© 2017 IJSRST | Volume 3 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Consequence of Security Attacks in MANET

K. Ramakrishna Reddy
Associate Professor, Department of CSE, Malla Reddy Engineering College (A), Hyderabad, Telangana, India

ABSTRACT

Now a days Security in MANET is a major challenge as it has no incorporated authority which can regulate the individual nodes functioning in the network. Moreover the attacks can come from both inside the network and from the outside. We are exasperating to classify the present attacks into two broad categories: DATA traffic attacks and CONTROL traffic attacks. In continue with that I discussed the Consequence of Security Attack in MANET over inter network layer.

Keywords : MANET, DATA traffic attacks, CONTROL or REGULATE traffic attacks.

I. INTRODUCTION

A mobile ad hoc network is a self-configuring network of mobile nodes. It privations any fixed infrastructure like access points or base stations. It lacks centralized administration and is connected by wireless links/cables. MANET has no reasonable line of safeguard, thus, it is available to both true network users and malignant attackers. Different types of attacker endeavor distinctive ways to deal with decreasing the network performance. Within the sight of noxious or malicious nodes, one of the principle challenges in MANET is to outline the hearty security arrangement that can shield MANET from different steering assaults.

Security is a noteworthy concern towards safe communication between portable hubs in an outsider domain. In outsider situations, attackers can bundle dynamic and inactive attack against impalpable directing in routing message and information packets. This adaptability alongside their self-organizing facilities is some of MANET's greatest qualities, and also their greatest security vulnerabilities.

II. SECURITY CHALLENGES IN MANET

Our focus of arriving at this model was to focus on the mobility of the network as opposed to the mobility of nodes, inferring the movement of whole sub networks regarding each other, while individual clients at first connected with one such sub network may likewise move to different areas.One illustration is a war zone network that incorporates boats, airplane, and ground troops. In this "network of networks" subnets (e.g., shipboard systems) are interconnected by means of an earthly mobile wireless network (e.g., between moving boats). The clients are at first connected with their home systems yet are allowed to move between spaces. Challenges in such a situation incorporate interoperation among various stages, upkeep of security affiliations, and circulation of policies to protect QoS.

1.1 Features Challenging Security in MANET

In view of dynamic topological structures, Ad-hoc networks at the physical link are more helpless and vulnerable. An attacker can effortlessly attack ad hoc networks by loading accessible network resources. The attackers deploy special systems that access assets

such as wireless links and energy (battery) levels of other users and create disturbance to the users. The accompanying difficulties demonstrate the inefficient aspects and confinements that must be overcome in a MANET situation:

1.2 Limited computational capabilities

In MANET typically, nodes are free and constrained in computational capacity and modular in nature, which yields to source of vulnerability.

1.3 Limited wireless transmission range

In remote systems, the radio band will be constrained and consequently information rates it can offer are much lesser than the wired system. This requires the routing protocols in ad-hoc networks to utilize the bandwidth in an ideal way by keeping the overhead as low as could be allowed.

1.4 Device Compatibility

In MANETs, the main challenge is to set up communication between heterogeneous devices with changing energy profiles, diverse hardware configurations or running distinctive versions of software.

1.5 Battery constraints

There is limited energy supply for the wireless nodes which is a major constraint. To maintain portability of the devices, the devices are dependent on the power source.

1.6 Challenging key management

There is lack of incorporating security features as the nodes tend to move in the network making key management between pair of nodes difficult. Though cryptography is used in the routing protocols, the prevention of potential attacks is at stake due to difficulty in key management.

1.7 Packet losses due to transmission errors

MANET encounters a much higher packet loss because of elements, for example, high bit error rate (BER) in the remote wireless channel, expanded crashes because of the nearness of concealed terminals, presence of impedance, area subordinate conflict, unidirectional connections, successive way breaks because of versatility of nodes, and the intrinsic blurring properties of the remote wireless channel.

1.8 Bandwidth usage

Transfer speed or bandwidth accessibility influences the network. In MANETs, transfer speed is utilized for availability of connection, maintenance and for information or data exchange. In the event that all accessible transmission capacity is spent by information communication and other connection establishment exercises then more up to date connections may not be set up or existing connections may not be re-set up when portable nodes migrate themselves.

III. SECURITY ATTRIBUTES IN MANET

The field of security is large and if the described attributes holds good, then we can say that the network is secure. Networks using security sensitive information exchange need to use some model controlling the attacking problems. The accompanying attributes should be considered for characterizing the diverse security needs of the uses of Ad Hoc network.

Since nodes are connected to MANETs for a short duration, real-time constraints should be maintained to achieve the goal of controlled access to the limited resources. The key requirements for networks are as follows:

Confidentiality – In MANET, each application or node has permission to access a specified set of services of

the application in use. Confidentiality is required to prevent an opponent from traffic analysis and protect the data.

Authentication- There should be trustable communications between two different nodes. Nodes should respond only to the messages transmitted by legitimate members of the network. Thus, it is very important to authenticate the sender of a message and authorize another node to update information or to receive information.

Availability – It is the property of the network to ensure that in-spite of all attacks the authorized node is able to provide data and services. The network should be accessible even if it is under an attack using alternative mechanisms without affecting its performance. Decentralized System Cooperative Communication Open Medium Dynamic Topology Reasons on Security Threats in MANET

Integrity – It is the ability of the authorized nodes to create, edit or delete packets. It ensures that data or messages packets are not altered by attackers during transmission. Otherwise, users are directly affected by the altered emergency data.

Non-Repudiation- This property ensures that neither source nor destination can refuse their behavior of sending or receiving data. It helps in isolation of malicious nodes. At any point of time when there is an investigation on identity of a node, the sender must not deny the message transmission.

Certainty of discovery – This ensures that source node by the help of Route Discovery mechanism obtains the address of destination node before transmitting the packets to the destination.

Isolation – It is preventing a given node in the network to communicate with any other node.

Lightweight computations – Computations on route discovery can be performed.

Data Verification - Once the sender is validated, the receiving node performs information confirmations to check whether the message contains the right or undermined information.

Privacy – It prevents the individual's personal information data against unapproved or unauthorized access.

Resilience to attacks -It is required to support the system functionalities when some nodes are traded off or crushed.

Freshness -It guarantees that malicious node does not resend beforehand captured packets.

IV. TYPES OF SECURITY ATTACK IN MANET

Classification of MANET Attacks described in Figure 1:

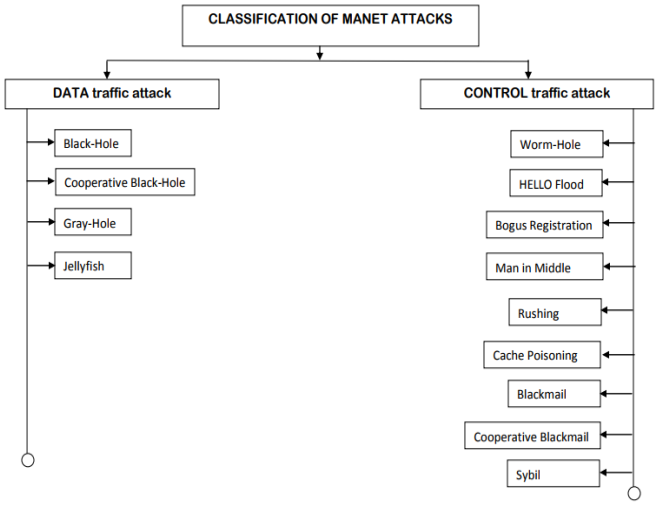

Figure 1. Classification of MANET Attacks

1.9 DATA traffic attack:

It deals either in node dropping data packets passing through them or in delaying of forwarding of the data packets.

Black-Hole Attack:

Attacker sets up a route to some destination via itself and sends out forged routing packets. At the point when the actual data packets arrive they are just dropped, framing a dark gap (a black hole) where information enters yet never takes off. [1].

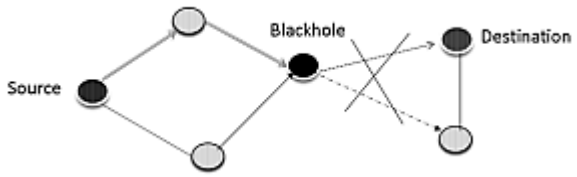

Figure 2: Black-Hole Attack

Cooperative Black-Hole Attack [2] : This is a complex type of attack which is done by two or more colluding nodes. The invisible colluding nodes participate in the attack and make the source node believe that there is a reliable route.

Gray-Hole Attack [9]: In this type of attack the packet is purposely fully dropped or dropped for a certain time period by the malicious node. The state of malicious node is reversed back to behave as a normal node. The malicious node that receives the packet to be forwarded is dropped off after the route discovery process..

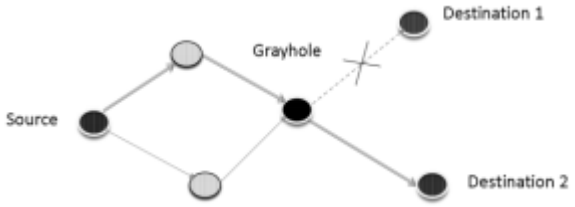

Figure 3. Gray-Hole – Node dependent attack

Jellyfish Attack: In this type of attack, the attacker accesses the system intrudes into the group and turn into a part of the system for forwarding the packets. Once it becomes a part of the system, before forwarding the data packets it delays the packets and increases the performance factor End-to-End value to very high. The overall network communication is impacted due to high delays. [12]

1.10 CONTROL Traffic Attack:

Network traffic control is the process of managing, controlling or reducing the network traffic, particularly Internet bandwidth.

Worm Hole Attack [5]: 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.

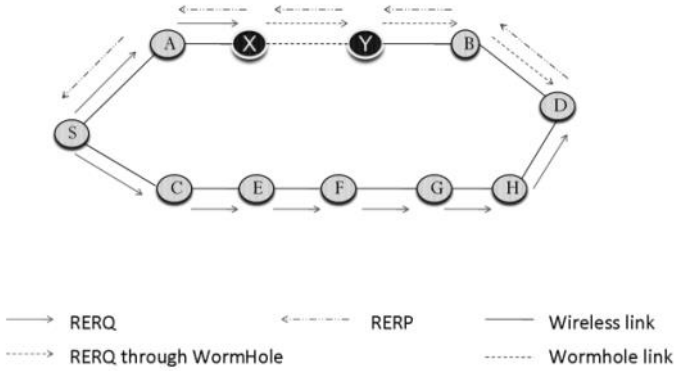

Figure 4. Worm-Hole attack

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.

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.

Man in Middle Attack: in Man in Middle attack, the attacker node sneaks into a effective route and tries to sniff packets sinuous through it. [10]

Rushing Attack: In this type of attack, attacker multiplies the route request sequence numbers. The sequence numbers are maintained by reactive protocols to suppress duplicate packets at the nodes.

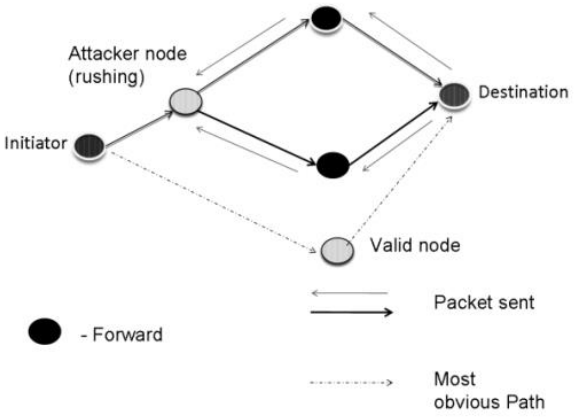

Figure 5. Rushing Attack

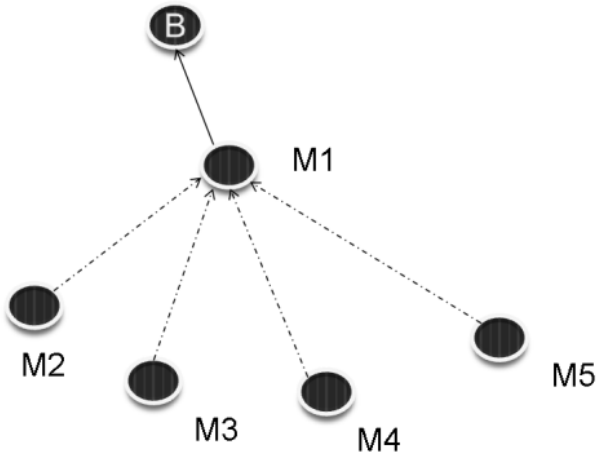

Figure 6. Sybil Attack

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.

V. INFLUENCE OF SECURITY ATTACK IN MANET

Table 1. Effect of Security Attack in MANET over Internetwork Layer.

Network Layer	**Attacks**	**Effects**
Physical Layer	Eavesdropping	It keeps an eye on information bundles, takes critical data, and puts itself between the gatherings to contact.
	Jamming attack	It sends counterfeit flags and meddles with successful correspondence. It influences the execution of the system by decreasing the limit of the bundle and postponing the conveyance of parcels, and the parcels may achieve harmed.
Data Link Layer	Traffic Analysis	It depends on the track and investigation of the stream of activity in order to know the system plot, prompting distinguish hubs and approach them.
	Malicious behavior of nodes	It depends on crippling crafted by direction conventions and possesses a place between hubs.
	Monitoring	It depends on access to private information without having the capacity to change or revise them.
Network Layer	Black hole attack	It happens amid the execution of the parcel controlling procedure. It utilizes a direction convention in order to recognize itself as the course of validation to the objective hub. It makes an answer message to with the goal that it takes the

		briefest way to the objective. It utilizes a phoney method to achieve the objective.
	Rushing Attack	It sends a demand to the hubs that will be assaulted, and the hubs answer to the genuine request, and after that, the phony request is endorsed, and in this manner, the assailant comes into contact.
	Sinkhole attack	It depends on deceiving the information activity way and endeavors it for its advantage in changing or obliterating the private data.
	Gray Hole Attack	It depends on dropping messages to delude the way to the goal, and there is a trap of where to drop the bundle.
	Replay attack	It depends on a rehash of the assault on information parcels in order to infuse the activity that has been caught before, prompting deluding the controlling way in the MANET organize.
	Resource consumption	Depends on the revelation of the way or re-coordinating superfluous ones over and over and consistently.
	Wormhole	It is spoken to in the collaboration between two assaulting hubs. The principal assailant picks a bundle and to the next aggressor by utilizing a fast medium.
	Byzantine attack	It comprises of an arrangement of hubs and is aggregate sets up control rings, and it additionally manages bundles in most exceedingly bad tracks
	GRAY HOLE attack	It deludes the track and drops parcels, which can be viewed as a revelation of itself as the correct track to drop bundles.
Transport Layer	SYN flooding attack	It comes amidst the contact by sending SYN to the objective hub and adventures a reaction from the ACK target hub.
	Session hijacking	It depends on the abuse the address of the IP focus by distinguishing the right serial number. It attempts to prevent benefit from the objective hub as though they were non-existent in the system.
Application Layer	Repudiation attack	It listens stealthily and afterwards rejects or denies hitches a support hub in contact after it had contributed to some extent or entire contact.
	Malicious code attacks	It assaults working framework and applications which live like infections, worms and spyware, and Trojan steed.

VI. CONCLUSION

In this paper i have been tried to group the different types of ad hoc security attacks exclusively based on their characteristics to significantly reduce the justification period. An attempt has been made to present an overview of all the existing security attacks in the MANET By bringing the attacks under these two broad categories the complicacy of naming also decreases. Additional revision is in evolvement to notice more common characteristics of the attacks to more intensely bind them into these categories and to capably design more powerful algorithm in mitigating DATA and CONTROL traffic attacks more over also presented Impact of Security Attack in MANET.

VII. REFERENCES

[1]. C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel," Proc. /E€€ SICON '97, Apr. 1997, pp. 197-211

[2]. Th. Clausen et al., "Optimized Link State Routing Protocol," IETF Internet draft, draft-ietfmanet-olsr11.txt, July 2003.

[3]. B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A. Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensor networks, October 2007, page, 85-91

[4]. Z. Karakehayov, "Using REWARD to Detect Team BlackHole Attacks in Wireless Sensor Networks," Wksp. RealWorld Wireless Sensor Networks, June 20–21, 2005.

[5]. S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.

[6]. S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," 2002 Int'l. Conf. Parallel Processing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

[7]. S. Kurosawa et al., "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec., 2006.

[8]. D. Johnson and D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Ed., pp. 153-81. Kluwer, 1996.

[9]. Jyoti Raju and J.J. Garcia-Luna-Aceves, " A comparison of On-Demand and Table-Driven Routing for Ad Hoc Wireless etworks'," in Proceeding of IEEE ICC, June 2000.

[10]. Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[11]. Eli-Chukwu, Ngozi Clara, Onoh, Greg Nwachukwu," Improving Service Accessibility (CSSR) In GSM Network using an Intelligent Agent-Based Approach." International Journal of Computer Engineering In Research Trends., vol.4, no.11, pp. 478-486, 2017.

[12]. Prof. R. Poorvadevi , S.Keerthana , V.S. Ghethalaxmipriya , K. Venkatasailokesh," An Enforcement of Guaranteed Client Level Defensive Mechanism in Public Cloud Services." International Journal of Computer Engineering In Research Trends., vol.4, no.2, pp. 20-24, 2017.

[13]. Yashoda B.S, Dr. K.R. Nataraj," Performance Analysis of Existing Beam forming Methods for Various Antenna Elements and Interference Sources." International Journal of Computer Engineering in Research Trends., vol.4, no.4, pp. 142-149, 2017.