ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

A Study on Security Problems in Mobile Ad-hoc Network

Nisha Gupta

Professor, Department of Computer Engineering, Parul Institute of Engineering& Technology College, Gujarat, India

ABSTRACT:A Mobile Ad Hoc is a group of specialized device that is used to desire to connect inside themselves without any fixed foundation of system. Mainly the utilization of MANET are regions where no requirement of physical wiring and fast sending and dynamic reconfiguration is required. Previous Studies MANET used to suggest some solutions to a few essential issues, which include routing, copying with the new challenges just only because of node functions and network's nodes without taking the security issues under consideration. This paper is going to discuss about the existing issues in MANET security issues into record. This paper discusses the issues existing in MANET.

KEYWORDS:MANET , Ad-hoc, DoS, Attacks, Hijacking.

I. INTRODUCTION

MANET-Mobile Ad-hoc network. "Ad-hoc" signifies "for that specific reason". [1]. There is no requirement of any base like infrastructure and devices are associated without wires. All devices in MANET are self-configured. Every node in this network contain mobile and it can also change to other device frequently. As ad hoc need flat infrastructure, ad-hoc are totally different from alternative network, work on shared medium (example: - radio), have dynamic topology. Still as finish hosts this network on each pc device act as a router. Paper is organized as follows. Section II describes automatic text detection using morphological operations, connected component analysis and set of selection or rejection criteria. The flow diagram represents the step of the algorithm. After detection of text, how text region is filled using an Inpainting technique that is given in Section III. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

II. RELATED WORK

Internet style and led to the robust scalable protocols, may result in poor performances once applied to mobile ad-hoc networks. The nodes concerned in a manet ought to collaborate amongst themselves and every node acts as a relay once required to implement functions. Multi-hop sessions are studied. The manet nodes are mobile devices with less central process unit (CPU), little memory size, and low power storage. The traffic sorts in ad-hoc networks are quite totally different from AN infrastructure wireless network, as well as peer to peer, remote to remote, and dynamic traffic [17In dynamic traffic, the drawback happens once nodes are mobile and touring, thus , routes should be reconstructed. This causes poor network activity and property briefly bursts. A painter is a self-configuring network of mobile devices connected by a wireless link while not fixed infrastructure [17]. A MANET is a self-configuring network of mobile devices connected by a wireless link without fixed infrastructure [18]. . In MANET, the info packet could fail to be delivered for numerous reasons such as nodes movement, packet collision and dangerous channel condition.

III. APPLICATIONS

1. In wireless communication there's primary demand of MANET that provides effective communication, even wherever efforts in cluster is needed.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

2. At the instance of disaster, there is would like of wireless network. The places where wired network might even be stricken by the disasters, MANET square measure usually implemented [2].
3. Ad hoc networking would alter the military to require care of all the data network finite by the troopers, vehicles and every one military information headquarters.
4. As in economic and industrial ad-hoc plays necessary role in emergency or rescue operations like earthquake emergency, flooding etc. at the opposite side business state of affairs it includes spontaneous mobile communication from ship to ship ,etc.

IV. ATTACKS IN MANETS

1.ATTACKS AT PHYSICAL LAYER

Eavesdropping [3]:- This attack is passive. Eavesdropping alludes to unapproved checking of the communication of the otherspeople. thanks to eavesdropping, traditional knowledge transmission in networks doesn't have an effect on, Sender or receiver can hardly notice knowledge being taken, intercepted or deactivated. It obtains guidance like non-public key, location and routing data, node passwords that ought to be restricted once communication.

1. Obstruction:- It's one amongst the particular DoS attack kind. This attack is geared toward preventing the legitimate sender and receiver from sending and sending packets on the network, i.e. busy between 2 authentic nodes that communicate By injecting dummy packets into the shared medium, it'll interfere with live communication. In some cases the mac layer of alternative nodes is additionally abused.

2. Active disruption:-It's reasonably a DoS attack. during this attack, the wireless channel is interrupted. In active interception, the transmitted messages may be overheard by the unwelcome person so duplicate messages into the network on behalf of the user wherever, as in passive interception, the network traffic is habitually monitored to assemble qualitative info or different info not communicated expressly through a knowledge stream. The message sequence changes to replay recent messages attacker. recent messages may be re - vie or out-of-date info may be re - introduced.

2. ATTACKS AT DATA LINK/MAC ADDRESS

1. **Egotistical node misconduct [4]:** - These square measure the nodes wherever you would like to preserve your own resources whereas using others ' services and overwhelming their resources. The node uses its resource once it's required within the network and becomes calm, not visible to the network when it's used. If packet resources area unit required, packets are going to be impartial and born. self-centered nodes will take action in ad - hoc networks below:
a) Being quite once nodes unable to speak.
b) It doesn't broadcast these messages within the network once receiving RREQ messages.
c) Re - broadcasting RREQ, forwarding RREP to reverse path, however not forwarding knowledge packets.
d) To combat the present mechanism, it by selection drops knowledge packets
Based on the higher than threats, we are able to see however harmful these nodes may be in Manet, particularly in terms of lowering delivery rates by dropping packets.

2.**Misleading node behaviour [5]: -**
If a node breaches any of the principles of security and is therefore under any attack, it maliciously acts in the networ k. This node shows the following behaviour:
1. Dropped packet
2. Drained battery

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

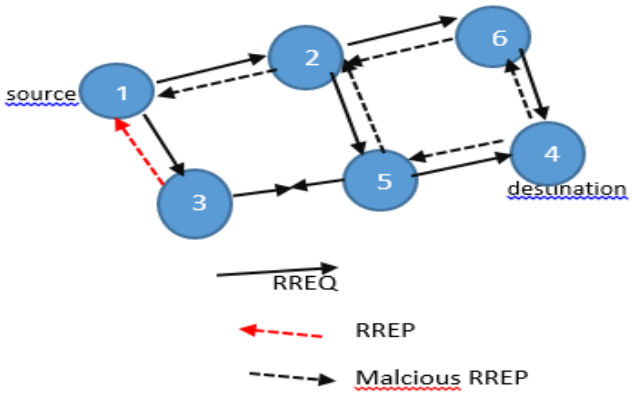
Vol. 8, Issue 4, April 2019

3. Dropped packets
4. Delay
5. Dropped link
6. Not available node
7. Information stealing
8. Delay

2. **Analysis of traffic: -** Traffic analysis will leak info like node location, configuration of communication; node roles, supply and destination offered. Traffic analysis will leak info like node location, network communication topology; node-played roles, supply and destination nodes offered.

3. ATTACKS AT NETWORK LAYER

1. Black hole attack: - The malicious node here advertises itself as having the simplest path within the method of route discovery. Once the RREQ packets are received, the pretend RREP packet are going to be sent to the supply node [6][7][8].



3.3.1 Black hole attack

2. In the figure **on top of**, **we tend to** see node **three** acting as a malicious node. **once** node **one** (SN) sends RREQ packets **to any or all** nodes, node **three can** reply **to the current** network as having the shortest path. **it'll** take from the **supply** node all the packets and drop all the packets **rather than** forwarding to node **four** (DN).

3. Rushing attack: - Use rushing attacks against all routing protocols on demand [9].

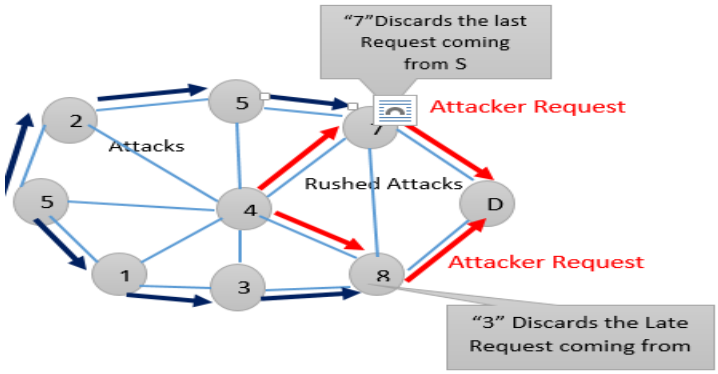
ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

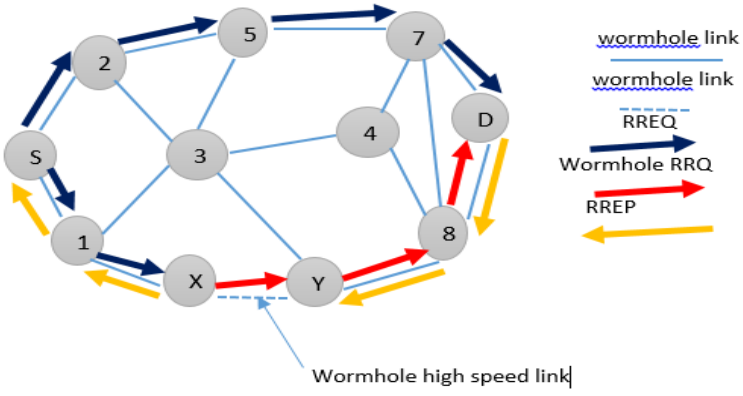
Vol. 8, Issue 4, April 2019



3.3.2 Rushing attack.

3. When a supply node sends a route request packet to a network, the malicious node (node four within the on top of figure) accepts the RR packet and sends it at high speed compared to alternative nodes on the network [10]. This packet are going to be received by the destination node and also the alternative actual knowledge packets are going to be discarded later. This route are going to be found by the receiver as a legitimate route and also the attacker can gain access to communication with success.

4. **Wormhole attack:** - The malicious node receives knowledge packet from the supply node during this attack and transmits it to a different node in a very network that produces it as malicious. This route forms a tunnel referred to as a hollow between 2 malicious nodes. These are extreme threats to protocol routing.There are 2 malicious nodes that kind tunnel within the given figure nodes "X" and "Y." so as to seek out a path, the supply node "S" sends RREQ message to the destination node "D." The neighboring node of supply node "1" and "2" forward it to their neighbors "X" and "5."



3.3.3 Wormhole attack

When the node "X" receives the RREQ packet, it immediately transmits it to "Y" and later initializes RREQ to "8." The result is that "D" ignores the late arriving packet and selects the < S-1-X - Y-8-D > path.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

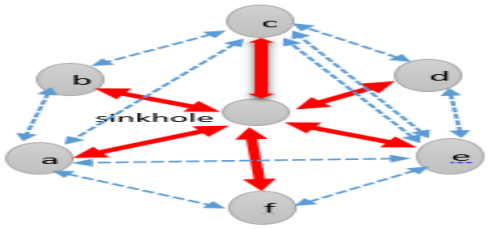
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

4. Sinkhole attack [11]:- The malicious node itself broadcasts as a fixed node in the sinkhole attack and draws all network traffic to itself.After receiving it modifies the confidential information and makes these attacks complicated by the network difficult to counter because it becomes difficult to verify the node that provided the routing information.



3.3.4 sinkhole attack.

5. Replay attack: This attack keeps track of all other nodes ' control messages and sends them back later. This results in other nodes with stale routes to record their routing table. These replay attacks are subsequently misused to disturb a MANET's routing operation**.**

In connection withholding attack, malicious node ignores the need to advertise to group of nodes resulting in loss to these networks. It leads to the loss of the nodes ' links.

Spoof means to hoax, trick. Malicious node impersonates another device in a network to launch attacks in connection spoofing attack.

7.Resource consumption attack: - These area unit usually spoken because the attack on sleep deprivation and occur largely before of devices that don't supply any network services. By passing extra knowledge to victims, it tries to consume battery life.

It creates fake node identity. In this, the node itself produces variety of fake identities instead of one node. Sybil attack is named the extra identities that the node needs. totally different effects area unit thanks to Sybil nodes.

8. Sybil attack:- It creates fake node identity. In this, the node itself produces variety of fake identities instead ofone node. Sybil attack is named the extra identities that the node needs. totally different effects area unit thanks to Sybil nodes:-

a)Prevents the allocation of truthful resources among the network nodes.

b)It becomes tough to spot the affected node within the presence of Sybil node and additionally it generates fakeidentities.

c) The result might vary thanks to these duplicate identities.

d) Sybil node seems at totally different locations and so affects traditional operation

4. ATTACKS AT TRANSPORT LAYER

1. **Session hijacking: -**Also referred to as address attack, session hijacking affects the OLSR protocol. The attacker spoofs the victim's scientific discipline address during this attack then launches many DoS attacks.
2. During this attack, malicious node makes an attempt to assemble all secret info from network nodes, like personal key, public key, knowledge and every one different info.

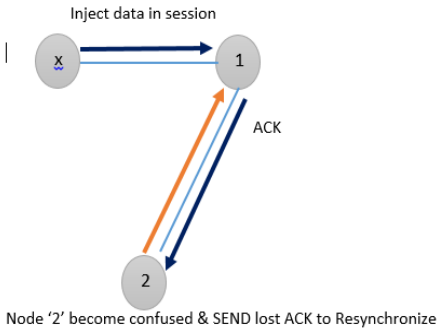
ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019



3.4.1 Session hijacking

In the figure node above, X injects the data into node 1 in session and then sends acknowledgement to node 2. Node 2 receives the packet and attempts to synchronize with node "1" again with the TCP session. This process is repeated over and over, leading to the storm of ACK.

[1] **SYN flooding:** - - In this attack, the attacker sends SYN requests to the target system to consume enough server resources to render the system unresponsive. This attack involves sending packets of synchronization to each port on the server repeatedly using fake IP address.The server sees multiple attempts to communicate when the attack starts. The server responds to each attempt with the reconnaissance packet from each port.

5.ATTACKS AT APPLICATION LAYER

1. **Malicious code attack:** - this sort of attack includes viruses, worms, and Trojan horses, spywares which will attack each user application and package.
2. **Repudiation attack**: - This attack may be used to modify data concerning actions performed by malicious users to log incorrect knowledge into incorrect files. this is often transferred from transport layer to network layer by the offender. It denies system involvement to speak with the network industrial system is an example of this attack. there's not enough network and transportation layer to stop this attack.

REFERENCES

[1] PimalKhanpara and BhushanTrivedi, "Security in ad hoc networks", Proceedings of International
[2] Conference on Communication and Networks,Springer, pp. 501-511, 2017.
[3] Dr. SS Tyagi and Aarti, MANET-characteristics, challenges, applications, vol.3.
[4] Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay "Different Types Of Attacks on Integrated MANET-Internet Communiaction" International Journal of Computer Science and Security(IJCSS) Volume(4): Issue (3).
[5] Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay "Different Types Of Attacks on Integrated MANET-Internet Communiaction" International Journal of Computer Science and Security(IJCSS) Volume(4): Issue (3).
[6] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey".
[7] Jangra1,A. Goel,N. Priyanka and Bhati,K.-Security aspects in Mobile Ad Hoc Networks (MANETs): A Big Picture, International Journal of Electronics Engineering, pp. 189-196, 2010.
[8] GauravSandhu&MoitreyeeDasgupta, (2010) "Impact of blackhole attack in MANET", International Journal of Recent Trends in Engineering and Technology, Vol. 3, No. 2.
[9] Hongmei Deng & Wei Li, Dharma P. Agarwal (2002) "Routing security in wireless ad hoc networks",
[10] Ochola EO &Eloff MM, "A review of black hole attack on AODV routing in MANET".
[11] R. Chandra, V. Rama subramanian, and K. Birman, "Anonymous Gossip: Improving Multicast Reliabilityin Mobile Ad-Hoc Networks,"Proc. 21st Int'l Conf. Distributed Computing Systems (ICDCS '01), 2001.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

[12] Mr. Rajesh H. Davda1, Mr. Noor Mohammed, " Text Detection, Removal and Region Filling Using Image Inpainting", International Journal of Futuristic Science Engineering and Technology, vol. 1 Issue 2, ISSN 2320 – 4486, 2013
[13] Benjamin J. Culpepper and H. Chris Tseng, "Sinkhole Attack Detection in DSR MANETs: A Fuzzy Logic
[14] Muthukumar S, Dr.Krishnan .N, Pasupathi.P, Deepa. S, "Analysis of Image Inpainting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighborhood Methods", International Journal of Computer Applications (0975 – 8887), Volume 9, No.11, 2010
[15] PimalKhanpara and BhushanTrivedi, "Security in ad hoc networks", Proceedings of International
[16] S. Albert Rabara1 and S.Vijayalakshmi2, "Rushing Attack Mitigation In Multicast MANET (RAM3)",
[17] Masoumeh Karimi, Deng Pan," Challenges for Quality of Service (QoS) in Mobile Ad-Hoc Networks (MANETs)", Proceedings of IEEE 10th Annual Wireless and Microwave Technology Conference, WAMICON '09,pp.1-5,2009
[18] S.J. Lee, E. Royer and C.E. Perkins, "Scalability study of the ad hoc on-demand distance vector routing protocol", International Journal of Network Management, Vol.13, 2003, pp. 97–114.