ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Security Issues in MANET: A Review

Pulkit Berwal
Department of Electronics and Communication
pulkit.berwal123@gmail.com

Abstract

A Mobile Ad hoc (MANETs) is a Dynamic protocol wireless network that can be created without any pre-existing infrastructure in which each node can operate as a router. It has no fix boundaries, so it is accessible to both legitimate network users and malicious attackers. The main challenge is to design a secure solution which can protect the MANET from various kinds of security attacks. In this paper, we consider the most common types of attacks, namely snooping, rushing attack, blackhole attack, flood storm attack. — One of the major reasons to address the security aspects in MANETS is the usage of wireless transmission medium, which is highly susceptible or vulnerable to attacks.

Keywords: MANETs, Security, Leashes, Wormhole , Attack, Intrusion Detection

Introduction

This A MANET[1] is a type of self forming network similar to stationary mesh networks. Every device-whether a notebook computer, Smartphone, or wireless router serves as relay point. Unlike a wireless hotspot, in which devices connect to a single router like spokes to a hub, on a MANET data can hop from wireless device to wireless device, forming a chain. MANETs have characteristics that network topology changes very rapidly and unpredictably in which many mobile nodes moves to and from a wireless network without any fixed access point where routers and hosts move, so topology is dynamic. MANETs support Multi hop paths for connection between nodes and can have multi hop over links, also connection point to the internet may also change. Connection point to the internet may also change. Communication can be done directly from source to destination between nodes which are in range but if nodes are not in range then it can communicate through intermediate node [2]. The open structure, lack of existing infrastructure and un-accessibility to trust as servers make traditional security methods and system insufficient for application in mobile wireless ad hoc networks. Achieving different levels of security therefore represents a major issue for the distribution and use of ad hoc network. Routing protocols for
ad hoc networks need to account for several aspects. Since nodes can move around, and enter and leave the network, the network topology can change rapidly. So the security issue is an important and different than those that exist in conventional networks. Wireless networks are more vulnerable to attacks than wired networks due to open medium, dynamic changing network topology, cooperative algorithm, lack of centralized monitoring and lack of clear line of defense. Ad hoc networks are vulnerable to security attacks on both physical and virtual levels [3].

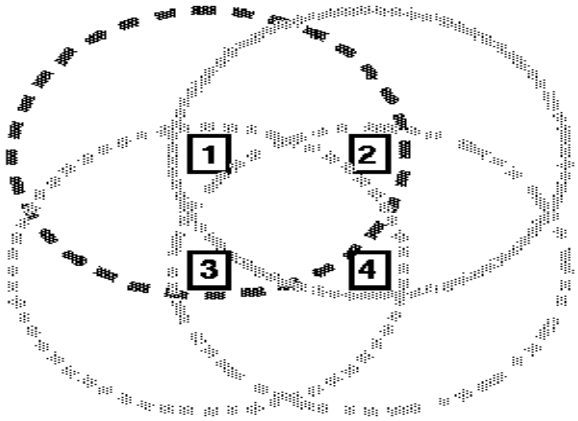

Fig. 1. MANETs

Security Attributes

MANETs are especially sensitive to security attacks; because the dynamic nature and lack of infrastructure make data transmission can be easily intercepted and corrupted. Thus it is very important to provide strong security mechanisms.

A. Confidentially: This service provides security such that information must not really others, not only data, routing information must also remain secure.

ISSN: 2277-9655
Impact Factor: 1.852

B. Integrity: This service assures that the message is received as sent such that one shouldn't be able to modify the data transit.
C. Authentication: This service guarantees that the communication is authentic. The receiver should be able to identify the sender correctly. No other person can disguise as the sender.
D. Non-repudiation: This service prevents either sender or receiver from denying a transmitter message. This is useful for detection and isolation of compromised nodes.
E. Access control: Authorized nodes can handles the information. The service requires that the authenticate service be available.
F. Key Management and Exchange:This service allows negotiating security keys between communication entities. While other security services can be implemented in a similar manner for unicast and multicast communications, the key management service is much harder to extend from unicast to multicast.

Challenges in Security

In this section we discuss about various vulnerabilities that exist in the mobile ad hoc networks.
A. Unconsistent wireless links between nodes Mobility of nodes and limited energy supply for the wireless links between nodes for the communication participants.
B. Dynamic Topology:Due to dynamic nature of MANETs, multi hop network topology may change randomly and rapidly at unpredictable time. A priori trust cannot be developed, since no central administration is maintained. It is necessary for each pair of adjacent nodes to incorporate in routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.
C. Lack of Secure Boundaries:As in traditional wired networks, these are no clear secure boundaries in MANETs that increases vulnerabilities. Malicious nodes can meaningfully altered, discard forge, inject and replay control and data traffic, generate floods of spurious message and in general avoid complying with the employed protocols.
D. Selfish Nodes:Detection of selfish activities is tricky. Nodes may refuse participation to preserve power or, avoid congestion (black hole attack). Some nodes may refuse to forward packets in order to conserve their limited resources (for example, energy), resulting in traffic disruption. Nodes exhibiting such behavior are termed selfish [4]. Selfishness is usually passive behavior. Additionally, malicious nodes may intentionally, and without concern about their own resources, attempt to disrupt network operations by mounting denial-of- service attacks or by actively degrading the network performance.
E. System failure:Communication failures like fading, loss of packets, blocking and congestion are common. Therefore malicious failures will be more difficult to distinguish.
F. Physical Security: Mobile nodes, while roaming in a hostile environment might face physical insecurity. So measures are needed to make the nodes temper resistant.

Attacks in Manets

A. Jamming:Jamming is defined as a DoS attack that interferes with the Communication between nodes. The objective of the adversary causing a jamming attack is to prevent a legitimate sender or receiver from transmitting or receiving packets. Adversaries can launch jamming attacks at multiple layers of the protocol suite.. This condition is called jamming. Jamming attacks can be mounted from a location remote from the targeted network.
B. Snooping: Due to broadcast nature of radio signals from transmitter, it is possible to eaves drop packets. Due to inherent trust between mobile nodes, they are allowed to look at the whole packet data.
C. Wormhole Attack: In a wormhole attack a malicious node can record packets (or bits) at one location in the network and tunnel them to another location through a private network shared with a colluding malicious node [5]. As a result, network would be unable to find consistent routes to any destination and performance is securely degraded.
D. Blackhole Attack: A black hole is a malicious node that falsely replies for route requests without having an active route to the destination. It exploits the routing protocol to advertise itself as having a good and valid path to a destination node. It tries to become an element of an active route, if there is a chance. It has bad intention of disrupting data packets being sent to the destination node or obstructing the route discovery process. Cooperative black hole attack is caused by many neighbor black holes cooperating each other. Black hole attack may be internal or external.
E. Flood Storm Attack: This is a Denial of Service Attack. Malicious node deliberately floods the whole network with meaningless Route Request(RREQ) and Route Reply (RREP)messages.
F. Packet Modifications and Dropping: It is possible for intermediate nodes to modify the packet content, if proper integrity checks are not maintained. Also it is possible to change the header information including source and destination address. Any node can take the role of router, which is not the case in wired network, where dedicated machines are routers. The malicious intermediate nodes can also simply drops data or route packets. Such types of attacks can be

detected by Secure Neighbor Detection Techniques discussed in further sections.

G. Rushing attack: In rushing attack, a malicious node wants a route to be established through it. For this purpose, a malicious M node waits for route request RREQ of sources either selectively or collectively. Whenever the RREQ arrives, the malicious node M rushes the request to the next intermediate node, in a hope to get a route through it. The probability of getting a route through M is higher, because of the property of all nodes to select the first RREQ and forward it, and discarding the duplicate RREQ.

Security Solutions in Manet

Intrusion detection system applied in wired networks cannot apply directly to MANETs. The optimal IDS architecture for a MANET may depend on the network infrastructure itself.

A. Stand-alone Intrusion Detection System

Intrusion Detection is run independently on each node, no cooperation between nodes established, decision made only on information collected as its own node[6]. This type of Intrusion Detection System is not effective and suitable only for Flat infrastructure than for multilayered network infrastructure.

B. Distributed and Cooperative Intrusion Detection System

In this type of Intrusion Detection System, node cooperate with each other means every node participate in intrusion detection and response by having an IDS agent running on them [7]. Responsibility of IDS is to detecting and collecting local event and data to identify possible intrusion detection and response to independent node. It is more suitable than first one. Zhang and Lee propose this type of System.

C. Packet Leashed

Packet Leashed is a mechanism to detect a wormhole attack. In wormhole attack, an attacker records packet at one location in the network, tunnels them to another location, and retransmit them into network. Leash is any information added to packet designed to restrict the packets maximum allowed transmission distance [8]. Geographical leash insures that the recipient of the packet is within a certain distance from sender and Temporal leash ensures that the packet has an upper bound of its lifetime (restrict the maximum travel distance).

Conclusion

Now days the area of security is very important. The area of security in wireless ad hoc network has been attracting much attention. While many problems have been addressed, there are many others that need attention. Area of security is to be explored as there are many issues which still need some attention of researchers. There is need to design more secure protocols to deal with these security problems. A lot of works is to be done in the field of security issues of MANET. This paper discuss the basic properties of the MANET, the vulnerabilities unit, different types of attacks, secure protocols provided by the researchers.

References

[1] C.E.Perkins, E.M.Royer, I.D.Chakers, “Ad hoc On-Demand Distance Vector (AODV) Routing Protocol”, draft-perkins-manet-aodvbis-00.txt, October 2003.

[2] I.F.Akyildiz, W.Su.Sankaransubramaniam and E.cayira, Wireless sensor networks: a survey.

[3] T. Karygiannis and L. Owens, “Wireless Network Security, 802.11, Bluetooth and Handheld Devices,” NIST Publication, p. 800(48), November 2002.

[4] P. Michiardi and R. Molva, “ Simulation based analysis of security exposures in mobile ad hoc networks,” Proceedings of the European Wireless Conference, February 2002.

[5] David B. Johnson and David A. Maltz. “Dynamic Source Routing in Ad Hoc Wireless Networks”. In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996.

[6] R. Heady, G.Luger, A.maccabe and M.serviller, The architecture of a network level intrusion detection system, Technical Report, Computer Science Department, University of New Mexico (August 1990).

[7] Lundin E, Jonsson E.(2002) Survey of Intrusion Detection Research, Technical report 02-04, Dept. of Computer Engineering, Chalmens University of Technology.

[8] Y. Desmedt. Major Security Problems with the “Unforgeable” (Feige-)Fiat-Shamir Proofs of Identity and How to Overcome Them. In proceedings of the 6th worldwide computer congress on computer and communications security and protection (SecuriCom 88), pages 147–159, March 1998.