Classification of Attacks in Mantes

Shamikh Faraz

Abstract— **Mobile ad -hoc network (MANET) is an independent network which consists of many nodes and these nodes use wireless links to communicate with each other. A mobile ad hoc network due to its open nature, dynamically changing topology, lack of infrastructure and central management is vulnerable to various attacks. There is an attack which causes many serious threats to the network and it is known as Sybil attack. In other words a 'Sybil attack' in network security is an attack wherein a reputation system is subverted by forging identities in peer to peer network. In this, attackers use many identities or IP addresses to gain control over the network and creates lots of misconception among nodes present in the network. Malicious attackers can create multiple identities and influence the working of systems that rely upon open membership. Examples of such systems range from communication systems like email and instant messaging to collaborative content rating, recommendation and delivery systems.**

Index Terms—Sybil attacks, Sybil Attack Detection mechanism, prevention techniques for Sybil attacks, Mobile Ad-hoc Network (MANETs).

I. INTRODUCTION

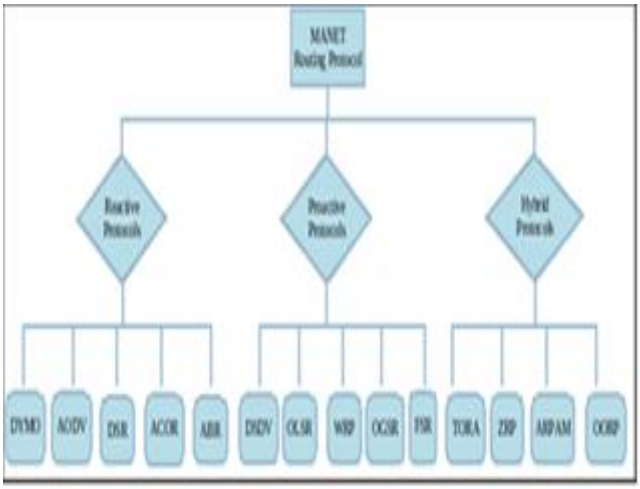
A collaborative attack in MANET is a *homogeneous* attack (i.e. black-hole or wormhole attack), involving *two or more* colluding nodes; classified as internal active attack that can be processed using wired or wireless link and triggered by single or multiple attackers. It can also be referred to as the first level of attack, in which the adversary only interests in disrupting the foundation mechanism of the ad hoc network, for instance routing protocol, which is crucial for proper MANET operation. In collaborative attacks, there are numerous nodes involved during the attack. These nodes can be physically existent or not existing at all.

II. CLASSIFIED ATTACKS ON THE BASIS OF LAYERS

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing.

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
- Physical: Interference, Traffic Jamming, Eavesdropping.

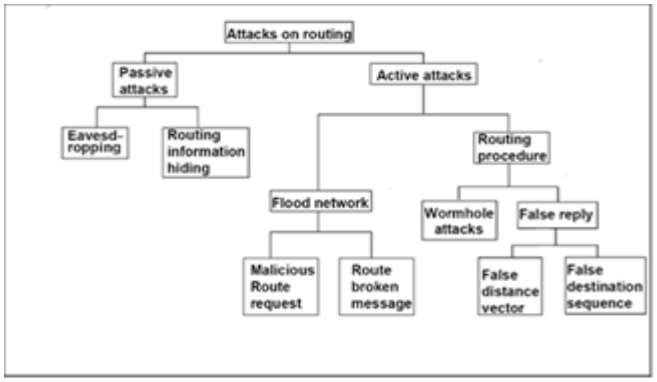
The mobile nature of nodes, limited bandwidth, high error rates, limited battery power and continuously changing topology brings out new complexities while designing the routing protocols for this kind of network. The conventional routing protocols need to be refurbished or modified, in order to compensate the MANETs mobility and to provide efficient functionality. A number of routing protocols have been proposed by a number of researchers that can be classified into proactive, reactive and hybrid. Proactive protocols are also called table driven protocols in which each node maintains the routing information of other nodes in the network, through regular exchange of network topology packets. In reactive routing protocols, the packets are flooded into network to discover the routes, on demand. Hybrid protocols are the combination of both proactive and reactive protocols.



MANET routing protocol

Moreover, due to distributed nature of this network, the centralized security control is hard to implement. These characteristics of MANET pose both challenges and opportunities in achieving the security goals, such as confidentiality, authentication, integrity, availability, access control and non-repudiation. There are a wide variety of attacks that target the weakness of MANET routing protocols. Most sophisticated and subtle routing attacks have been identified in some recently published papers such as Black-hole, Rushing, Byzantine, wormhole and Sybil attack etc.

Manuscript received April 24, 2015.
Shamikh Faraz, M. Tech CSE. Final sem./ Uttrakhand Technical University,Dehradun, Utrakhand, India,



III. COLOBORATIVE ATTACKS

Practically, MANET could be attacked by several ways using multiple methods; before going to deeper investigation, it is necessary to classify security attacks within the context of MANET. The classification can be based on the behavior of the attack (Passive vs. Active), the source of the attacks (Internal vs. External), the processing capacity of the attackers (Wired vs. Mobile) and the number of the attackers (Single vs. Multiple). I choose these attack classifications because they are applicable to the collaborative attacks are categorizing.

A. Passive vs. Active attack

Typically, passive attacks aim to steal valuable information in at least two communicating nodes or even in the whole network. There are many variations of passive attacks, but in MANET, there exist two types: eavesdropping and traffic analysis. Practically, depending on situations, passive attacks can be considered as legitimate or illegitimate actions. If the purpose is benign, for example, if the administrator wants to use some tools to probe the network traffic, in order to troubleshoot or account the network then it is legitimate. On the contrary, if the purpose is malicious, one attacker can steal valuable information by probing the network traffic such as credit card information, credential email, and then use the information to illegally withdraw money from bank accounts or blackmail the victims. Roughly speaking, passive attacks do not intend to disrupt the operation of the particular network, but active attacks are able to alter the normal network operation. Typical example of active attacks can be: masquerade attack, replay attack, modification of message.

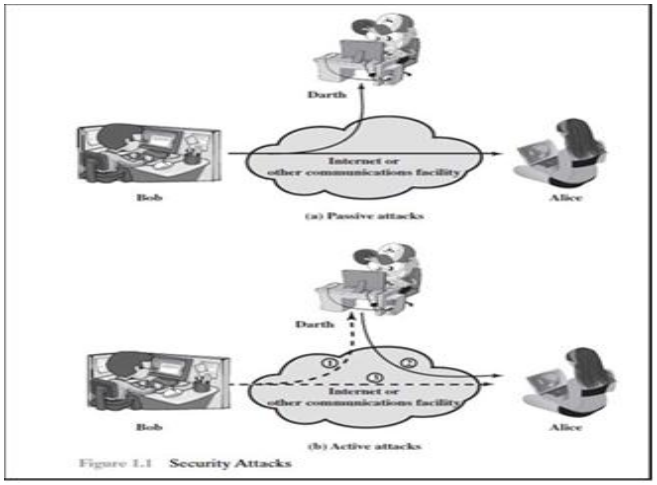
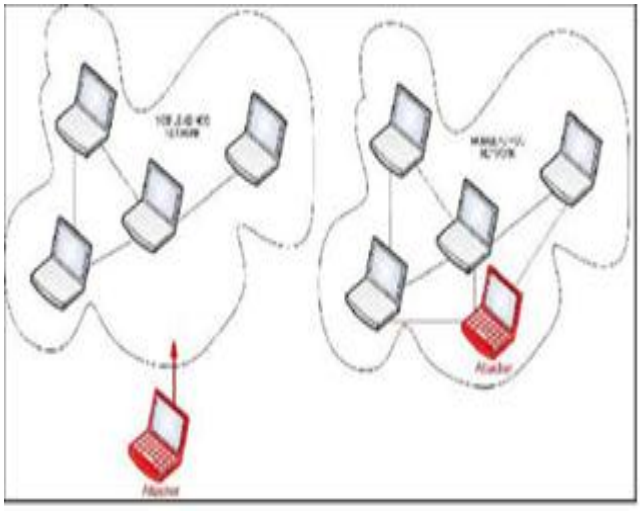
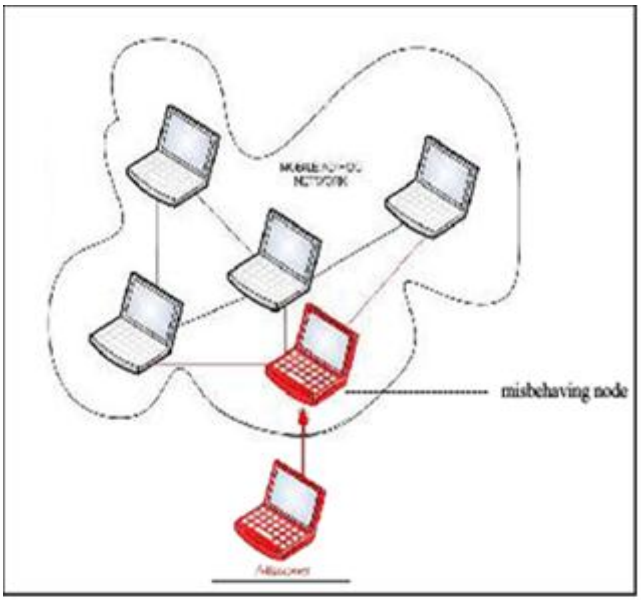


Figure 1.1 Security Attacks

B. Internal vs. External attack

As the name implies, external attacks are launched by attackers who physically stay on outside of the attacked network. These attacks usually aim to deny access to specific function in the network (i.e. http traffic), or to cause network congestion or even to disrupt the whole network. While external attacks would be difficult to be launched if the network was properly configured and protected, the internal attacks are much tougher to defend against. One of the reasons is because we tend to protect the network from being attacked by outsiders rather than insiders. Also because of the fact that an external attack can easily be traced compared to the internal attack.


I
nternal vs. External attacks



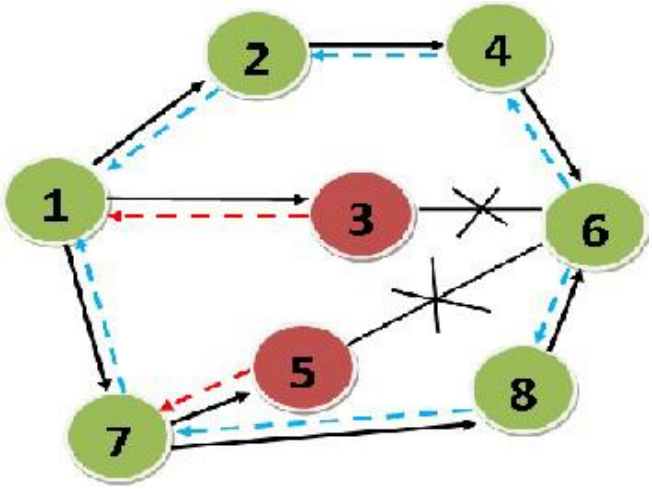
IV. HOMOGENIOUS ATTACK

A homogeneous attack in MANET is a black hole or wormhole attack with the involvement of *two or more* colluding nodes that can be processed using wired or wireless link and triggered by single or multiple attackers. It can also be referred to as the first level of attack, in which the adversary only interests in disrupting the foundation

mechanism of the ad hoc network, for instance routing protocol, which is crucial for proper MANET operation.

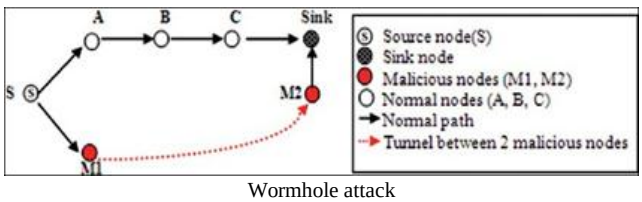
A. *Direct Homogeneous Attacks*

Here, the attacker nodes are already in existence in the original network or a malicious node joins the network or an internal node is compromised in the network. This kind of collaborative attacks can be referred to as direct homogeneous attacks. Black hole and Wormhole attacks belong to this category. The reason for this classification is based on the behavior of these attacks. In the black hole attack, one or more malicious nodes try to disrupt the network routing operation by advertising itself as the shortest path to the destination node. Therefore, there will be at least three physical nodes must be involved in this attack, namely: the source node, black hole node (malicious node) and the destination node.



Direct Homogeneous Attacks with the involvement of two or more colluding nodes

Node 1 wants to send data packets to Node 6; it will first broadcast the RREQ (Route Request) to the neighbouring nodes. Node 3 and 5 are black hole nodes and then also received RREQ from source node. These malicious nodes will immediately send out the RREP (Route Reply) to claim that it is the shortest path to destination node 5. The RREP from 3 and 5 will reach the source node before other nodes, thus the source node 1 start transmitting data packets. On the receipt of data packets, 3 can either simply drop them or forward them to 5, and then 5 may simply drop or forward the data packets. Finally, little or no data packet can reach the intended destination node 6.



Wormhole attack

The second attack belonging to this category is the wormhole attack; there always exists two colluding malicious nodes, since they can tunnel data packets back and forth even packets not addressed to them without being known by other nodes. Thus, the wormhole attack involves at least two physical nodes. In Figure, two malicious colluding nodes M1 and M2 can tunnel data packets to each other to analyze and tamper the network by using either a wired link or a long-range wireless medium.

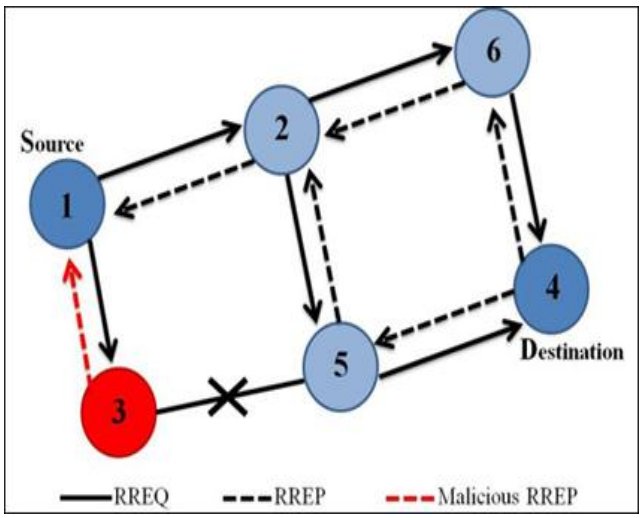
B. *Indirect Homogeneous Attacks*

The attacks in this category use different non-existent nodes in order to fake other nodes to redirect data packets to malicious node. This kind of collaborative attacks can be referred to as indirect collaborative attacks. The attacker nodes are not already in existence in the original network but created along the line of their attack. Sybil attack belongs to this category of collaborative attacks. The malicious node in Sybil can generate arbitrary number of additional identities for itself while using only one physical node. This physical node may be a legitimate node or an already compromised or malicious node by Sybil attack in the MANET. Routing table overflow is another attack in this category in which the malicious node tries to create as much as possible routes to non-existent nodes. It aims to prevent new routes from being produced or to overpower the routing protocol.

V. MULTIPLE NODE ATTACK

A. *Black hole attack*

A black hole attack occurs when a malicious node impersonates the destination node or forging route reply message that is sent to the source node, with no effective route to the destination. The malicious node may generate unwanted traffics and usually discards packets received in the network. When this malicious node (black hole node) has effects on one or more nodes, making them malicious as well, then this kind of attack can be referred to as multiple node attack or collaborative attack. In a black hole attack, the malicious node presents itself as having the shortest path to the node it is impersonating, making it easier to intercept the message. To achieve this, the malicious node waits and tries to get the replies from nearby nodes in order to discover a safe and valid route. This route could be forged, illegitimate or an imitation but it appears genuine to the source node.



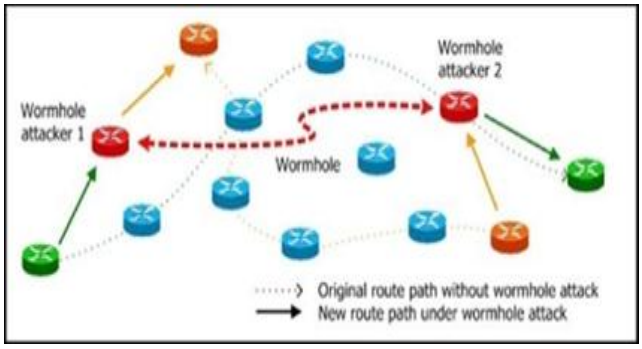
Single node black hole attack

Above figure is an example of single node black hole attack in the mobile ad hoc networks. Node 1 stands for the

source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. In the mobile ad hoc networks, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem

B. *Wormhole attack*

A wormhole attack is an attack in which the attacker provides two choke-points that are used to degrade the network or analyze traffic as preferred any time. False impressions are used in creating these choke-points with two or more nodes joint together. In other words, wormhole attack creates a tunnel that records traffic data (in bits or packets) at one network place and channels them to another place in the network. This kind of attack is usually against many ad hoc routing protocols and the attacker is hidden at higher layers; thus the wormhole and both colluding attacker nodes at each choke-point of the wormhole are invisible in the MANET route. There are different adaptations of wormhole attack where in-band and out-of-band wormholes are the two main variations.



Worm-hole attack

C. *In-band Wormhole*

This method of wormhole attack builds up a secret overlay tunnel within the active wireless medium. In-band wormhole could be more dangerous than out-of-band wormhole because it does not have any need for an extra hardware device or node and it also utilizes the existing communication medium in its routing. Self contained wormhole and extended in-band wormhole are two types of in-band wormhole. The self-contained wormhole promotes a false link connecting the attacker nodes while the extended in-band wormhole promotes its fake link between two nodes, which are none attacker nodes. The latter type produces a wormhole that goes further than the attacker nodes, thus creating the end choke-points.

D. *Out-of-band Wormhole*

In this variation of wormhole, the attacker nodes create a direct connection linking the two choke-points. This established link is an external link that could be wired or a kind of wireless medium. One end of the connection is used to accept packets while it is forwarded using the second end of the connection, thus giving room for huge amount of data to be transmitted through the wormhole.

E. *Routing table overflow attack*

This is the kind of multiple node attack that sends non-existent node data into the MANET and also tries to degrade the rate at which new updates are made into the routing table [26]. This kind of attack is aimed at flooding or disrupting the routing node of the victim with non-existent node data and it usually occurs against proactive routing protocols like OSPF and OLSR. Proactive routing protocols use periodic updates of routes even before they are required to transpire and this make them vulnerable to routing table attack. On the contrary, reactive routing protocols only produce a route when it is required, thus it is not vulnerable to routing table overflow attack.

F. *Sybil attack*

A Sybil attack is a situation where a malicious node acts like two or more nodes rather than just a node like previously mentioned attacks. The Sybil nodes are created by series of false identities, imitations, or impersonation of nodes in a MANET, and these additional node identities could be generated by just a physical device. There exist three proportions of launching a Sybil attack.

VI. Conclusion

Studies on MANET have focused more on single attacks. In the meanwhile some attacks involving multiple nodes have received little attention since they are unanticipated and combined attacks. There have been no proper definition and categorization of these kinds of attacks (multiple node attacks) in MANET. Some mitigation plans have been proposed to counteract against some form of multiple node attacks; thus, there is need to figure out the consequences of the category of collaborative attacks and their possible mitigation plans. Moreover, the effects of these kinds of attacks on MANET have not been well measured since each researcher tends to use different simulators to visualize those attacks and determine the consequences such as impact on packet delivery ratio, throughput, and end-to end delay

Acknowledgment

I am thankful to my parents and friends, without their moral support this paper would not be possible in real. Also I am indebted to all who have contributed directly and indirectly in this paper.

References

[1] K. Gopalakrishnan & Rhymend Uthariaraj, in V.. 2011, “Neighborhood Monitoring Based Collaborative Alert Mechanism to Thwart the Misbehaving Nodes in Mobile Ad-Hoc Network ”, European Journal of Scientific Research ISSN 1450-216X Vol.57 No.3 pp.411-425.

[2] Marti, S., Giuli, TJ., Lai, K., Baker, M., 2000. “Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks”, *In: 6th International*

Conference on Mobile Computing and Networking, pp.255-265. ACM, Boston.

[3] Nguyen Tran, Combating Sybil attacks in cooperative systems, Department of Computer Science, Courant Institute of Mathematical Sciences, New York University, Sep 2012,

[4] G. Kesidis, A. Tangpong, C. Griffin, "A Sybil-proof Referal System Based on Multiplicative Reputation Chains, IEEE Communication Letters, 2009.

[5] Douceur, J. R. (2002) "The Sybil Attack," in *Proc. IPTPS*, Cambridge, MA.

[6] Priyanka Goyal, Vinti Parmar and Rahul Rishi, *"MANET: Vulnerabilities, Challenges, Attacks, Application",* IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[7] Mohammad Wazid , Rajesh Kumar Singh and R. H. Goudar, *"A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques "* International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011.

[8] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao " *A survey of black hole attacks in wireless mobile ad hoc networks"* Human-centric Computing and Information Sciences 2011.

[9] J. Kong, X. Hong and M. Gerla, "A new set of passive routing attacks in Mobile ad hoc networks", Proc. IEEE Military Communication conference MILCOM, OCT. 2003

Shamikh Faraz has dons done MCA from U.P. technical university, Lucknow. Now he is pursuing M. Tech in computer Science & engineering from Uttrakhand technical university, Dehradun. He got published two international papers in international journal and conference and some national papers in national seminars and conferences.