A Review on Classification of Attacks on Mobile Ad-hoc Network

[1]Prof. Ketki Tiwari, [2]Prof. Gaurav Mandloi, [3]Prof. Pawan K Gupta

[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor
Acropolis Institute of Research & Technology, Indore

Abstract: **Mobile ad-hoc network (MANET) is a wireless network that can transfer the information from source to destination wirelessly. Now days this network is widely used all around the world because it does not require any fixed wired network to establish communication between the source and the destination. The integral network can be established by using transmitter, receiver, processor and the battery. In today's scenario the mobile ad hoc network used in many real time applications like military surveillance, disaster management, air pollution monitoring etc. Due to the open communication media the mobile ad-hoc network has some security limitations there are the possibility of information leakage in the network. Many researchers are working on it to achieve the privacy concern. Gray-hole attack, black-hole attack, wormhole attack are the big threats in the mobile ad-hoc network. In gray-hole attack selective dropping of the packets occurs, and the information cannot be further transmitted .this research paper investigate the appropriate solutions and developed the suitable solution to prevent the network from the gray-hole attack.**

***Keywords*: MANET, AODV, Black-hole-attack, Gray-hole Attack, Wormhole Attack**

I. INTRODUCTION: A mobile Ad-hoc network (MANET) is a self-developed network of mobile nodes. It lacks any complete infrastructure like access points or base stations. It lacks centralized administration and is connected by wireless links/cables. Wireless ad hoc network can be built up where there is no support of wireless access or wired backbone is not feasible. All mobile network applications of ad hoc network are configured and created on the fly. Thus, it is necessary that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes implicit weakness. Nodes within nomadic environment with access to common radio link can easily participate to set up ad hoc infrastructure. But the assure communication among nodes requires the assure communication link to communicate. Before developing secure communication, link the node should be able enough to identify another node. As a conclusion, the node requires to provide his/her identity as well as associated credentials to another node. However, delivered identity and credentials require to be authenticated and preserved so that authenticity and integrity of delivered identity and credentials cannot be questioned by receiver node.

Every node need to be sure that delivered identity and credentials to recipient nodes are not compromised. Therefore, it is necessary to provide security architecture to secure ad-hoc networking. We found that many of the presently existing attacks have some similar features and have been classify into different attacks based on their minor differences. So hereby we are trying to classify them into two major categories: DATA traffic attacks and CONTROL traffic attacks. This will help in future designing of security measures.

II. CLASSIFICATION OF ATTACKS: As already discussed, we have classified the presently existing attacks into two broad categories: DATA traffic attacks and CONTROL traffic attacks. This categorization is based on their similar characteristics and attack goals. For example: Black-Hole attack leaves packets all time, while Gray-Hole attack also leaves packets but its action is based on two conditions: time or sender node. But from the point of network, both attacks drop packets and Gray-Hole attack can be treated as a Black-Hole attack when it starts dropping packets. So, they can be categorized under a single category. There are some attacks that have implications on both DATA & CONTROL traffic, so they cannot be classified into these categories easily. So those attacks are left for future consideration.

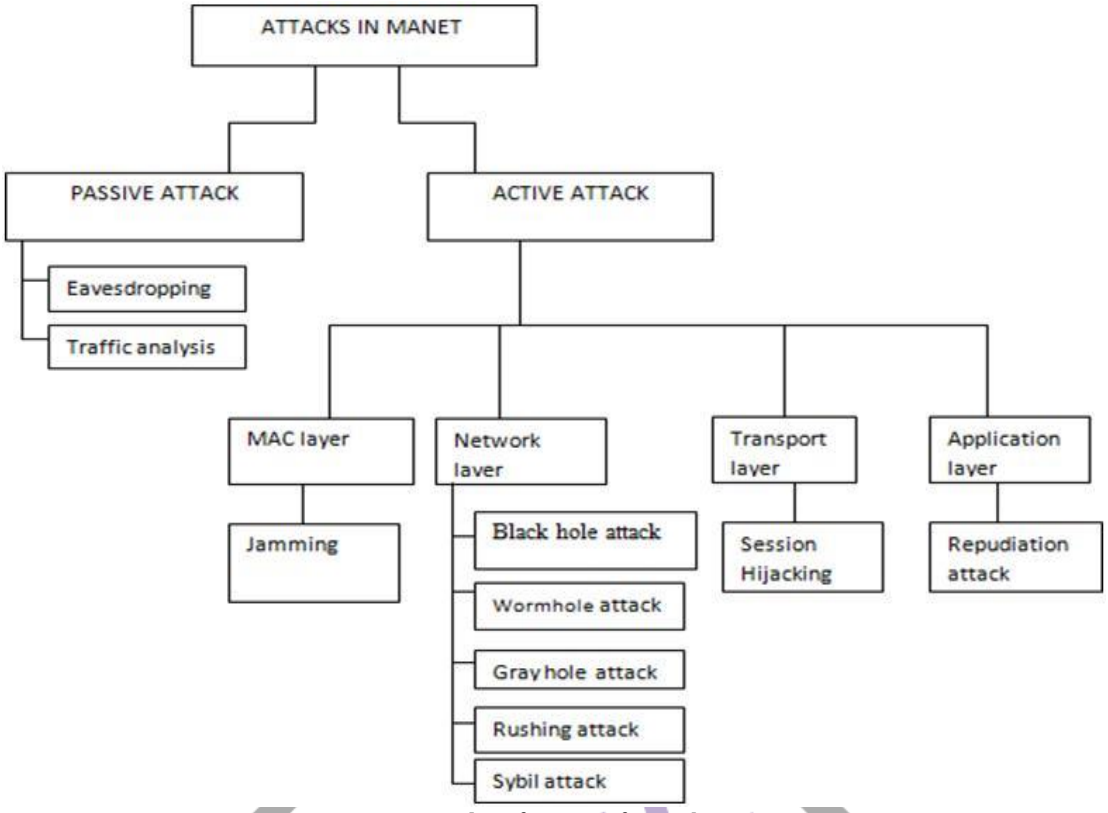

Fig1: Classification of Attacks

In MANET each device is free to move in any direction, so the links to other devices will change frequently. Here each node acts as a router. The main challenge in building MANET is that each device in it should maintain updated information to properly route traffic. Each layer in MANET is subjected to attacks. Mainly the attacks can be at two broad levels one is at routing level and other is to compromise the security mechanism used in network.

Attacks in MANET can be classified into two categories this are active attack and passive attack. In passive attack they add unauthorized listening in network and data is transferred without change. In the active attack they pull out information and they permit information flow between nodes. The active attack can be classified into four categories they are:

- **Dropping attacks**: Here data packets that are transmitted are dropped at selfish or vulnerable node.
- **Modification attacks**: In this type of attack they change the packets and interupt the communication between the nodes in the network
- **Fabrication attacks**: In this attack attacker node send fake message without getting any related message and this can be called as forge reply.
- **Timing attacks**: Here attacker attack other nodes to it by advertising itself as a node near to actual node Indicate that it is having a latest shortest path to destination.

III. ATTACKS IN MANET

MANET has five layers they are:

TABLE 1 MANET PROTOCOL STACK

APPLICATION LAYER	It defines application protocols and how host programs interact with transport layer services to use the network.
TRANSPORT LAYER	It defines the level of service and status of the connection used when transporting data.
NETWORK LAYER	It encapsulate Packages data into IP datagram and Performs routing of IP datagrams.
DATA LINK LAYER	It provides error-free transfer of data frames from one node to another
PHYSICAL LAYER	It concerned with the transmission and reception of the unstructured raw bit stream over a physical medium

Physical layer Attacks: Physical layer attack are classified in to three types, these are:
- Eavesdropping: In eavesdropping attack the attacker place themselves in communication path between sender and receiver. They extract information by receiver tuning to proper frequency.
- Jamming: It is one of the type of denial of service attack. This attack is initiated after determining the communication frequency.
- Active interference: This is also a denial of service attack which disrupt the communication. [1]

Data link layer Attacks: Data link layer also classified into three types of attack they are:
- Selfish misbehavior of nodes: These are selfish nodes that deliberately drops packet to conserve battery power or prevent undesirable share of bandwidth.
- Malicious behavior of nodes: They Disrupts behavior of routing protocol and its effect will be considerable only when more communication takes place between neighboring nodes. [1]
- Traffic Analysis: In this type of attack they examine the traffic flow to get important information on network topology that in turn reveals the information about the nodes.

Network layer: Network layer contains the following attacks they are:
- Black hole attack: In black hole attack compromised node advertises itself having shortest route to destination and thus attracts the data in the network.
- Wormhole attack: This type of attack it creates tunnel between two malicious nodes and attracts the data flow through these attacker nodes.
- Rushing attack: In this attack it floods the RREQ packet faster before another node react to the request. Thus, it attracts all the packet through the rushing attacker. [1]

Transport layer: Transport layer classified in to two types of attack they are:
- Session hijacking: In this type of attack the victims IP address is used to find the correct sequence number and causes DoS attack. There main aim is to collect secure data about the nodes.
- SYN flooding attack: In this attack, attacker create many numbers of half opened TCP connection so that handshake will not be done completely to establish connection. [1]

Application layer: Application layer is classified in to two types of attack
- Malicious code attack: It includes virus, worm, Trojan horse.
- Repudiation attack: This type of attack is caused by refusing to take part in communication. In this attack the compromised node act as, selfish node and deny the information or operation that is meant for communication [7].

- **DATA Traffic Attack**

DATA congestion attack deals either in nodes dropping data packets passing through them or in delaying of forwarding of the data packets. Some kinds of attacks choose dupe packets for dropping while some of them drop all of them regardless of sender nodes. This can highly disgrace the quality of service and increases end to end delay. This is also the reason for significant loss of important data. For e.g., a 100Mbps wireless link can behave as 1Mbps connection. Furthermore, unless there is a related path around the erratic node, some of the nodes can be unreachable from each other altogether.

- **Black-Hole Attack [1][2][3][4]**

In Black-Hole attack, a compromise node acts like a Black hole, dropping all data packets passing through it as like matter and energy vanish from our world in a black hole. If the attacking node is a connecting node of two connecting devices of that network, then it in-effect separates the network in to two disconnected devices.

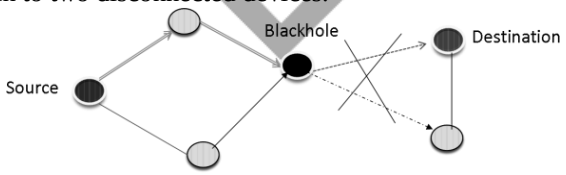

Fig 2: Black-Hole Attack

Here the Black-Hole node separates the network into two parts.
Few strategies to overcome the problem:
(i) Collecting multiple RREP messages (from more than two nodes) and thus hoping multiple similar paths to the recipient node and then buffering the packets until a safe route is found.
(ii) Sustain a table in each node with previous sequence number in increasing order. Each node before forwarding packets increment the sequence number. The sender node broadcasts RREQ to its connecting node and once this RREQ reaches the destination, it replies with a RREP with last packet sequence number. If the middle node finds that RREP contains a wrong sequence number, it knows that somewhere something went wrong.

- **Cooperative Black-Hole Attack [1][2][3]**

Cooperative is similar to Black-Hole attack, but more than one malicious node tries to interrupt the network simultaneously. It is one of the most serious DATA traffic attack and can totally interrupt the operation of an Ad-Hoc network. Mostly the only solution becomes finding substitute route to the destination, if at all exists.
Detection method is as same as ordinary Black- Hole attack.

In addition, another solution is ensure routing and node discovery in MANET by any desirable protocol such as SAODV, SNRP, SND, SRDP etc. Since every node is already trusted, black hole node should not be appearing in the network.

- **Gray-Hole Attack**

Gray-Hole attack has its own characteristic behavior. It also drops DATA packets, but node's suspicious activity is limited to certain conditions or trigger. There are two most common type of behavior:
(i) Node dependent attack – In this it drops DATA packets destined towards a certain victim node or coming from certain node (fig 3), while for some other nodes it behaves normally by routing DATA packets to the destination nodes correctly.
(ii) Time dependent attack – In this it drops DATA packets based on some predetermined/trigger time while behaving normally during the other instances. (fig. 4)
Detecting this behaviorist attack it is very hard unless there exists a system wide detection algorithm, which takes care of all the nodes performance in the network. Sometimes nodes can interact with each other and can advise compromised nodes existence to other friendly nodes. This approach is similar to Black- Hole attack where sequence number feedback might detect some Gray-Hole attack. If number of paths exist between sender and destination then buffering packets with proper acknowledgement (for e.g. 2ACK [14]) might detect active Gray-Hole attack in progress. But dormant or triggered attack is very difficult to detect with this approach.

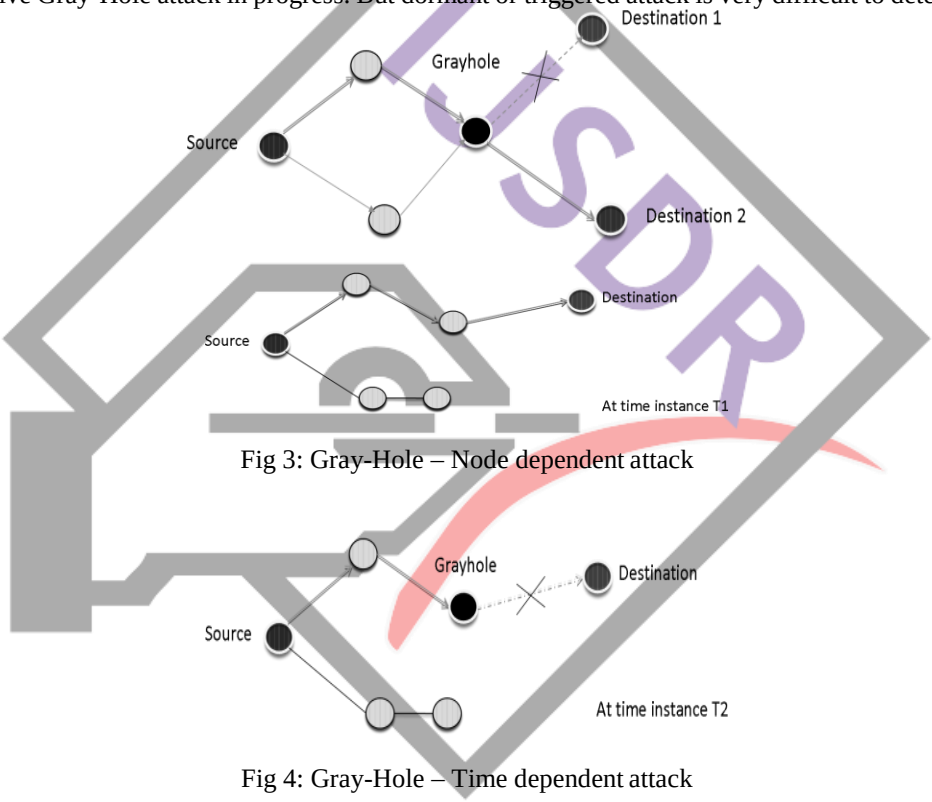

Fig 3: Gray-Hole – Node dependent attack

Fig 4: Gray-Hole – Time dependent attack

- **Jellyfish Attack**

Jellyfish attack is different from Black-Hole & Gray-Hole attack. Instead of blindly dropping the data packets, it holds them before finally delivering them. It may even change the order of packets in which they are received and sends it in random order. This interrupts the normal flow control mechanism used by nodes for reliable transmission. Jellyfish attack can result in substantial end to end delay and thereby degrading QoS. Few of the methods used by attacker in this attack:
(i) One of the methods is changing the packet order before finally delivering them instead of received FIFO order. ACK based flow control mechanism will yield duplicate ACK packets which will unnecessarily consume precious network bandwidth and battery life.
(ii) Other method can be, performing selective Black-Hole attack by dropping all packets at every RTO. So it will cause timeout in sender node at every RTO for that duration. If nodes use traffic shaping, default flow control mechanism might be triggered to the sender node as it is similar as destination overwhelm.
(iii) In this method the attacking node can contain all the received packets in its buffer but sends them after some random delay maintaining the received packet order. Here also the flow control mechanism gets confused. Sometimes the source node may take a longer route instead of the most obvious shortest route.

Few of the solutions to Jellyfish type attack includes:

(i) 2ACK [14] : The idea of the 2ACK scheme is that, when a node forwards a data packet successfully over the next hop, the recipient node of the next-hop link will send back a special two-hop acknowledgment called 2ACK to indicate that the data packet has been received successfully. This type of 2ACK transmission takes place for only a fraction of data packets, but not for all.
(ii) Credit based systems [12]: This method provides motivation for successful transmission of some kind of token or credit which the node might use when it starts sending its own packet.
(iii) Reputation based scheme [2]: In this approach individual nodes collectively detect misbehaving nodes (such as CONFIDANT).

- **CONTROL Traffic Attack**

Mobile Ad-Hoc Network (MANET) is inherently vulnerable to attack because of its fundamental characteristics, such as open medium, distributed nodes, autonomy of nodes participation in network (nodes can join and left the network on its will), lack of centralized authority which can impose security on the network, distributed co-ordination and cooperation. The existing routing protocols cannot be used in MANET because of these reasons.
Most of the routing protocols formulate for use in MANET have their individual characteristic and rules. The most widely used routing protocols are Ad-Hoc On-Demand Distance Vector routing protocol (AODV), which relies on individual node's cooperation in establishing a valid routing table and Dynamic MANET On-Demand routing protocol (DYMO), which is a fast light weight routing protocol devised for multi hop networks. But both protocols are based on trust on nodes participating in network. The first step in any successful attack requires the node to be part of that network. As there is no protocol in joining the network, suspicious node can join and disrupts the network by hijacking the routing tables or bypassing valid routes. It can also eavesdrop on the network if the node can establish itself as the shortest route to any recipient by exploiting the unsecure routing protocols. Thus, it is of utmost importance that the routing protocol should be as much secure as it can be.
Though there can be some other kinds of attack, such as jamming attacks, which is not CONTROL attack. They can be handled as a part of physical layer security protocols. Henceforth those attacks will not be discussed as are out of scope of this paper.

- **Worm Hole Attack**

Worm hole attack, in cosmological term, connects two distant points in space via a shortcut route. In the same manner in MANET also one or more attacking node can interrupt routing by short- circuiting the network, thereby disrupting usual flow of packets. If this link becomes the lowest cost path to the destination then these compromised nodes will always be chosen while sending packets to that destination. The attacking node then can either eavesdrop the traffic or can even disrupt the flow (via one of the DATA traffic attack). Wormhole attack can be done with single node also but generally two or more suspicious node connects via a wormhole-link. In figure 5, Node X and Node Y performing wormhole attack.
There have been few proposals recently to protect networks from worm-hole attack:
(i) Geographical leashes & temporal leashes: A leash is added to each packet in order to confine the distance the packets are allowed to travel. A leash is associated with each hop. Therefore, each transmission of a packet requires a new leash. A geographical leash is intended to limit the distance between the transmitter and the receiver of a packet. A temporal leash provides an upper bound on the lifetime of a packet.
(ii) Using directional antenna: Using directional antenna confine the direction of signal propagation through air. This is one of the crude ways of limiting packet dispersion.

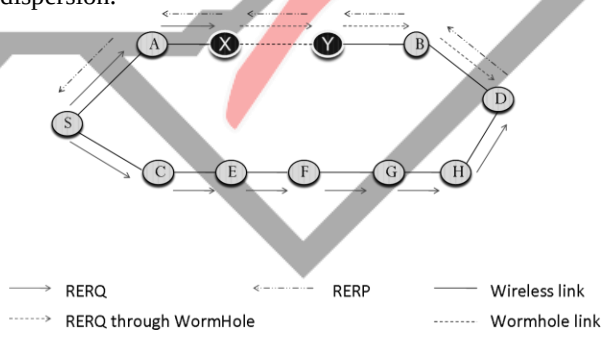

Fig 5: Worm-Hole attack

- **HELLO Flood Attack**

The malicious node floods the network with a high-quality route with a powerful transmitter. So, each node can forward their packets towards this node hoping it to be a better route to destination. Some of them can forward packets for those destinations which are out of the reach of the attacker node. A single high-power transmitter can convince that all the other nodes are his neighbor. The malicious node need not generate a legitimate traffic; it can just perform a selective replay attack as its power overwhelms other transceivers.

- **Bogus Registration Attack**

In Bogus registration attack the attacker pretend itself as another node either by sending stolen beacon or generating such false beacons to register himself with a node as a neighbor. Once registered, it can snoop transmitted packets or may interrupt the network altogether. But this type of attack is hard to achieve as the attacker needs to intimately know the masquerading nodes identity and

network topology. Encrypting packets before sending and secure authentication in route discovery (SRDP, SND, SNRP, ARAN, etc.) will decrease the severity of attack to some extent as malicious node has no previous knowledge of encryption method.

- **Man in Middle Attack [3]**

In Man in Middle attack, the suspicious node creeps into a valid route and tries to sniff packets flowing through it. To execute man in middle attack, the attacker first needs to be part of that route. It can do that by either temporarily interrupting the route by deregistering a node by sending suspicious disassociation beacon captured previously or registering itself in next route timeout event. Simple way of protecting packets flowing through MANET from prying eyes is encrypting each packet. Though key distribution becomes a security issue.

- **Rushing Attack**

In AODV or related protocol, each and every node before transmitting its data, first establishes a valid route to destination. Source node broadcasts a RREQ (route request) message in neighborhood and valid routes replies with RREP (route reply) with proper route information. Some of the protocols use duplicate suppression method to limit the route request and reply chatter in the network. Rushing attack exploits this duplicate suppression method. Rushing attacker quickly forwards with a suspicious RREP on place of some other node skipping any proper processing. Due to duplicate suppression, valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, malicious node does send packets to proper node after its own filtering is done, so from outside the network behaves normally as if nothing happened. But it might increase the delay in packet delivering to recipient node.

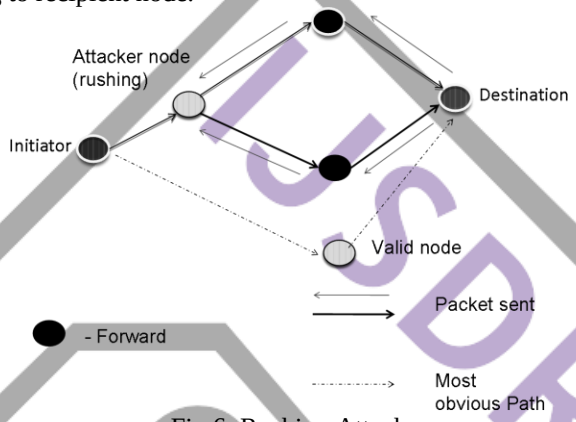

Fig 6: Rushing Attack

Few of the protocols that may help in resolving Rushing attack:
SEDYMO [24]: Secured Dynamic MANET On-Demand is as same as to DYMO but it dictates intermediate node must add routing information while broadcasting the routing messages and no intermediate node should delete any routing information from previous source node while broadcasting. It also adds hash chains and digital signature to protect the identity.
(i) SRDP [13]: Secure Route Discovery Protocol is security enhanced Dynamic Source routing (DSR) protocol.
(ii) SND [13]: Secure Neighbor Detection is another method of confirming each neighbor's identity within a maximum transmission range.

- **Cache Poisoning Attack**

Generally, in AODV, each node contains few of its most recent transmission routes until timeout occurs for each entry. So, every route halts for some time in node's memory. If some attacker node performs a routing attack then they will stay in node's route table until timeout occurs or a better route is found. A malicious node can advertise a zero metric to all of its destinations. Such route will not be rewritten unless timeout occurs. It can even advertise itself as a route to a node which is out of its reach. Once it becomes a part of the route, the malicious node can perform its malicious activity. Effect of Cache poisoning can be reduce by either adding boundary leashes or by token authentication. Also, every node can maintain its friend-foe list based on historical statistics of neighboring nodes performance.
Some of the mitigation methods proposed:
(i) SAODV [9]: Secure AODV is an extension to AODV protocol that includes each node to exchange signed routing messages. Every node has its own public key which it uses to sign routing messages. Also, SAODV uses hop count as a metric for shortest-route as AODV and uses hash chains to protect hop count information in route messages.
(i) ARAN : Authenticated Routing protocol for Ad-hoc Networks uses same techniques as SAODV. ARAN uses certificates issued by a third-party certification authority.
(ii) SNRP [6]: Secure Neighbor Routing protocol uses security enhanced Neighbor Lookup Protocol (NLP) to secure routing in MANET. Newly added node uses public key to participate in MANET.

- **Blackmailing and Co-operative Blackmailing Attack**

In a blackmailing attack or co-operative blackmailing attack, malicious nodes impeach an innocent node as harmful node. This attack can effectively be done on those scattered protocols that establish a good and bad node list based on review of participating

nodes in MANET. Some of the protocols effort to make them more secure by using majority voting principle, but still if enugh no. of malicious nodes becomes part of the MANET it can bypass that security also.
Another method of this attack will be, sending invalid RREP messages with advertising an unnecessarily high cost to certain nodes.
Some Known mitigation techniques:
(i) Dynamic Trust based, Distributed IDs [2]: As we know that MANET routing is a co-operative process, while building a route every node must evaluate its neighbor nodes. This method builds a distributed trust relationship and maintain dynamic trust information. As the trust is part of a long chain, single suspicious node cannot victimize an innocent node easily.
(i) Friend List based [2]: Another solution will be building a friend list of trusted nodes. Nodes identity must be dictated by the user who created the MANET. Therefore, it becomes a closed system of trusted nodes.

- **Sybil Attack**

Sybil attack certifies itself by faking multiple identities by pretending to be comprised of multiple nodes in the network. So, one single node can assume the role of multiple nodes and can supervise or hamper multiple nodes at a time. If Sybil attack is performed over a blackmailing attack, then level of interruption can be quite high. In Sybil attack success depends on how the identities are generated in the system.

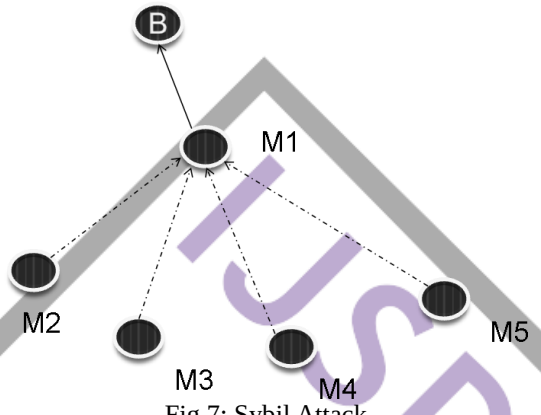

Fig 7: Sybil Attack

In figure 7, node M1 acquires identities of M2, M3, M4, and M5. So, for node B, M1 is equivalent to those nodes. One way of mitigating this attack is keeping a chain of trust, so single identity is generated by a hierarchical structure which may be hard to forge.

IV. CONCLUSION

We have tried to categorize the different categories of ad-hoc security attacks entirely based on their characteristics to considerably slow down the mitigation period. By bringing the attacks under these two broad categories the complicacy of naming also mitigate. We have also kept a close look on the already available algorithms needed to reduce the attacks and have tried to bind the attacks into categories according to that.
Few attacks have some characteristics which make them inapplicable to be categorized into these categories, so they have been kept away from this topic of discussion for the time being.
Further study is in progress to uncover more common characteristics of the attacks to more strongly bind them into these categories and to competently design more powerful algorithm in mitigating DATA and CONTROL traffic attacks.

REFERENCES

[1]. S. marti, T.Guili, K. Lai, & M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks”, In proceedings of MOBICOM 2000.
[2]. H. Yang, J. Shu, X. Meng, and S. Lu, “SCAN: Self-organized network-layer security in mobile ad hoc networks,” IEEE Journal on Selected Areas in Communications, February 2006.
[3]. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. “Prevention of cooperative black hole attack in wireless ad-hoc networks” In Proceedings of 2003 International Conference on Wireless Networks (ICWN’03).
[4]. Piyush Agrawal, R. K. Ghosh, Sajal K. Das, “Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks” In Proceedings of the 2nd international conference on Ubiquitous information management and communication, 2008.
[5]. A. Nadeem, M.Howarth “ Protection of MANETs from a range of attacks using an intrusion detection & prevention system” published in Springer science + Business Media in 2011.
[6]. H. Deng, H. Li, and D.P. Agrawal, “Routing security in wireless ad hoc networks,” IEEE Communications Magazine, October 2002.
[7]. M. Jackobsson, J. Hubaux, and L. Buttyan, “A micro-payment scheme encouraging collaboration in multi-hop cellular networks,” In Proceedings of Financial Crypto 2003.
[8]. Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., & Tolle, J., “Detecting black hole attack in tactical MANETs using topology graph” In Proceeding of 32nd IEEE conference on local computer networks 2007.
[9]. V. Solomon Abel, “Survey of Attacks on Mobile Ad- Hoc Network” IJCSE, Vol.3, No.2, Feb 2011.

[10]. M. Wazid, Rajesh Kumar Singh, R.H.Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad- Hoc Network & Some available Detection Techniques" IJCA , Vol.3, No,2 Feb 2011.
[11]. D. Manikantan shila, Yu Cheng , Tricha Anjali "Mitigating selective forwarding attacks with a Channel aware detection Approach in WMNS" IEEE Transactions on Wireless communications Vol.9, No.5, May 2010.
[12]. A.Saini, R. Sharma, "A Study of various Security Attacks & their countermeasures in MANET" IJARCSSE, vol.1, Issue.1, Dec 2011.
[13]. G.S Mamatha, Dr.S.C. Sharma "Network layer attacks and defense mechanism in MANETS- A Survey" IJCA Nov 2010.
[14]. Dhamande C.S and Deshmukh H.R "A Competent to diminish the brunt of gay hole attack in MANET" Vol.2, Issue 2 Mar 2012.
[15]. Pradip M. Jawandhiya, Mangesh m.ghonge, DR. M.S Ali and Prof. J.S Deshpande " A Survey of Mobile adhoc network attacks" Vol.2, No.9, Sep 2010.