A Review on the Security of Mobile Ad Hoc Networks

Amruth V[1], Mudassira Tahneet B. Lahori[2], Reema Abdul Rauf[2], Mariyamath Rifaina[2], and Jeril Kuriakose[3]
[1]Department of Information Science and Engineering, Bearys Institute of Technology, Mangalore, India
[2] Department of Computer Science and Engineering, Bearys Institute of Technology, Mangalore, India
[3] School of Computing and Information Technology (SCIT), Manipal University Jaipur, India

***Abstract*— In wireless networks, Mobile Adhoc Network (MANET) is one of the most promising field for research and development. As popularity of wireless networks and mobile devices has considerably improved over the past few years, wireless ad hoc networks has become one of the most active and vibrant field in communication and networks. The unique features of MANETs such as dynamic network topology, limited battery power, limited bandwidth has made it a challenging task to provide secure routing in MANETs than in other conventional networks. In this paper we present an overview of various security issues in MANETs. In particular, we have examined attacks such as wormhole, black hole, greyhole, rushing, Sybil and flooding attacks as well as existing solutions to protect MANET.**

Keywords—Mobile Adhoc Network; Wormhole; Blackhole; greyhole; Security; Rushing; Sybil;

I. INTRODUCTION

MANET is a dynamic wireless network that can be formed without any fixed and pre existing infrastructure. This ability of MANETs is extensively used in areas where communication has to be provided temporarily such as in battle fields, disaster hit area [1]. Importance of wireless networks cannot be denied as the world of computing is getting portable and compact. MANET can be established extremely flexibly without any fixed base station in military applications, battlefields and other emergency and disaster situation. Some applications of MANET technology could include industrial and commercial applications involving cooperative mobile data exchange.

MANET poses a number of challenges due to their unpredictable and changing topology and absence of central and base [2]. The networks are composed of mobile nodes which are powered by battery, therefore energy must be used judiciously by the participating nodes. MANETs forward the packets from source to destination using intermediate relay nodes. Hence it is important that all the nodes cooperate and faithfully forward the packets to the destination. This is an ideal situation but like all other real life aspects, conditions are not ideal and there exists nodes with malicious or selfish attitude. The selfish attitude may be due to a nodes low power status and the malicious attitude can be due to opponent's intervention into the network.

A. Salient Features of MANETs

i. Dynamic topologies: Communication in MANETs occurs directly between the nodes or with the help of intermediate nodes. MANETs don't have a fixed topology, the nodes enter and leave frequently making the network dynamic.
ii. Bandwidth constraints: The throughput of wireless networks are affected by fading, interference conditions and noise. Wireless links have variable and lower capacity than wired links.
iii. Energy constraints: MANETs depend on batteries for their energy. Therefore energy conservation is the most important parameter for optimization.
iv. Limited physical security: Providing security in MANETs is challenging and difficult to achieve as the nodes are mobile. Absence of central server and base stations produces less harm than wired networks during single point failure.

A. Network Security Goals

The template is a secure networking environment should provide some or all of the following services:

i. Confidentiality: This is generally achieved through encryption. Confidentiality ensures that the transmitted data can only be accessed by the intended receivers and ensures that the intended receivers can only access transmitted data.
ii. Integrity: This can be provided using cryptographic hash functions with some form of encryption. It ensures that the information is unaltered during transmission.
iii. Authentication: It is important that both sender and receiver are sure of each others identity. Authentication can be provided using, digital signatures and certificates, encryption with cryptographic hash functions.
iv. Non-repudiation: This service ensures that the transmission or reception of data by other parties can be proved by it. For example, a party cannot deny having transmitted or received certain information. This service makes use of public key cryptography to provide digital signatures.
v. Availability: This service ensures that the network security services listed above are available when required. The availability is ensured by physical protection, redundancy and other non-cryptographic means [3].

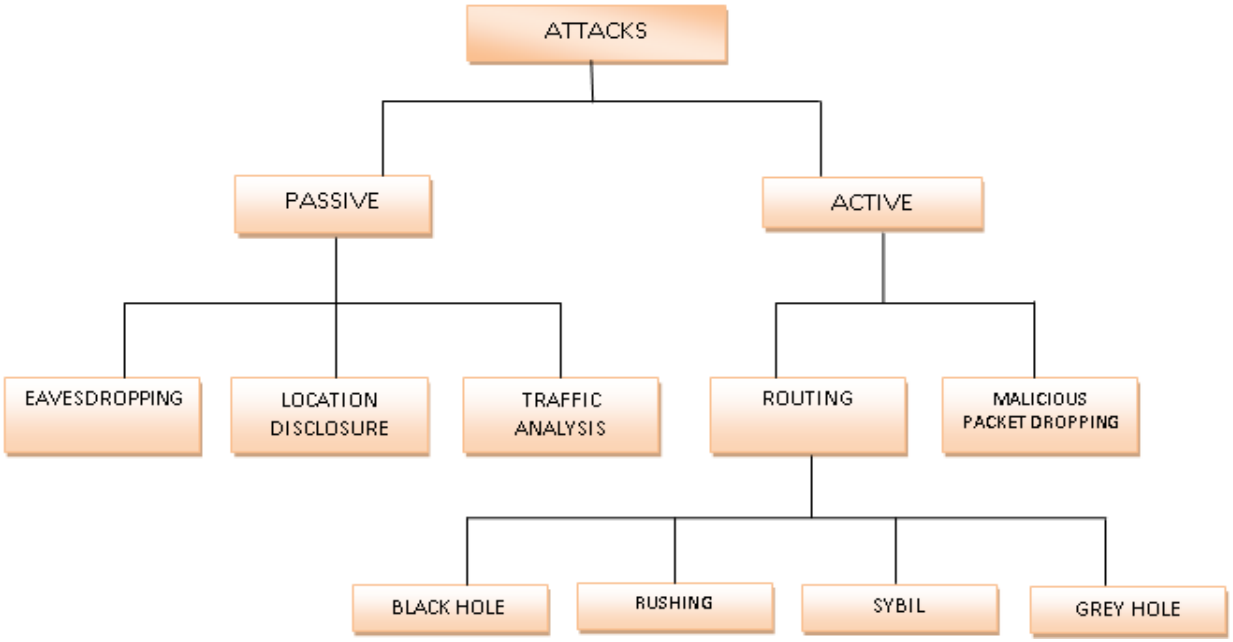

Fig. 1. Classification of attacks.

II. SECURE ROUTING FOR MANET

Security protocols for MANET's can be categorized into two: Prevention: This mechanism involves protocols which prohibit the attacking node to take any action. This approach requires encryption technique to authenticate the confidentiality, integrity and non-repudiation of routing packet information.

Detection and Reaction: As the name suggests this protocol will identify any malicious nodes or malicious activities in the network and take suitable actions to maintain the proper routing in the network.

III. DIFFERENT TYPES OF ATTACKS

Passive vs. active attacks: Passive attacks are initiated to steal important information from the networks. Examples of passive attacks are eavesdropping attacks and traffic analysis attacks. Active attacks are launched to alter the information with the intention of interrupting the network operations in the targeted network. Examples of active attacks are modifications, replays, fabrications of messages and the denial of service attacks.

External vs. internal attacks: External attacks are launched by nodes that are initially not authorized to participate in the network operations. These attacks cause network congestion and disrupt the whole network operations. Examples of external attacks are bogus packets injection, denial of service, and impersonation attacks etc. Internal attacks are launched by the nodes that are initially authorized to participate in the network operations. Internal nodes are said to be compromised when the external attackers hijack them and use them against the ad hoc network.

With the compromised internal nodes, security requirements are severely vulnerable in the network because communication keys used by these nodes might be stolen and passed to the other colluding attackers. On the other hand, internal nodes are said to be misbehaving if they fail to use the resources in the way they should. Misbehaving nodes do so to save their resources, such as processing capabilities and battery power. Attacks by the misbehaving nodes are difficult to detect because it is not easy to differentiate between normal network failures and misbehavior activities in the ad hoc network [4].

In this paper, the following attacks along with the security mechanism are discussed:

- Black hole attack
- Wormhole attack
- Flooding
- Gray hole attack
- Rushing attack
- Sybil Attack

A. Black hole Attack

In black hole attack, the malicious node broadcasts fake routing information saying that it has an optimum route, causing other good nodes to transmit their packets through this malicious node. For instance, in an AODV protocol, the malicious node can send RREP (route reply) to the source node, asserting that it has an optimal route to the destination. As a result the source node selects the path through the malicious node which can misuse or drop the packets.

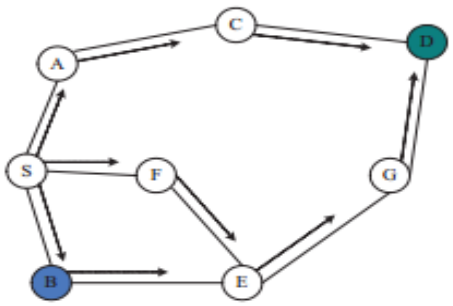

Fig. 2. Network flooding of RREQ

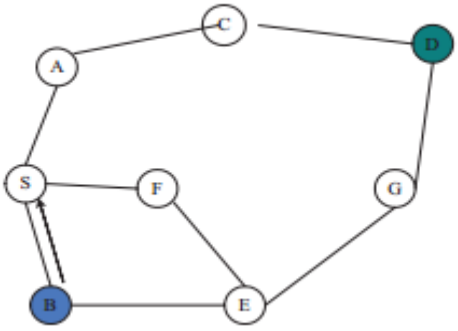

Fig. 3. Propagation of RREP message.

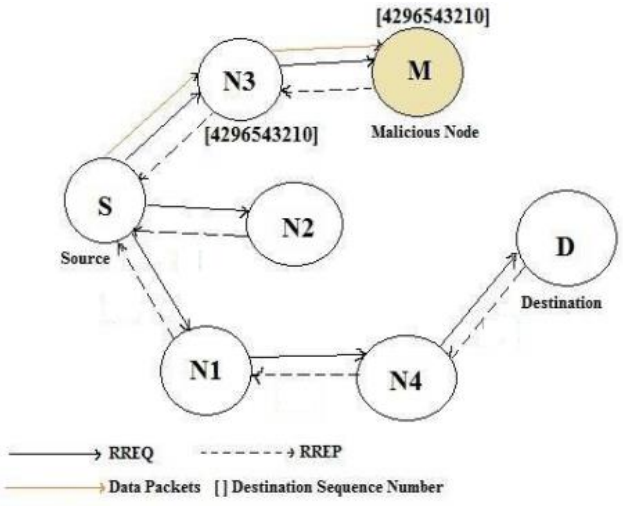

Fig. 4. AODV protocol packet exchange.

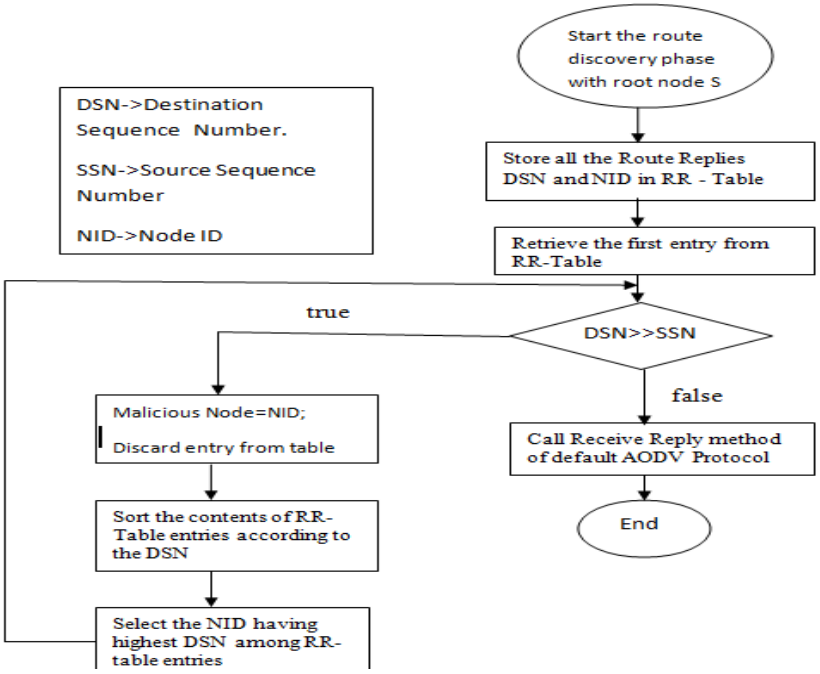

Fig. 5. Flowchart showing RREP method.

To avoid black hole attack, route CREQ (confirmation request) and CREP (confirmation reply) has been introduced. In this approach, the intermediate node not only sends RREP to the source node but also sends CREQ to the next hop node towards the destination. As soon as the neighboring node receives CREQ, it checks it cache and looks for a route to destination. If it finds a route, then it sends CREP to source node. The source node can then validate the route by comparing the path in RREP and CREP, if they match then the route provided is correct. The drawback of this method is that it cannot prevent black hole attack if two attackers are colluding with each other, because the next hop node, if malicious, may send fake CREP to the source node, misleading it. The solution to this method is that the source node must wait for more than two RREPs before making a decision. But the drawback of this solution is time delay, as the source node must wait until it receives more than 2 RREPs.

In another approach the researchers observed that the malicious node must amplify the destination sequence number to convince the source node that it can provide an optimum route. Black hole attack can be detected based on the difference in the destination sequence numbers provided by different RREPs. The main advantage of this approach is that it can detect attack at low costs without causing extra routing traffic. However, false positives are the main drawbacks of this approach [5].

The benefits of this solution are:

- The malicious nodes are easily identified at the initial stage without any delay and removed immediately, to prevent it from taking part in further process.
- No modification is made in the default operations of AODV Protocol.
- We achieve better performance by making little modification.
- Less memory overhead occurs as only few new things are added [6].

Wormhole Attack

In worm hole attack two colluding nodes that re geographically separated attack a network, wherein one conspiring node tunnels the packets to another conspiring node located at a distance. The second conspiring node then replays the packets locally. There are several methods to establish a tunnel and two of them have been discussed below.

In the first method, a malicious node X encapsulates a packet received by its neighboring node A, which is then forwarded to the colluding malicious node Y. Node Y then replays the decapsulated packet in the neighborhood. Thus, the packet transmitted by node A is replayed by node Y in it neighborhood which includes node B.

For instance if node A transmits a hello packet to node B through node X, then node B n receiving this packet may assume that node A is its neighbor, which is not true. As another example, if node a sends a RREQ to node B, then node X can tunnel this packet to node Y by encapsulating it. Thus the route request packet will reach the destination node B with a lower hop count than other packets going through other routes.

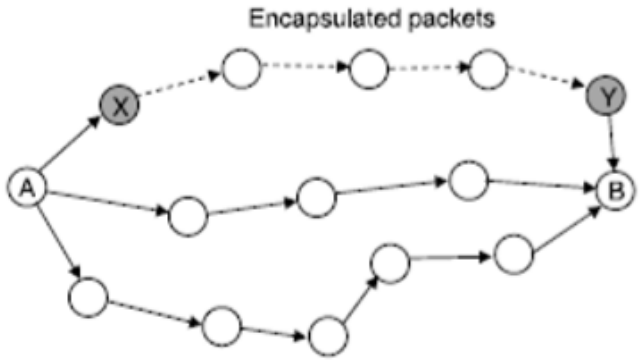

Fig. 6. Wormhole attack for encapsulated packet.

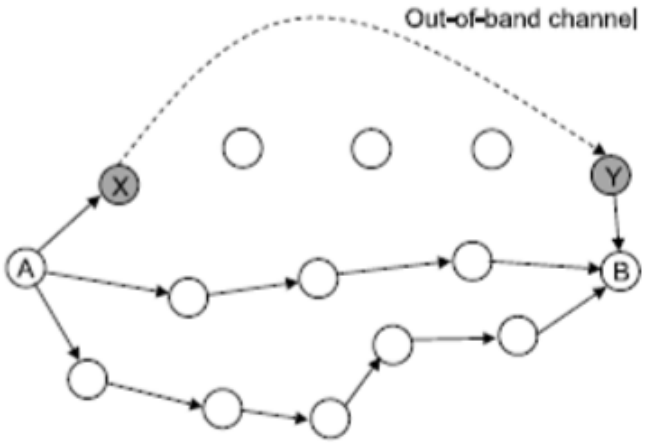

Fig. 7. Wormhole attack for out of band channel.

In the second method, the two colluding nodes X and Y are presumed to have access to a channel with out-of-band high bandwidth. This can be achieved by having wireless link of high bandwidth with a long range operating at a different frequency or by having a wired link between the two nodes. Therefore, this method needs specific hardware capacity and hence it is more difficult than the first method. In this method too, node A transmits a hello packet to node B through node X, then node B on receiving this packet may assume that node A is its neighbor, which is not true. In the same way, if a route request packet (RREQ) is sent from node A to node B, reaches node B faster with few hops as a high bandwidth link is used. So the two endpoints in the tunnel may appear closer than they actually are as shown in figure below.

Existing Solutions for Wormhole Attack

Two approaches to detect wormhole attacks are concept of leashes and deploying directional antennae.

Concept of leash:

Any information that is added to a packet in order to limit the distance it travels is called leash. It is associated with each hop, so, each transmission of a packet requires a new leash. There are two types of leash, geographical leash, that are meant to restrict the distance between the transmitter and the receiver of the packet, and temporal leash, to provide an upper bound over the lifetime of the packet, so that the packet can travel only a limited distance . These leashes can be used to determine whether the packet has travelled more than the distance allowed, if so, the packet can be dropped.

Deploying directional antennae:

This approach is based on the direction of packet arrival to detect whether the packets are arriving from proper neighbors. It is possible to obtain such information by using directional antennae [7]. This information can lead to accurate information about the set of neighbors a node has, which can be used to detect worm hole attacks as such attacks originate from malicious nodes.

Two Novel Solutions Proposed to Combat Wormhole Attack Limiting Packet Propagation Parameter (LP3):

In this novel technique, the Limiting Packet Propagation Parameter (LP3) is embedded with a multicast packet similar to Time to Live (TTL) field. A random value is assigned to this field which constraints the journey of the packet through the tunnel. This field value expires once the packet dissolves. It is designed in such a way that it reaches the destination safely before expiring. It is impossible for an attacker to crack this field as it is encrypted or digitally signed by the sender. Even though by the addition of this field, the packet size increases, it is of utmost importance to prevent wormhole attack.

The main target of wormhole attack are multicast routing protocol. In the absence of a wormhole attack, an optimal multicast route is chosen after determining the propagation delay, time and the number of intermediate nodes between the transmitter and receiver. After finding a potential position and status in the multicast routing, the malicious wormhole sends a fake optimal route advertisement promising optimal hop count value, propagation delay and time. The sender instead of accepting the promising offer, confirms the existence of a valid route using a multicast trace route test packet. This technique has very little chance of the sender falling to the wormhole adversary. This approach helps to instantly get rid of the wormhole adversaries providing secure zone.

i. Neighbor Aware Wormhole Adversary Axing (NAWA2):

The wormhole adversaries can attack freely until spotted by multicast neighbors. The genuine multicast neighbors sense a dip in the performance metric like Multicast Packet Delivery Ratio (MPDR) and jitter. These two multicast nodes join hands and locate the adversary node along with its colluder and assist in adding them to the Node Conviction List (NCL). As each node in MANET is constantly under scanning, monitoring and inspection of its neighbor, it is robust to falsified reports. The genuine neighbors act as watch dogs and handcuff the immediate neighbor if it tries to

protect the colluding node. This has led to the definition of this novel technique by name Neighbor Aware Wormhole Adversary Axing (NAWA2)

Fig. 8 below shows the adoption of two novel techniques like LP3 and NAWA2 in the wormhole infected MANET Multicast distribution tree. Fig. 9 registers the reaction of the solution techniques in arresting the wormhole adversaries and appending them to NCL [8].

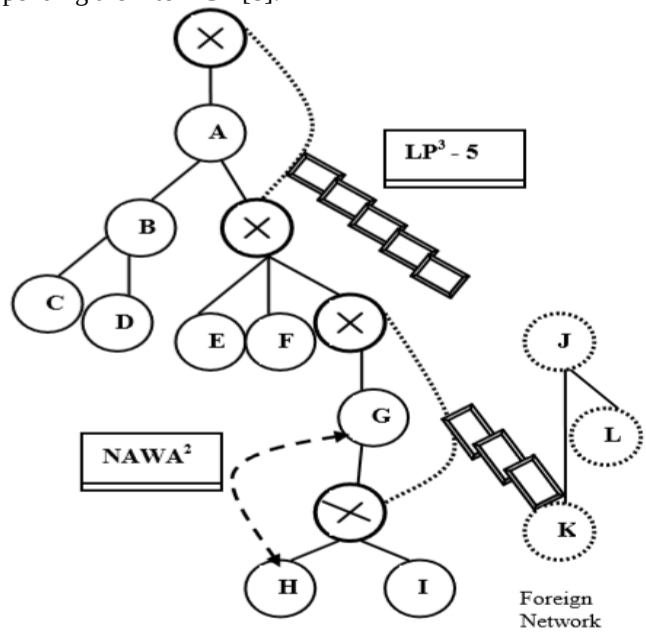

Fig. 8. NAWA example 1.

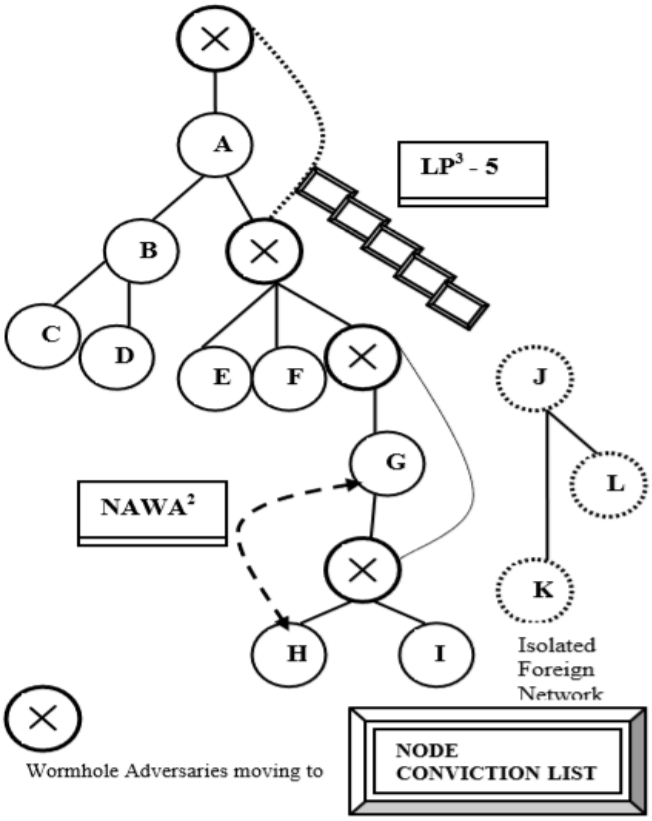

Fig. 9. NAWA working.

Flooding Attack

In flooding attack, the adversaries exhaust the network resources like bandwidth, computational and battery power to interrupt routing, which results in network performance degradation. For instance, in an AODV protocol, a malicious node can send large number of requests (RREQ) to a destination node that does not exist. As no node exists to reply to these requests, they flood the network. Consequently, all the node's bandwidth and battery drain up which may result in Denial of Service. The researches show that the flooding attack can decrease throughput by 84%.

A simple method projected to prevent flooding attack is, here each node keeps track of its neighboring nodes' rate of RREQs, and if this RREQ rate surpasses the predefined threshold then the ID of this neighboring node is recorded in a blacklist. Any further requests from the nodes in the blacklist are dropped. The limitation of this method is that the nodes cannot prevent the flooding attack where the flooding rate is less than the predefined threshold. Another setback of this method is that if the ID of a legitimate is impersonated by a malicious node and if it misuses the node by broadcasting RREQs, then other nodes may consider this legitimate node as malicious and add it to blacklist. As a result further requests from this legitimate node will be denied.

In another approach to prevent flooding attack was proposed to mitigate the limitations of previous method. In this approach, the threshold is set based on the statistical analysis of RREQs. Here, each node monitors the rate of RREQs sent by its neighboring nodes, if it exceeds the threshold, its requests are dropped without sending it further. The advantage of this approach is that it can prevent flooding attacks of any rate [9].

In the next model, each packet goes through a rate-limitation component which reduces the flooding attacks based on the requirement that each node has to share its bandwidth its. The list of thresholds used by the rate limiting component is as shown in the table below.

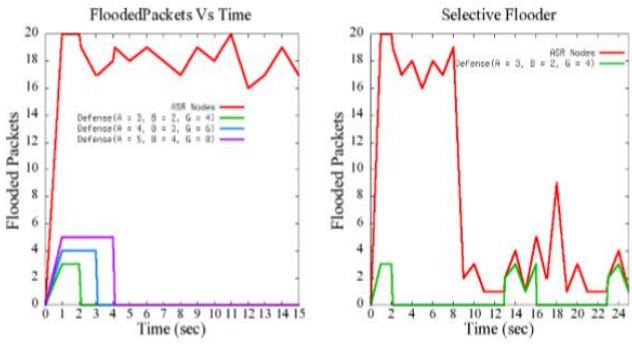

Fig. 10. Continuous and Selective flooding nodes.

If the number of packets sent by the neighbor is more than the predetermined threshold [α], then the packets are dropped. If the same neighboring node surpasses the transmission-threshold [α] by blacklist-threshold [β], then it is considered to be flooding and it is blacklisted. However, the behavior of the blacklisted node is monitored. The blacklisted node can be white listed if it continues to exhibit benign behavior for 'γ' intervals. This provides a mechanism for the blacklisted node to return to the network and makes

sure that the blacklisted node drains its resources to show that it has been repenting.

The graphical representation of continuous flooding attacks is as shown in fig. 10. In the graph 'α', 'β' and 'γ' are represented as 'A', 'B' and 'G' respectively. The graph shows that greater the value of 'β', then higher the flooded packets. After time interval 'β', the malicious nodes are reprimanded for time interval 'γ', during which their flooding behavior is monitored. If the nodes are flooding continuously then they are categorized as persistent nodes and their packets are continuously dropped. The value of 'γ' has no relevance for such nodes. Therefore it is evident that this approach isolates continuously flooding nodes and limits the flooded packets in the environment.

The graphical representation of selective flooding attacks is as shown in figure 10. As in Figure 10 (b), 'γ' is activated after the flooding nodes reduce their transmissions to 'α'. As soon as the flooding nodes transmissions are within the threshold 'α' (from 9s to 12s in Fig. 10 (b)), the packets are transmitted for the flooding nodes (from 13s to 16s in Fig. 10 (b)). But, if the flooding nodes crosses 'α' after being white-listed (at 14s and 16s in Fig. 10 (b)), then 'β' is activated to prevent flooding. However, if the transmissions are within 'α' in alternate intervals after being black-listed at 16s (from 17s to 21s in Fig. 10 (b)), then 'γ' remains insignificant. From this study, it is clear that selectively flooding nodes are considerably penalized before rejoining them to the network. From the assessment, it is recommend that the value of 'γ' must be at least twice than the value of 'β'.

The main advantage of this method is that it can effectively identify and wipe out the flooding nodes in the network. Moreover this technique provides a mean for repenting nodes to rejoin the network. This technique appears to be capable of securing MANET against flooding attacks [10].

Grayhole Attack

It is a kind of active attack where the gray hole may allow to forward all packets to certain nodes but it may also drop the packets that are going to or coming from specific nodes as given in fig 12. In this gray hole attack, for some duration the node may behave maliciously and then it will become normal later [11]. Malicious nodes do not allow particular packets to be forwarded and they drop them. Here attacker drops packets originating from single or range of IP addresses allowing remaining packets to be forwarded. In MANETs nodes of gray hole are very much effective. Each node contains routing table which stores information about next node to route the packet to a destination node.

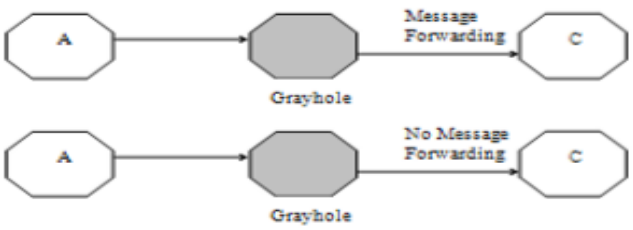

Fig. 11. Greyhole attack.

Malicious node is indirectly affecting adhoc network by damaging packet when the data transmission takes place by which network get disturbed so as to reduce the network performance. If a node is found as malicious, a notification mechanism sends messages to other nodes that are not malicious so that this malicious node can be separated and deprived of network resources. This kind of mechanism contains way of finding malicious nodes that are sequentially invoked. This kind of security procedure are invoked by a node when it recognizes a malicious node by investigating the DRI table. The node which initiates the malicious node detection process is Initiator node. The Initiator node selects Cooperative node within its neighborhood on the basis of DRI records and transmit a RREQ-message to its 1 hop neighbors asking for route to Cooperative node.

As a reply to RREQ-message Initiator node will obtain number of RREP-messages from its nearby nodes. As gray holes sends RREP-messages and drops data packets, it will receive a RREP-message from malicious node. Once after receiving RREP, Initiator node will send a packet to Cooperative Node through malicious node. After hop limit value of packet is over the Initiator node checks the Cooperative node whether packet has received. If it receives then Initiator node updates the DRI table as 1.If the packet is not reached Cooperative network, the Initiator node rise level of its suspicion about malicious node and activates the malicious node detection process. The Malicious node, Initiator node and Cooperative node is shown in fig. 11 [12].

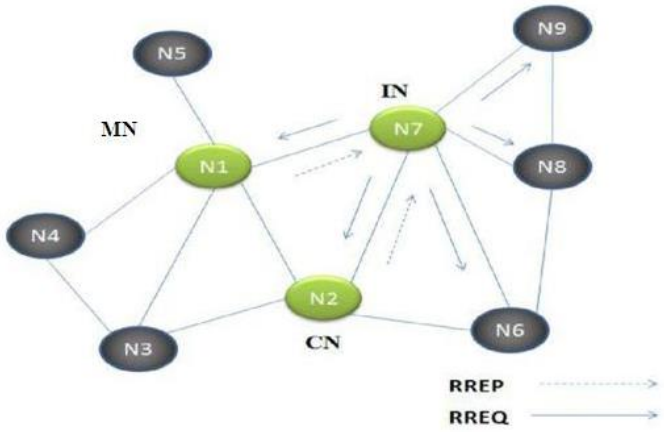

Fig. 12. Nodes after greyhole attack.

Rushing Attack

It is one of the attacks in MANETs where a targets neighbor node receives the rushed request from attacker. The neighbor node then forwards this request to the target and it does not forward any other requests through this route. Later if any non-attacking requests arrive via these nodes, the requests will be discarded. Fig. 13 shows how rushing takes place.

The rushing attack acts as effective Dos (denial of service) attack against all formerly proposed on demand adhoc network routing protocols. . The rushing attack prevention technique process diagram is given below in fig. 14.

The Steps of Prevention Technique for Rushing Attack in LGF Protocol are as follows.

i. Source node S multicast RREQ-packets to the Destination node D this is goal of an interaction of protocol.
ii. First Source node S send RREQ-packets towards S-R, S-2 and S-5 have got the RREQ-packet from Intermediate node.
iii. After receiving above these Intermediate node values to R, 2 and 5, the Rushing R attacker node values are R-3 which is malicious route immediately forwarding the RREQ-packet towards Destination node D. But the intermediate nodes, will take little time after receiving Destination node D.

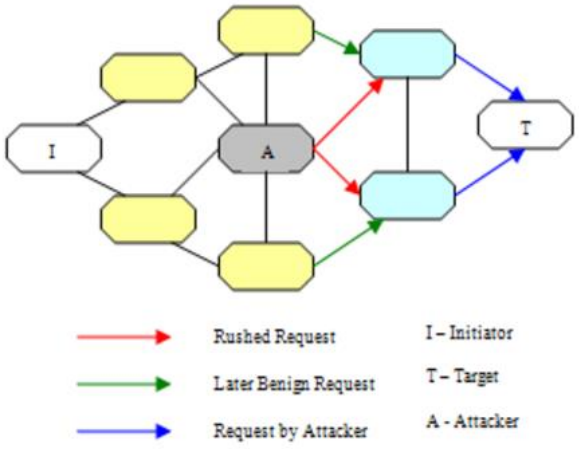

Fig. 13. Rushing attack.

iv. Then will regain the safe RREQ-packets from the rushing attacker's node. There are some preventive mechanisms they are as follows:

Assume destination node D value as 6.

Intermediate node that is near to destination node D is 6 i.e.; intermediate RREQ-packet value 6 received to Destination node is equal to destination node D value 6.

{

Accept RREQ-packet from intermediate node value 6 towards destination.

}

Else

{

Discard malicious/suspected RREQ-packets from Rushing R attacker's node from intermediate node value 3 toward destination node D.

}

v. Above condition satisfies the Destination node DRREQ-packet from intermediate node values S-5-6-D.
vi. After receiving destination node D RREQ-packet it will be sending RREP-packet from intermediate node values D-6-5-S.
vii. The source node S receives the RREP-packet from intermediate node value 5 along this route, will be chosen for sending real-time data-interaction between S-to-D.

Sybil Attack

Every node in the MANET needs a distinctive address to join in routing, through which each nodes are identified. In MANET to confirm these identities central authority are not available. An attacker, can use this belongings and can send control packets using different identities. This is known as Sybil attack. We can prevent Sybil attacks by using trusted certificates via certificate authority. In MANETS mobility can be used for identifying Sybil identities, a single node can detect this attack keeping track of identity i.e. the MAC or IP address of nodes that fear transmitting. The group of nodes which are heard together are identified as attackers that are possible. It is suggested that multiple trusted-nodes can share their observation to increase detection accuracy. Radio-resource tests of the devices could allow to detect identities of Sybil in the network which assess power and performance of various radio-resource tests including simultaneous receiver test, sender test, and forced collision test [14].

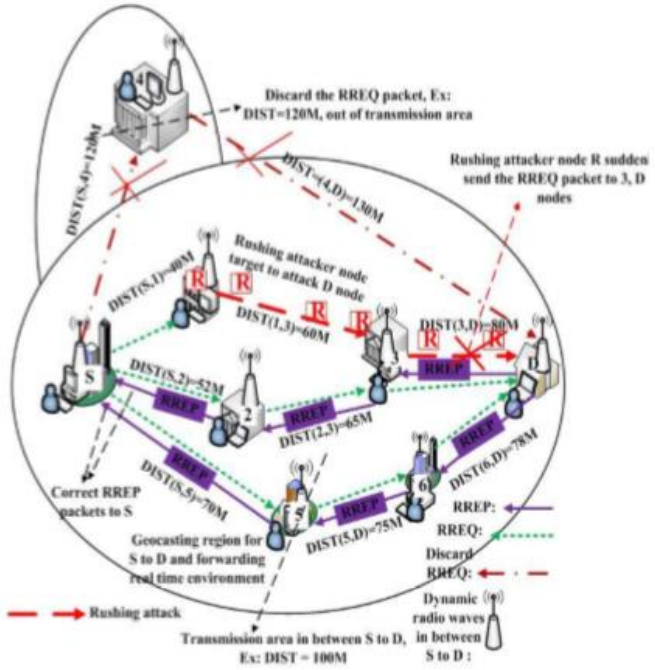

Fig. 14. DoS attack.

IV. CONCLUSION AND FUTURE WORKS

MANET is an emerging technology that gives a great insight of- anywhere, anytime and cheap communication. It has been attracting remarkable attention from researchers due to its great features where the network topology changes dynamically. In this paper we have presented some of the attacks on MANETs, their mode of function and the mechanisms used to counter these attacks.

The main drawbacks of MANET are that its resources are limited and is short of trustworthy centralized administration. Therefore the existing security solutions for wired networks cannot be applied to wireless networks. Even though some solutions proposed like cryptography seem promising, they are too expensive to be implemented in MANETs where the resources are constrained. Future work should not only be focused on providing effective solution but also focus on minimizing the cost, so that they can be easily implemented in networks like MANETs.

REFERENCES

[1] Kuriakose, Jeril, et al. "A Review on Mobile Sensor Localization." *Security in Computing and Communications*. Springer Berlin Heidelberg, 2014. 30-44.

[2] Kurkowski, Stuart, Tracy Camp, and Michael Colagrosso. "MANET simulation studies: the incredibles." *ACM SIGMOBILE Mobile Computing and Communications Review* 9.4 (2005): 50-61.

[3] Shi-Chang, Li, Yang Hao-Lan, and Zhu Qing-Sheng. "Research on MANET security architecture design." *Signal Acquisition and Processing, 2010. ICSAP'10. International Conference on*. IEEE, 2010.

[4] Kuriakose, Jeril, et al. "A Comparative Analysis of Mobile Localization and its Attacks." *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*. ACM, 2014.

[5] Kuriakose, Jeril, M. D. Lakshmi, and Afshanaaz Khan. "A Comparative Analysis of Attacks in Wireless Network." *Journal of Network Security* 2.3 (2015): 22-28.

[6] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. "RFC 3561-ad hoc on-demand distance vector (AODV) routing." *Internet RFCs* (2003): 1-38.

[7] Kuriakose, Jeril, et al. "A review on localization in wireless sensor networks."*Advances in signal processing and intelligent recognition systems*. Springer International Publishing, 2014. 599-610.

[8] Vijayalakshmi, S., and S. Albert Rabara. "Weeding Wormhole Attack in MANET Multicast Routing Using Two Novel Techniques-LP3 and NAWA2." (2011).

[9] Syed, Zeba, et al. "A novel approach to naval architecture using 1G VLAN with RSTP." *Wireless and Optical Communications Networks (WOCN), 2014 Eleventh International Conference on*. IEEE, 2014.

[10] Raju, R., et al. "A review on host vs. Network Mobility (NEMO) handoff techniques in heterogeneous network." *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on*. IEEE, 2014.

[11] Sen, Jaydip, et al. "A mechanism for detection of gray hole attack in mobile Ad Hoc networks." *Information, Communications & Signal Processing, 2007 6th International Conference on*. IEEE, 2007.

[12] Kuriakose, Cyril, et al. "Confiscation of Malicious Anchor Nodes in Wireless Sensor Networks." *Int. J. of Recent Trends in Engineering & Technology* 11 (2014).

[13] Douceur, John R. "The sybil attack." *Peer-to-peer Systems*. Springer Berlin Heidelberg, 2002. 251-260.