MANET SECURITY BREACHES : THREAT TO A SECURE COMMUNICATION PLATFORM

Ms.Supriya[1] and Mrs.Manju Khari[2]

[1]M.Tech(Information Security).Ambedkar Institute of Technology,GGSIPU

supriya.14489@gmail.com

[2]Computer Science Engineering Department,Ambedkar Institute ofTechnology.GGSIPU

manjukhari@yahoo.co.in

Abstract:

Ad-hoc networks are the collection of autonomous nodes where all the nodes are configured dynamically without any centralized management system. Mobile Adhoc Networks (MANETs) are self-configuring network of mobile routers connected via a wireless link. However,the feature of decentralization and dynamic configuration of nodes makes MANETs vulnerable to various security attacks,that are otherwise not so common in a wired network. For mitigation of these attacks,several secured routing protocols are being proposed till now. This paper provides the view of overall security breaches present in the Ad-hoc Networks till now and will discuss in brief about the several proposed secure routing protocols.

Keywords:

Security breaches, Wormhole attacks, blackhole attacks, byzantine, DDOS attacks, constraints

1 Introduction

Mobile Ad-hoc Networks are the networks comprising of autonomous nodes that utilize multi-hop radio-relaying and work without the support of any infrastructure. There is no centralized mechanism for routing of packets in MANETs. The communication between the nodes is solely on the basis of mutual trust.

In MANETs,the nodes that are available in radio-frequency of each other communicates directly and for communication with other available nodes,intermediate nodes are being used. To provide security to MANETs,a protocol is required which encapsulate a set of all necessary security mechanisms in it.

In order to work in a secure and reliable ad-hoc network environment,some security criterias are necessarily be addressed[1][3]:

Security Attacks in MANETs:

Categorisation of attacks in MANETs is as follows[5]:

- **Active Attacks:** An active attack attempts to destroy or modify the data being exchanged in the network,hence disrupting the normal functioning of attacks. Further these attacks are divided into:
    - **External attacks:** These are carried out by the outsider nodes i.e. the nodes not belonging to the concerned network.
    - **Internal attacks:** These attacks occur because of compromised nodes present inside the network.
- **Passive Attacks:** These attacks do not interfere with the running operations of the network. It just performs the eavesdropping of the data exchanging via the concerned network.

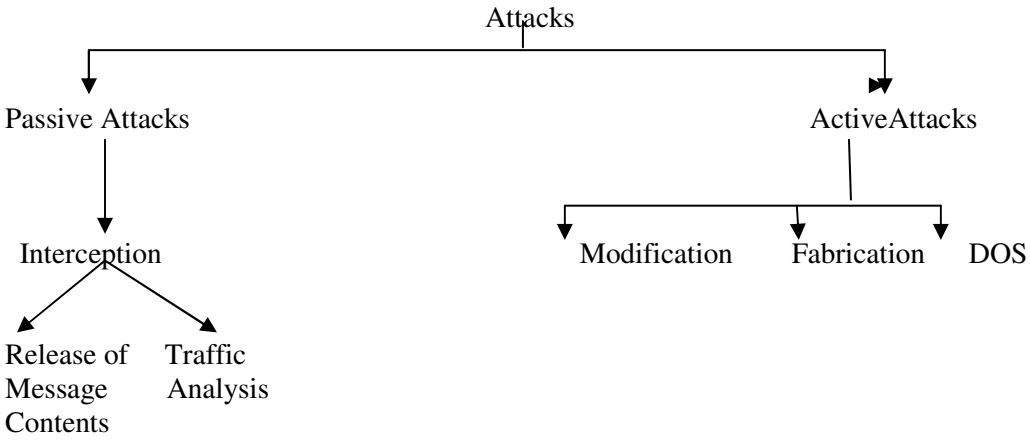

Fig 1: Classification of Attacks

Broad categorization of some of the preliminary attacks on the basis of their active and passive nature.[7]:

Table 1: Categorisation of Attacks

Attack Name	Passive Attacks	Active Attacks
Impersonation		✓
Eavesdropping	✓	
Masquerading		✓
Denial of Service		✓
Traffic Analysis	✓	
Replay		✓
Message Modification		✓

Several major attacks that are being studied till now in order to provide security to MANETs are as follows[2][3][7]:

- **Routing Attacks:** These attacks are aimed on the routing protocols and are being performed in a manner to disrupt the operation of the network.
  These attacks are further categorized into following:

  - Routing Table Overflow
  - Routing Table Poisoning
  - Packet Replication
  - Route Cache Poisoning
  - Rushing Attack

- **Wormhole Attacks:** In wormhole attacks,the malicious nodes pretends to provide the shortest path between the two distant nodes. If the source node opts for this route,then,it gives rise to a loop and the packets sent via this route are either dropped or keep on revolving but don't reach to their legitimate destination.

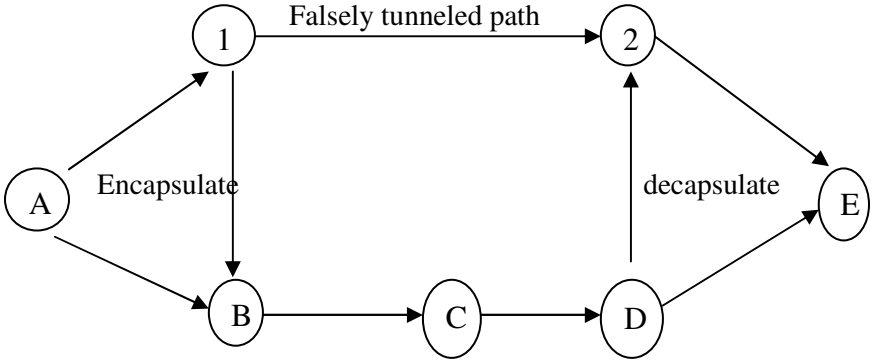

Fig 2: Wormhole Attack

In this fig, source node-A, destination node- E, malicious nodes- 1 and 2.
Malicious nodes are making a tunnel in order to create a fake path between source and destination node, hence making the packet to enter in an infinite loop. This will lead to the loss of packets as it will not reach its legitimate destination. Thus, creating the wormhole attack in the network.

Modes of wormhole attacks[9]:

- Wormhole Attack using Encapsulation
- Wormhole Attack using Out-Of-Band Channel
- Wormhole with High Power Transmission
- Wormhole using Packet Relay
- Wormhole using Protocol Deviations

- **Blackhole Attacks:** In these attacks,the malicious node keep on sending positive replies for the route requests it is getting,inspite of the fact that whether the related routes are available or not.Ultimately,drops all the packets that are routed to its destination via this node.
  Like-Jellyfish Attack

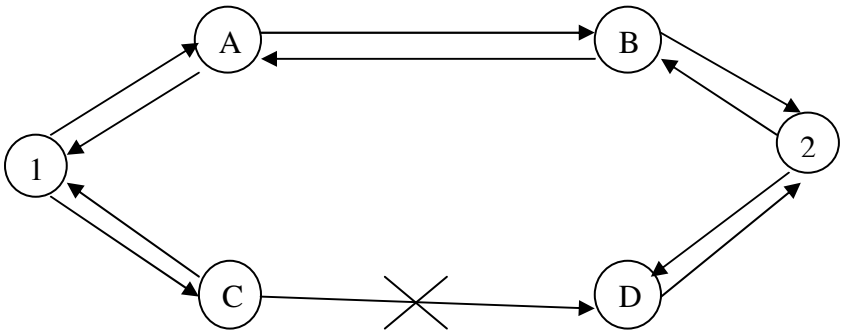

Fig 3: Blackhole Attacks

In this fig, 1 and 2 are source and destination nodes respectively, C is the malicious node.
C will soon advertise its route as the shortest to the source node 1, so that it will assuming it as authenticate reply send the packet to it. It will then, drop the packet as it actually has no valid route to the destination. Hence, creating the blackhole attack.

Blackhole attacks are further categorized into[10]:

- Internal Blackhole
- External Blackhole

- **Grayhole Attacks:** This attack on MANETs also provides the smallest route to the nodes that are searching for a route to send the packets.But here,malicious nodes drops the packets with some probability.There is no certainty of the fact whether the packet will be surely dropped or will be surely forwarded.

- **Denial of Service Attacks:** In this attack,the main aim of the attacker is to flood the network,so that maximum resources of the network are being consumed at their par like network bandwidth and energy resources etc.

  Several DOS attacks are as follows:

  - Sleep Deprivation Torture
  - Jamming Attack
  - SYN Flooding
  - Link Spoofing Attack

- **False Information Attacks:** Malicious nodes commutes the wrong information about the legitimate nodes,hence isolating them while themselves remain connected in the network. This type of attacks includes stacking attack.

- **Incomplete Information:** Malicious nodes misleads the communication process in the network by providing incomplete information.
- **Modification:** Packets may be modified or malicious packets may be inserted in the network by the illegitimate node.

- **Fabrication/Masquerading:** A malicious node having bad reputation in the network,register itself as a new node/new user in the network.
- **Sybil Attack:** In this attack,a malicious node impersonate itself as more non-existent nodes,to give a feel of being several malicious nodes conspiring together.

- **Blackmailing:** This attack makes use of false information attack for propagating wrong reputation of a node hence,blackmailing the node alongwith creating DOS attack.

- **Replay Attacks:** It includes replay of previously captured routing traffic by the malicious node.It is done to create errorneous routing information and misleading the network.

- **Selective Misbehaving Attacks:** Node act as malicious for certain traffic and otherwise remains the good node. Hence,behaving in a selective manner.

- **On-off Attacks:** To conceal its identity and preventing itself from being detected, a malicious node keeps on changing its behaviour between good and bad.

- **Conflicting Behaviour Attacks:** Here,the main aim of malicious nodes is to break the trust-relationship among the legitimate nodes of the network which is the basis of communication in MANETs.

- **State Pollution Attacks:** Malicious nodes provide incorrect responses regarding the requested parameters,leading to broadcast of duplication address detection messages repeatedly.This obstructs the entry of new node in the network.

- **Session Hijacking Attacks:** In this attack,malicious nodes makes use of spoofing attack,hijacks the session by spoofing the ip address of victim's system.

- **Location Disclosure Attacks:** Here,malicious node collects the route map and other information regarding the nodes by analyzing and monitoring the traffic. This helps in planting more attacks onto the network.

- **Device Tampering Attacks:** The main cause of this attack is the absence of central administration which makes it easy for mobile nodes to change their identities.

- **Neighbour Attacks:** In this,attacker/malicious mode forwards the packet without recording the id in the packet,hence providing the misleading route,which will ultimately result in disrupted route.

- **Byzantine Attacks:** Here,the malicious nodes work in collusion and carries out the attack that create more disrupting or degrading attacks.They do so by creating routing loops,selective dropping of packets etc.[8]

Secure Routing Protocols for MANETs:

Mainly,MANETs works on TCP/IP structure for providing the better communication.
Because of the mobility factor of nodes involved in MANETs,they provide efficient functionality but it is the main reason of attacks performed on these networks,some of which we have been discussed so far. Broad categorization of routing protocols is as follows:

- Routing Information Update Mechanism
- Use of Temporal information for routing
- Routing Topology
- Utilization of specific resources
-

Designing issues for a secure routing protocol for MANETs:

- **Mobility:** Routing protocols for ad-hoc networks must be an efficient mobility management protocol that can effectively manage with the path-break disruption occur due to the dynamic topology of the MANETs.

- **Bandwidth Constriants:** In wireless ad-hoc networks,there is an availability of limited radio band. Therefore,for better services,a routing protocol which can use the bandwidth optimally minimizing all the overheads is well-suited for MANETs.

- **Error-Prone Shares Broadcast Radio Channel:** It is must for a wireless ad-hoc network routing protocol to interact with MAC layer so that it always have an availability of alternative routes to avoid collisions to cater the requirement of dynamic topology of ad-hoc networks.[11]

- **Hidden and Exposed Terminal Problems**: There may be the terminals in the network that are not in the transmission range of the sender but are there in the transmission range of the receiver,which may give rise to collision of packets while communication.This is referred to as the problem of hidden terminals.

  To overcome this,an efficient protocol is required like Medium Access Collision Avoidance for Wireless [12], Floor Acquisition Multiple Access [13], Dual Busy Tone Multiple Access [14].

  There may also be a condition in wireless network(MANETs) where a node is blocked due to transmission of a nearby transmitting node that are transmiting to another node. This problem is referred to as exposed terminal problem.

- **Resource Constraints:** The most important and limited resources that become a constraint for nodes in MANETs are battery life and processing power. Therefore, a routing protocol is required which can manage these resources optimally.

Conclusion:

In this paper,all types of attacks to which MANETs are vulnerable are being presented. A brief overview of issues required to be considered for designing a secure routing protocols is also presented towards the end of this paper. However,MANETs are still in a premature state and provides a wide scope of research. To utilize the dynamicity and robustness of these networks successfully and reliably,it is required to understand its security needs. This will enable to mitigate the security breaches and making it a more suitable communication medium. The flexibility and scalability of MANETs will make them an ideal platform for communication in near future.

References:

[1] "Security Issues in Mobile Ad Hoc Networks-A Survey",Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering,University of Maryland,Baltimore County [2007]

[2] "A Survey of Mobile Ad Hoc Network Attacks",Pradip M.Jawandhiya, Mangesh M.Ghonge,Dr.M.S.Ali and Prof.J.S.Deshpande, International Journal of Engineering Science and Technology,Vol.2(9),Pg No-4063-4071 [2010]

[3] "A Review Paper on Ad Hoc Network Security",Karan Singh, Rama Shankar Yadav and Ranvijay, International Journal of Computer Science and Security,Vol.1:Issue(1)[2008]

[4] "Securing Ad-Hoc Networks",L.Zhou and Z.J.Haas, IEEE Network Magazine,Vol.13,No.6,Pg No.24-30 [1999]

[5] "Review of Secured Routing for Wireless Ad Hoc Network",Satish Kumar Garg,International Journal of Computing and Business Research,Vol 2,Issue-1 [2011]

[6] "Rushing Attacks and Defense inWireless Ad Hoc Network Routing Protocols",Y.Hu,A.Perrig and D.B.Johnson ,Proccedings of the ACM Workshop o Wireless Security 2003,pp.30-40,September[2003]

[7] "A Survey on Trust Management for Mobile Ad Hoc Networks",Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen, IEEE Communications Surveys and Tutorials [2011]

[8] "A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad Hoc Networks" K.P.Manikandan, Dr.R.Satyaprasad, Dr.K.Rajasekhararao, International Journal of Advanced Computer Science and Applications, Vol.2,No.3 [2011]

[9] "Approaches towards Mitigating Wormhole Attack in Wireless Ad-Hoc Network",Ms.N.S.Raote and Mr.K.N.Hande,International Journal of Advanced Engineering Sciences and Technologies, Vol.2,Issue No.2,Pg no.172-175 [2011]

[10] "Security Threats in Mobile Ad-Hoc Network", K.Biswas and Md.Liaqat Ali Blekinge Institute of Technology, Sweden [2007]

[11] "Solutions to Hidden Ternimal Problems in Wireless Networks",C.L.Fullmer and J.J.Garcia-Luna-Aceves,Proceedings of ACM SIGCOMM, Pg no.39-49 [1997]

[12] "MACAW: A Media Access Protocol for Wireless LANs", V.Bharghavan, A.Demers,S.Shenker and L.Zhang, Proceedings of ACM SIGCOMM Pg No.212-225 [1994]

[13] "Floor Acquisition Multiple Access(FAMA) for Packet-Radio Networks", C.L.Fullmer and J.J.Garcia-Luna-Aceves,Proceedings of ACM SIGCOMM, Pg no.262-273 [1995]

[14] "Dual Busy Tone Multiple Access(DBTMA):A New Medium Access Control for Packet Radio Networks", J.Deng and Z.Haas Proceedings of ICUPC, Vol 1, Pg.no.973-977 [1998]