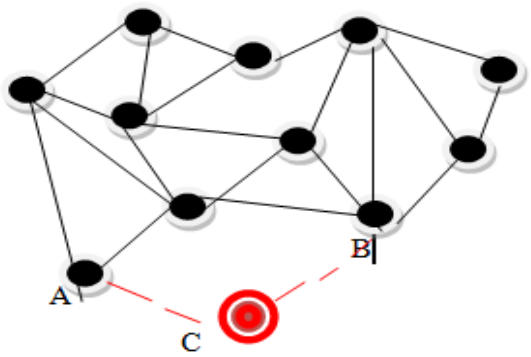

Figure 6: Wormhole Attack

2.4.3 Sleep deprivation torture attack

This attack belongs to layer 2. In this attack purposeless or worthless control traffic is send over the packet and this continues until all the nodes present in the network get overtire or exhausted and will stop working. The main aim of the intruder is to maximize the power consumption and hence lifetime of the nodes will minimize. Due to infrastructure and innocent nature it is very hard to detect and prevent sleep deprivation attack.

2.4.4 Jellyfish attack

In this type of attack firstly the attacker node tries to get access to the network. If the attacker node gets access network then it starts introducing the unwanted delays in the network i.e. as soon as the packet is received by the attacker node it will forward the packets after some delay as a result of which high end-to-end delay is generated by the intruder and it will affect the performance.

2.4.5 Misrouting attack

In this attack a selfish node reroute all the traffic originating from a source node and destined for a particular destination node to wrong destination. Hence when a packet does not find its destination, packet is dropped.

2.4.6 Sybil attack

In this attack an attacker simultaneously acts as different identity which leads to misunderstanding among nodes and it also hampers the communication among nodes [2]. For proper transmission of packet or information it is very important to remove Sybil nodes. Validation techniques are used to block this attack.

2.4.7 Dos attack

In this type of attack an attacker sends millions of packets or useless traffic simultaneously to a server and attempting to slow the server or making the resources unavailable to the users and hence due to which a user cannot able to access the facility.

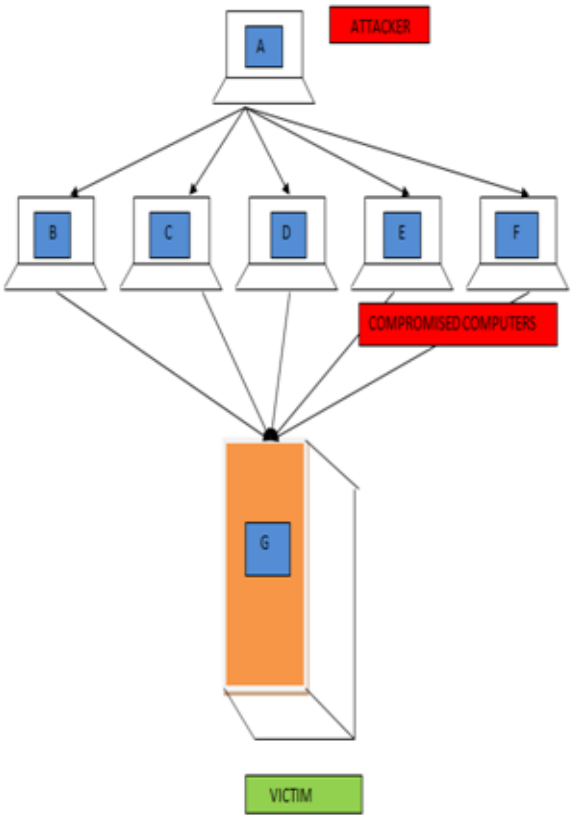

Figure 7: DOS attack

In this figure an attacker i.e. computer A will send request or packets to compromised computers say computer B, C, D, E, F and then these compromised computers simultaneously flood the server (computer G) with thousand and millions of requests. And hence user can't access the resources.

3. LITERATURE REVIEW

Jaspal Kumar, M.Kulkarni et al. analyzed the effect of black hole attack. Author worked on two protocols AODV and Improved AODV. Then the simulation is performed by adding malicious nodes in the network. Results show that Improved AODV is better than AODV. And effect of malicious node on IAODV is less as compared to AODV. Author concluded that IAODV is more vulnerable to black hole attack than AODV.

Neelam Khemariya and Ajay Khuntetha proposed an algorithm to detect black hole attack in AODV routing protocol. By using this algorithm one can detect black hole nodes when a node is idle (when there is no communication between the nodes) and when a node is not idle. It works for single black hole node as well as for multiple black hole nodes. Then the author two results one when there is only single black hole node and second is when there are more than two nodes. These two simulations made the approach secure, reliable and efficient

Boundpadith Kannhavong, Hidayamaehisa Nakyama et al. had discussed all the attacks possible on the MANET. Attacks are black hole, colluding misrelay attack, link spoofing attack, wormhole attack, replay attack, message withholding attack, flooding attack. Author also discussed about the advantage, disadvantages and countermeasures of each attack**.**

Romina Sharma and Rajesh Shrivastava tried to improve the AODV protocol and introduced a modified AODV protocol that can help us to prevent the black hole attack. And the effect of black hole node is compared with the previous protocol. Several performance metrics are evaluated and result shows that packet delivery ration and throughput is reduced. This modified AODV has one disadvantage it can only prevent single black hole node, when multiple black hole node is present in the network then this algorithm does not work.

G.S. Mamatha and Dr. S.C. Sharma had proposed a security mechanism to detect the attacks by identifying malicious nodes in the network, no packets dropped and misbehaving links in the network. Two approaches were used first one is to detect malicious nodes in the network and second one is to use acknowledgement approach which uses two way communication. Implementation is done using AODV protocol. As a result this mechanism proved to be efficient and secured.

Yih-Chun Hu and David B. Johnson proposed a mechanism known as packet leases to detect wormhole attack which is one of the severe attacks in the MANET. A packet lease is mechanism that detects and defends against wormhole attack. Author also discussed about topology based wormhole detection. Author distinguished between two type of leases i.e. geographical leases and temporal leases. And for implementation purpose TIK protocol is used and results shows that geographical leases is less efficient that temporal leases

K. Kayalvizhi1, N. Senthilkumar G. Arulkumaran proposed a RSS-bases mechanism to protect the network against the Sybil attack. RSS based mechanism worked on MAC layer using 802.11 protocols and it does not require any special hardware like directional antennas and geographic positioning system. And results show that Sybil attackers can be detected with high degree of accuracy.

Tapalina Bhattasali, Rituparna Chaki, Sugata Sanyal proposed a hierarchical model with the help of which sleeplessness of nodes can be detected. This technique was introduced to save power consumption of nodes and as a result of which lifetime of nodes will extend and hence nodes get less affected by this attack. Proposed model was based on anomaly detection technique which provides an energy efficient and reliable network. And it will also discard the fake packets and malicious nodes.

Annie Jenniefer, John Raybin Jose had described different type of denial of service (DOS) attacks. Three types of DOS attacks are explained in this paper first one is consumption of scarce, limited resources second is alternation of configuration information and third is physical alteration of network resources. Author also explained some of the techniques to detect DOS attacks and prevent it. The techniques are monitor nodes, gateway MAC, Evasion, multi dataflow, WCL and Lightweight Medium Access Control (LMAC) technique.

4. COMPARISON OF ATTACKS

Table 1: Attacks comparison

ATTACK	ATTACK CATEGORY	PREVENTION TECHNIQUES
Black hole	Active	SAODV
Wormhole	Active	Packet Leases, SAW DAW, DELPHI, HMTI etc
Sleep Deprivation torture	Active	Sensor MAC, Timeout MAC, Berkley MAC, Hash based scheme, Clustered Adaptive Rate limiting(CARL) etc
Misrouting	Active	Watchdog mechanism
Sybil attack	Active	Lightweight and robust detection technique
Denial Of Service (DOS)	Active	Evasion, LMAC
Eavesdropping	Passive	SSL
Traffic Analysis	Passive	Transmission schedules

5. CONCLUSION

Nowadays everyone has laptops, Smartphone's, PDA's and they want to connect these devices with others device so that they can exchange information and MANET is the only solution to it. It is temporary network which is set up on the temporary basis and disconnected when the work has been done. It is better for small area only. It has great applications in the field of military, hospitals (fast retrieval of data), education (virtual classrooms, conferences), emergency (disaster, earthquake). Sensors are small device that are deployed in a particular are for sensing the data or information. Micro sensors are used in military, health industries, food industries, used for environmental and weather information gathering. But it is also true that this network is vulnerable to several attacks i.e. security is the major issue in wireless network. Hence this paper shows different types of attacks in MANET. This paper focused on active attacks like black hole, Wormhole, Sleep deprivation

Torture attack, Sybil attack etc. And some of the detection techniques are also described to prevent these attacks.

6. ACKNOWLEDGEMENT

I express my gratitude to Lovely Professional University for giving me support and infrastructure to complete this paper.

7. REFERENCES

[1] Bhattasali, T.,Chaki, R. and Sanyal, S. 2012. Sleep Deprivation Attack Detection in Wireless Sensor Network, International Journal of Computer Applications (0975 – 8887)

[2] Garg, R., and Sharma, H. 2014. Proposed Lightweight Sybil Attack Detection Technique in MANET. International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering.

[3] Ullah. Irshad and Rehmaan, Shoaib. 2010. Analysis of Black hole Attack on MANET using different MANET routing protocols, Thesis no: MEE-2010-2698.

[4] Kumar, J., Kulkarni, M., Gupta, D. 2013. Effect of Black Hole Attack on MANET Routing Protocols, I. J. Computer Network and Information Security.

[5] L. Hu and D. Evans. 2004. Using directional antennas to prevent wormhole attacks, Proceedings of the Eleventh Network and Distributed System Security Symposium.

[6] Toh, C.K. 2001. Ad hoc mobile wireless networks: protocols and systems. Pearson Education.

[7] Hu, Y., Perrig, A. and Johnson, D. 2006. Wormhole Attacks in Wireless Networks, IEEE JSAC.

[8] Xu, Y., Chen, G., Ford, J., Makedon, F., Goetz, E., Shenoi, S. 2007. Detecting wormhole attacks in wireless sensor networks, Critical infrastructure protection, Springer US.

[9] Mamatha, G.S., Sharma, S.C. 2010. A Highly Secured Approach against Attacks in MANETS. International Journal of Computer Theory and Engineering.

[10] Khemariya, N., Khuntetha, A. 2013. An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs. International Journal of Computer Applications (0975 – 8887).

[11] Sharma, R., Shrivastava, R. 2014. Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc Network. IJCSNS International Journal of Computer Science and Network Security.

[12] Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N. 2007. A Survey Of Routing Attacks In Mobile Ad Hoc Networks. Ieee Wireless Communications.

[13] Kayalvizhi, K., Senthilkumar, N., Arulkumaran, G. 2014. Detecting Sybil Attack by Using Received Signal Strength in Manets. International Journal of Innovative Research in Science & Engineering.

[14] Jenniefer, A. and Jose, J. 2014. Techniques for Identifying Denial of Service Attack in Wireless Sensor Network: a Survey. International Journal of Advanced Research in Computer and Communication Engineering, ISSN: 2319-5940, Vol. 3.