Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review Paper on Security Challenges and Attacks in Mobile Ad-Hoc Networks

Jasleen Kaur
M.Tech CSE Department
Geeta Engineering College

Shakti Nagpal
HOD, CSE Department
Geeta Engineering College

Abstract- Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead hosts rely on each other to keep the network connected. The military tactical and other security sensitive operations are the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. In particular, we take advantage of the inherent redundancy in ad hoc networks — multiple routes between nodes — to defend routing against denial of service attacks. A literature study related to various types of attacks in ad hoc network has been carried out. To develop suitable security solutions for such environments, this paper provides a comprehensive study of attacks against mobile ad hoc networks and detailed classification of the attacks against MANETs.

Keywords: Ad-Hoc Network, Security Goals, Active Attacks, Passive Attacks, DATA traffic attacks and CONTROL traffic attacks

I. INTRODUCTION

A wireless ad hoc network is a decentralized network. The network is ad hoc because it does not have pre existing infrastructure. In this each node is participating for forwarding data to other nodes, to determine which nodes forwards data is dynamic on the basis of network connectivity. An ad hoc network is a set of networks where all devices are free to associate with any other ad -hoc network devices within range. Ad hoc network often refers to a mode of operation of IEEE 802.11wireless networks. An ad-hoc network is a type of peer to peer wireless network mode where devices directly communicate with each other, without any Wireless Access Point (WAP) device. Wireless networks typically depend on a base station or WAP device to manage or direct the data stream between wireless devices. These devices should be within close range of each other; however quality of connection and speed of the network will suffer as more and more devices are added to the network.

A. Types of ad-hoc networks

The self supporting nature of ad-hoc networks makes them quite useful in situations such as natural disasters, emergency military operations, or even to just quickly transfer information between two computers at home. The types of ad hoc networks are as follows:

- Mobile ad hoc networks

A mobile ad hoc network (MANET) is a self forming network of mobile devices connected wirelessly.

- Wireless mesh networks

A wireless mesh network (WMN) is a communications network of radio nodes structured in a mesh topology. The clients within the network are usually laptops, mobile phones, and other wireless equipment. In mesh network with the help of routers and gateways we can transmits data to and from the wireless devices. The communication is within the mesh and not to the internet Wireless sensor networks. A wireless sensor network (WSN) employs sensor based devices to jointly observe physical or environmental settings such as sound, pressure, climatic changes, and so on. Wireless sensor networks are used in a wide range of areas: traffic control, vehicle detection, greenhouse monitoring and so on.

II. SECURITY ANALYSIS

A. Mode of behavior in ad-hoc network

In this section, we analyze the security in the ad hoc networks based on their mode of behavior.
In the ad hoc networks, mobile nodes within each other's radio range communicate directly via wireless link using a protocol such as IEEE 802.11 [1] or Bluetooth [2], while those far apart rely on other nodes to relay messages as routers. Due to the mobility of the nodes, the network topology is frequently changed. Figure 1 shows an example. The original network topology is shown in (a) where node E is inside node A's radio range, therefore node A has a direct link with node E. When node E moves out of A's radio range, as shown in (b), the original direct link between A and E is broken.

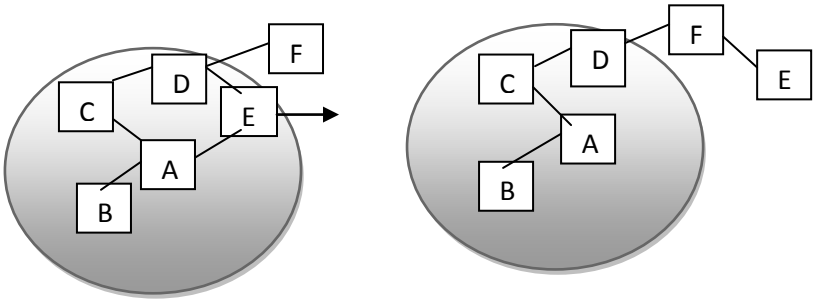

FIGURE 1 EXAMPLE SHOW THE MODE OF BEHAVIOR

However, the link from A to E is still kept, because A can reach E through C, D, and F. Behavior of the ad hoc networks are analyzed as the following.

- Dynamic topologies
- Bandwidth-constrained, variable capacity links
- Energy-constrained operation
- Wireless vulnerabilities and Limited physical security

B. Security goals[8]

There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment.

They are mainly:

- Privacy and Confidentiality
- Availability
- Authentication
- Data Integrity
- Non-Repudiation
- Access and usage control

III. VULNERABILITY IN MANETS

Malicious and selfish nodes are the ones that fabricate attacks [6] against physical, link, network, and application-layer functionality. Current routing protocols are exposed to two types of attacks:

- Active attacks
- Passive attacks

TABLE 1. SHOW DIFFERENT TYPES OF ATTACK

Active Attacks	Spoofing, Fabrication, Wormhole Attack, Modification, Denial of Service
Passive Attacks	Eavesdropping, traffic analysis, monitoring

A. Active Attacks

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. These attacks can be classified into further following types.

Spoofing: Occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather [3].

Fabrication: The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted [4].

Wormhole Attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols [5]. Active attacks Spoofing, Fabrication, Wormhole Attack, Modification, Denial of Service Passive Attacks Eavesdropping, traffic analysis, monitoring

Modification: The attacker performs such attacks is targeted to integrity of data, by altering packet or modifying packets.

Denial of Service: This active attack aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in resistance to Denial of Service attacks, compared to fixed networks.

B. Passive Attacks

In passive attacks the attacker does not perturb the routing protocol, instead try to extract the valuable information like node hierarchy and network topology from it. Passive attack is in nature of eavesdropping on, or monitoring of, transmission. The goal of opponent is to obtained information that is being transmitted [4]. Passive attacks are very difficult to detect because they do not involve any alteration of data.

C. Other Advanced Attacks

We will now discuss several specific attacks that can affect the operation of a routing protocol in ad hoc network.

Byzantine attack: A compromised with set of intermediate, or intermediate nodes that working alone within the network carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services within the network [7].

Replay attack: An attacker that performs a replay attack are retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions [9].

Location disclosure attack: An attacker discover the Location of a node or structure of entire networks and disclose the privacy requirement of network through the use of traffic analysis techniques [10], or with simpler probing and monitoring approaches [6]. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security.

External vs. Internal

External attacks are launched by adversaries that are not legally part of the network. These attacks usually aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Bogus packets injection, denial of service, and impersonation are some of the attacks that are usually initiated by the external attackers.

Internal attacks are sourced from inside a particular network. A compromised node with access to all other nodes within its range poses a high threat to the functional efficiency of the whole network. Attacks that are caused by the misbehaving internal nodes are difficult to detect because to distinguish between normal network failures and misbehavior activities in the ad hoc networks is not an easy task.

Mobile vs Wired Attackers

Mobile attackers have the same capabilities as the other nodes in the ad hoc networks. Their capabilities to harm the networks operations are also limited because of limited resources. With the limited transmitting capabilities and battery powers, mobile attackers could only jam the wireless links within its vicinity but not the whole networks operations.

Wired attackers are attackers that are capable of gaining access to the external resources such as the electricity. Since they have more resources, they could launch more severe attacks in the networks, such as jamming the whole networks or breaking expensive cryptography algorithms. Existence of the wired attackers in the ad hoc networks is always possible as long as the wired attackers are able to locate themselves in the communication range and have access to the wired infrastructures.

Single vs Multiple Attackers

Attackers might choose to launch attacks against the ad hoc networks independently or by colluding with the other attackers. Single attackers usually generate a moderate traffic load as long as they are not capable to reach any wired facilities. Since they also have similar abilities to the other nodes in the networks, their limited resources become the weak points to them [11]. If several attackers are colluding to launch attacks, defending the ad hoc networks against them will be much harder. Colluding attackers could easily shut down any single node in the network and be capable to degrading the effectiveness of network's distributed operations including the security mechanisms.

Attacks on Different Layers of the Internet Model

The attacks can be classified according to the five layers of the Internet model. Table 2 presents a classification of various security attacks on each layer of the Internet model. Some attacks can be launched at multiple layers.

TABLE 2. PRESENTS A CLASSIFICATION OF VARIOUS SECURITY ATTACKS ON EACH LAYER OF THE INTERNET MODEL.

Layer	Attacks
Application layer	Repudiation, Data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, Blackhole, Byzantine, Flooding, Resource consumption, Location disclosure attacks
Data link layer	Traffic analysis, Monitoring, Disruption MAC (802.11), WEP weakness
Physical layer	Eavesdropping, Jamming, Interceptions
Multi-layer attacks	DoS, Impersonation, Replay, Man-in-the-middle

Some security attacks use stealth, where the attackers try to hide their actions from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacks such as DoS cannot be made stealthy.

Cryptography vs Non-cryptography Related Attacks

Some attacks are non-cryptography related, and others are cryptographic primitive attacks.

TABLE 3 SHOWS CRYPTOGRAPHIC PRIMITIVE ATTACKS AND THE EXAMPLES.

Cryptographic Primitive Attacks	Examples
Pseudorandom number attack	Nonce, Timestamp, Initialization vector (IV)
Digital signature attack	RSA signature, ElGamal signature, Digital signature standard (DSS)
Hash collision attack	SHA-0, MD4, MD5, HAVAL-128, RIPEMD

DATA traffic attacks and CONTROL traffic attacks

Traffic attacks: This classification is based on their common characteristics and attack goals. For example: Black-Hole attack drops packets every time, while Gray-Hole attack also drops packets but its action is based on two conditions: time or sender node. But from network point of view, both attacks drop packets and Gray-Hole attack can be considered as a Black-Hole attack when it starts dropping packets. So they can be categorized under a single category.

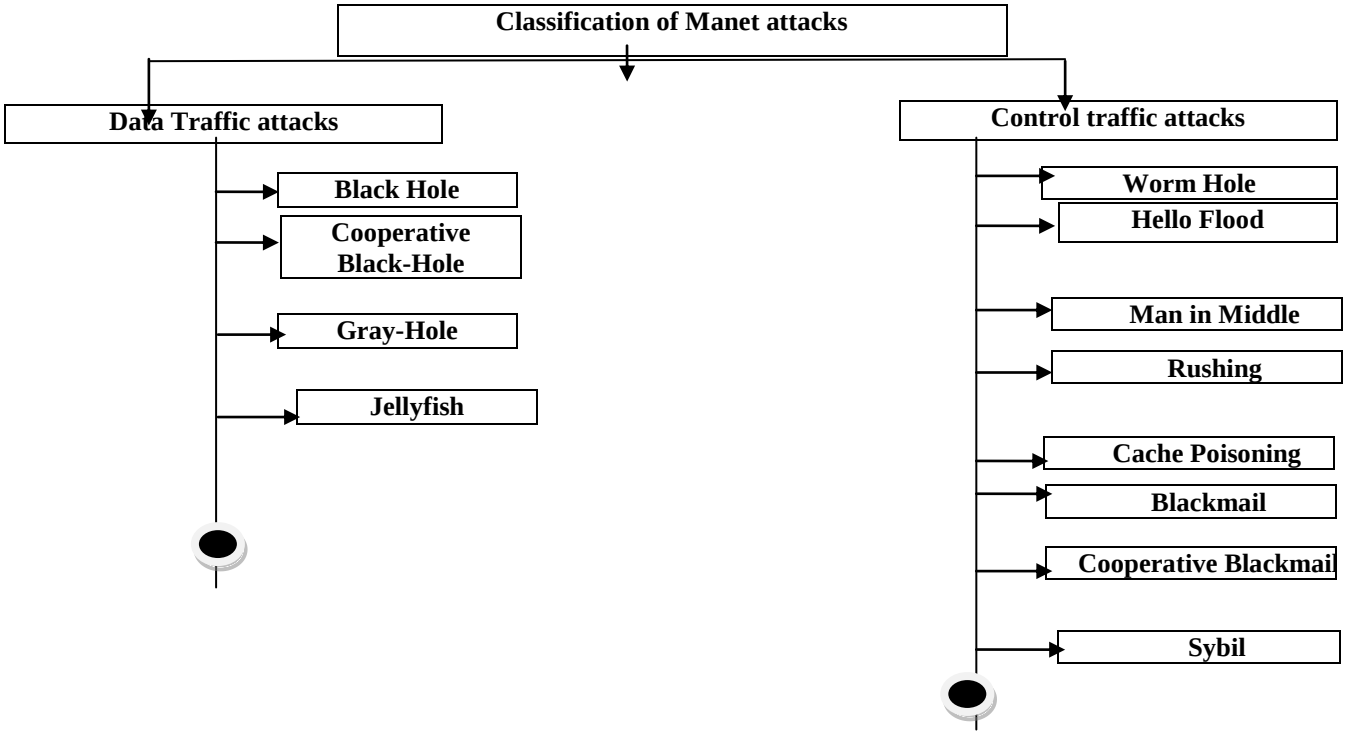

FIGURE 2 SHOW THE CLASSIFICATION OF MANET ATTACKS

DATA Traffic Attack

DATA traffic attack deals either in nodes dropping data packets passing through them or in delaying of forwarding of the data packets

Black-Hole Attack [12][13][14][15]

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network in to two disconnected components. Here the Black-Hole node separates the network into two parts.

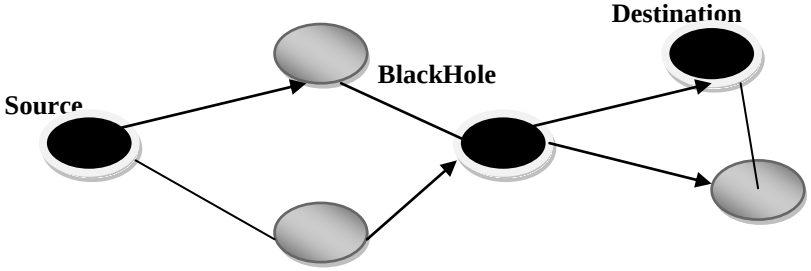

FIGURE 3 SHOW THE BLACK-HOLE ATTACK

Cooperative Black-Hole Attack [12][13][14]

This attack is similar to Black-Hole attack, but more than one malicious node tries to disrupt the network simultaneously. It is one of the most severe DATA traffic attack and can totally disrupt the operation of an Ad Hoc network. Mostly the only solution becomes finding alternating route to the destination, if at all exists.

Gray-Hole Attack [16][17]

Gray-Hole attack has its own characteristic behavior. It too drops DATA packets, but node's malicious activity is limited to certain conditions or trigger. Two most common type of behavior:

(i) Node dependent attack – drops DATA packets destined towards a certain victim node or coming from certain node, while for other nodes it behaves normally by routing DATA packets to the destination nodes correctly.

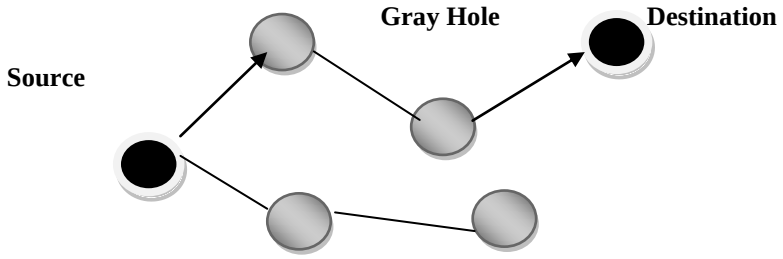

FIGURE 4 SHOW THE GRAY-HOLE ATTACK AT TIME INSTANCE T1

(ii) Time dependent attack – drops DATA packets based on some predetermined/trigger time while behaving normally during the other instances.

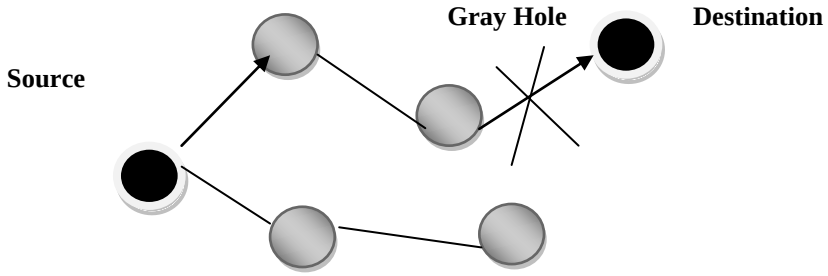

FIGURE 5 SHOW THE GRAY-HOLE ATTACK AT TIME INSTANCE T2

Jellyfish Attack [18]19][20]

Jellyfish attack is somewhat different from Black-Hole & Gray-Hole attack. Instead of blindly dropping the data packets, it delays them before finally delivering them. It may even scramble the order of packets in which they are received and sends it in random order. This disrupts the normal flow control mechanism used by nodes for reliable transmission. Jellyfish attack can result in significant end to end delay and thereby degrading QoS. Few of the methods used by attacker in this attack:

(i) One of the methods is scrambling packet order before finally delivering them instead of received FIFO order. ACK based flow control mechanism will generate duplicate ACK packets which will unnecessarily consume precious network bandwidth and battery life.

(ii) Another method can be, performing selective Black-Hole attack by dropping all packets at every RTO. This 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 same as destination overwhelm.

(iii) The attacking node can store 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 might take a longer route instead of the most obvious shortest route.

CONTROL Traffic Attack

Mobile Ad-Hoc Network (MANET) is inherently vulnerable to attack due to its fundamental characteristics, such as open medium, distributed nodes, autonomy of nodes participation in network (nodes can join and leave the network on its will), lack of centralized authority which can enforce security on the network, distributed co-ordination and cooperation.

Worm Hole Attack [20][21][22]

Worm hole, in cosmological term, connects two distant points in space via a shortcut route. In the same way in MANET also one or more attacking node can disrupt 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 malicious nodes will always be chosen while sending packets to that destination. The attacking node then can either monitor 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 malicious node connects via a *wormhole-link.* Node X and Y performing wormhole attack.

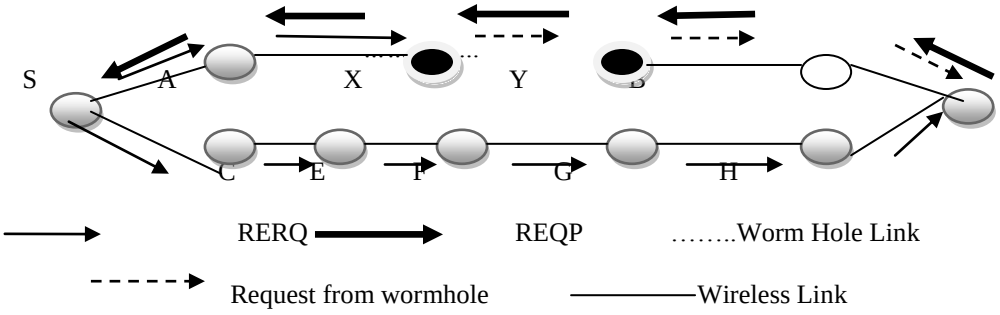

FIGURE 6 SHOW THE WORM-HOLE ATTACK

HELLO Flood Attack

The attacker node floods the network with a high quality route with a powerful transmitter. So, every node can forward their packets towards this node hoping it to be a better route to destination. Some 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 nodes are his neighbor. The attacker node need not generate a legitimate traffic; it can just perform a selective replay attack as its power overwhelms other transceivers.

Bogus Registration Attack

A Bogus registration attack is an active attack in which an attacker disguises 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 disrupt the network altogether. But this type of attack is difficult 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 limit the severity of attack to some extent as attacker node has no previous knowledge of encryption method.

Man in Middle Attack [24]

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

Rushing Attack

In AODV or related protocol, each node before transmitting its data, first establishes a valid route to destination. Sender 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 mechanism to limit the route request and reply chatter in the network. Rushing attack exploits this duplicate suppression mechanism. Rushing attacker quickly forwards with a malicious RREP on behalf of some other node skipping any proper processing. Due to duplicate suppression, actual valid RREP message from valid node will be discarded and consequently the attacking node becomes part of the route. In rushing attack, attacker 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 destination node.

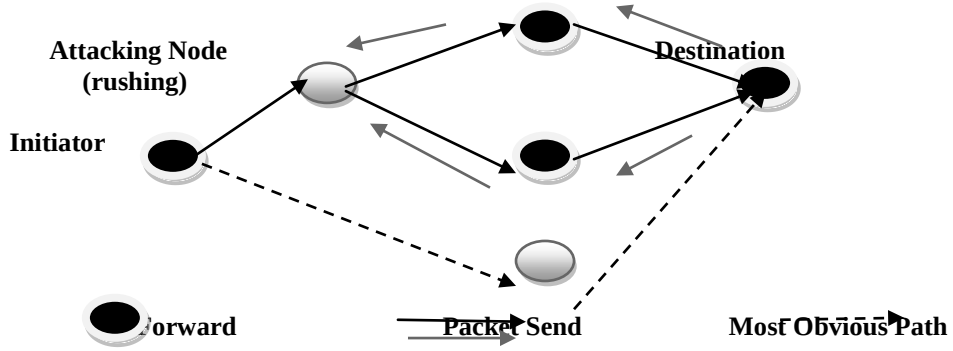

FIGURE 7 SHOW THE RUSHING ATTACK

Cache Poisoning Attack

Generally in AODV, each node keeps few of its most recent transmission routes until timeout occurs for each entry. So each route lingers for some time in node's memory. If some malicious node performs a routing attack then they will stay in node's route table until timeout occurs or a better route is found. An attacker node can advertise a zero metric to all of its destinations. Such route will not be overwritten unless timeout occurs. It can even advertise itself as a route to a

distant node which is out of its reach. Once it becomes a part of the route, the attacker node can perform its malicious activity. Effect of Cache poisoning can be limited by either adding boundary leashes or by token authentication. Also each node can maintain its friend-foe list based on historical statistics of neighboring nodes performance.

Blackmailing and Co-operative Blackmailing Attack

In a blackmailing attack or more effectively co-operative blackmailing attack, attacker nodes accuse an innocent node as harmful node. This attack can effectively be done on those distributed protocols that establish a good and bad node list based on review of participating nodes in MANET. Few of the protocols tries to make them more secure by using majority voting principle, but still if sufficient no. of attacker nodes become part of the MANET it can bypass that security also. Another generic method of this attack will be, sending invalid RREP messages with advertising an unnecessarily high cost to certain nodes. Known mitigation techniques:

(i) Dynamic Trust based, Distributed IDs [23]: As MANET routing is a co-operative process, while building a route each node must evaluate its neighbor nodes. This method builds a distributed trust relationships and maintain dynamic trust information. As the trust is part of a long chain, single malicious node cannot victimize an innocent node easily.

(ii) Friend List based [24]: Another solution will be building a friend list of trusted nodes. Nodes identity must be determined by the user who created the MANET. So it becomes a closed system of trusted nodes.

Sybil Attack

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

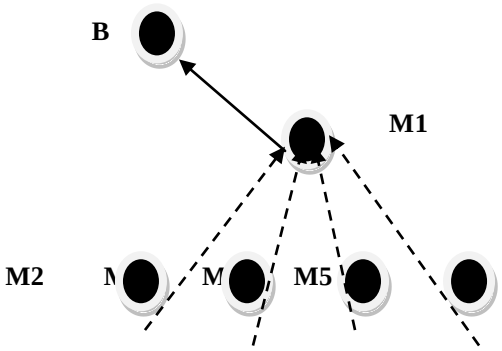

FIGURE 8 SHOW THE SYBIL ATTACK

IV. CONCLUSION

This paper analyzed the security challenges and different types of attacks in the ad hoc networks. We have tried to categorize the different types of ad hoc security attacks solely based on their characteristics to considerably reduce the mitigation period. Bringing, the attacks under two broad categories, some attacks have characteristics which makes them unsuitable to be categorized into these categories. Further study is in progress to find out more common characteristics of the attacks to more strongly bind them into these categories and to ably design more powerful algorithm in mitigating DATA and CONTROL traffic attacks.

REFERENCES

[1] E. Ayanoglu, C.-L. I, R. D. Gitlin, and J. E. Mazo. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Transactions on Communications, 41(11):1677–1686, November 1993.

[2] M. Castro, and B. Liskov. Practical Byzantine fault tolerance. In Proceedings of the 3rd USENIX Symposium on Operating System Design and Implementation (OSDI'99), pages 173–186, New Orleans, LA USA, February 22–25, 1999. USENIX Association, IEEE TCOS, and ACM SIGOPS.

[3] M. Ilyas. The Handbook of Ad Hoc Wireless Networks. CRC Press, 2003.

[4] C.K.Toh. Ad Hoc Mobile Wireless Networks: Protocols and Systems. Prentice Hall Englewood Cliff, NJ 07632, 2002.

[5] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002

[6] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L. Security in mobile ad hoc networks Challenge and solution. IEEE Wireless Communication. 11, 1, (2004), 38- 47.

[7] H Deng, W. Li, and D. Agrawal. Routing Security in Wireless Ad Hoc Networks. IEEE Communications Magazine. Vol. 40, No. 10, 2002.

[8] Jiejun-K, Petros-Z, Haiyun-Luo, Songwu-Lu, and Lixia- Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks, Proceedings Ninth International Conference on Network Protocols. ICNP 2001, Riverside, CA, USA, 11-14 Nov. 2001.

[9] Sonja Buchegger and Jean-Yves Le Buddec. Increasing Routing Security in Mobile ad hoc Network. IBM Research Report: RR 3354, 2001

[10] L. Zhou and Z.Haas. Securing ad hoc networks. IEEE, Networks, 13(6):24–30, 1999.

[11] Venkatraman-L, and Agrawal-D-P. A novel authentication scheme for ad hoc networks. Proceedings of IEEE Conference on Wireless Communications and Networking, vol.3, Chicago, IL, USA, 23-28 Sept. 2000.

[12] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard. Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, Vol. 2, No. 3, July, 2008

[13] Mohammad Al-Shurman, and Seong-Moo Yoo. Black Hole Attack in Mobile Ad Hoc Networks.. ICUMT 2010: 287-294

[14] Sheenu Sharma, Roopam Gupta: Simulation Study Of Blackhole Attack In Mobile AD HOC Networks. Journal of Engineering Science and Technology Vol. 4, No. 2 (2009) 243 - 250

[15] Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, and Pedro Gil. Black Hole Attack Injection in Ad hoc Networks.June ,2008

[16] M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar,Jaydip Sen. A mechanism for detection of Gray Hole Attack in Mobile Ad Hoc Networks (Submitted on 2 Nov 2011)

[17] Vishnu K, Amos J Paul. Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks. ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 22

[18] Ruiliang Chen, Michael Snow, Jung-Min Park, M. Tamer Refaei, and Mohamed Eltoweissy. Defence against Routing Disruption Attacks in Mobile Ad Hoc Attacks.

[19] Muhammad Zeshan, Shoab A.Khan, Ahmad Raza Cheema, Attique Ahmed. Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks. 2008 International Seminar on Future Information Technology and Management Engineering.

[20] Maria Alexandrovna Gorlatova. Review of Existing Wormhole Attack Discovery Techniques.

[21] Piyush Agrawal and R. K. Ghosh. Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks. © 2010 by IJCA Journal, Number 22 –Article 8

[22] Information Security magazine - December 2013 Vol. 15 / No. 10

[23] Zhaoyu Liu, AnthonyW. Joy, Robert A. Thompson. A Dynamic Trust Model for Mobile Ad Hoc Networks. 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04).

[24] S. Bouam, and J. B. Othman. Data Security in Ad hoc Networks using MultiPath Routing. in Proc. of the 14th IEEE PIMRC, pp. 1331-1335, Sept. 7-10, 2003.

