Survey on Distributed Certificate Authority Services and Security for Wireless Mesh Network

Shreya singh, Mr. Rishi Srivastava
Department of CSE
Babu Banarasi Das University Lucknow,India

ABSTRACT- Wireless mesh network has become very popular technology. Wireless mesh networks continue to receive important interest in an existing new technology that has application in military and disaster recovery etc. It allow a fast easy and inexpensive network deployment .Secure communication is very important in computer network and authentication is one of the most eminent preconditions however normal authentication scheme is not possible in wireless mesh network .In wireless mesh network security is the main issue of single certificate authority so we will use distributed certificate authority.

Keywords- Wireless mesh networks, wireless mesh network architecture, mesh router, mesh client, Security services, and security attacks, distributed certificate authority.

INTRODUCTION- Wireless mesh network topology is a new technology which is very beneficial for near future because wireless mesh network provide fast speed, low cost and easy deployment. It is a communication network which is made up of radio nodes and organized in mesh topology. In wireless mesh network each node is connected to several other nodes and if one node drops out of the network, its neighbors simply find another route. A wireless mesh network is wireless network where data is transmitted using mesh networking. That is, where nodes don't just send and receive data but also serve as a relay for other nodes and each node collaborates in propagating data on the network. Wireless mesh routers and wireless mesh clients are main component of wireless mesh network. Wireless mesh routers are same as conventional router it includes functionality of gateway and repeater. It creates backbone of wireless mesh network and it is a communication node and support others wireless sensor node, Wi-Fi, wimax etc for communication with different network. Wireless mesh router is static and fixed. Wireless mesh routers are directly connected to wire network. Wireless clients are same as mesh clients but it is includes some different functionality. Wireless mesh clients are dynamic because it changes its position, wireless mesh clients connected through a wireless link. Mobile, laptop PDA and printer are example of wireless mesh client.

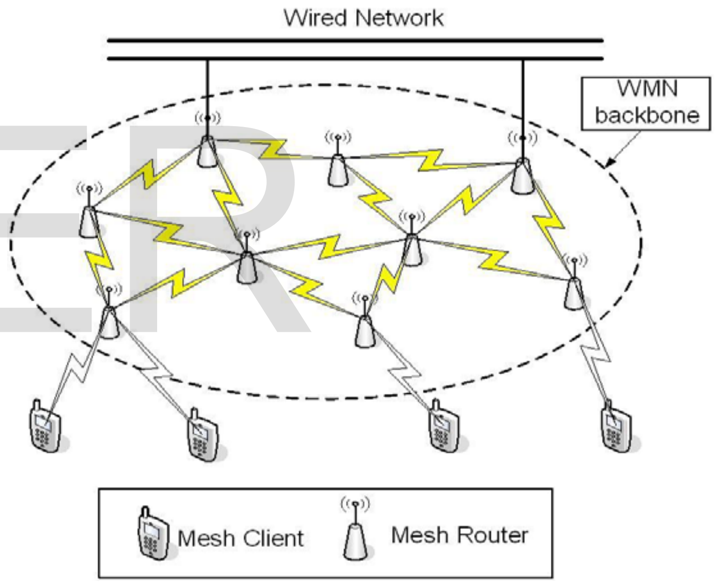

Fig: wireless mesh network

Architecture of wireless mesh network

Wireless mesh networks have three architectures.

1. Infrastructure/backbone wireless mesh networks.
2. Client wireless mesh networks.
3. Hybrid wireless mesh networks.

Infrastructure wireless mesh network: Infrastructure/backbone WMNs are composed of mesh routers which are relatively static and offers direct connectivity to the client. It is directly connected to internet with the help of (DSL) cable. It is also support the access of different type of network. For example wireless sensor network, Wi-Fi, WI-Max etc.

Client wireless mesh networks: It is made up of only with the help of mesh clients. In this architecture has no involvement of wireless mesh routers. Every client on this topology is self configured and act as a router for the other client in this architecture. It is dynamically changing topology with infrastructure-less networks.

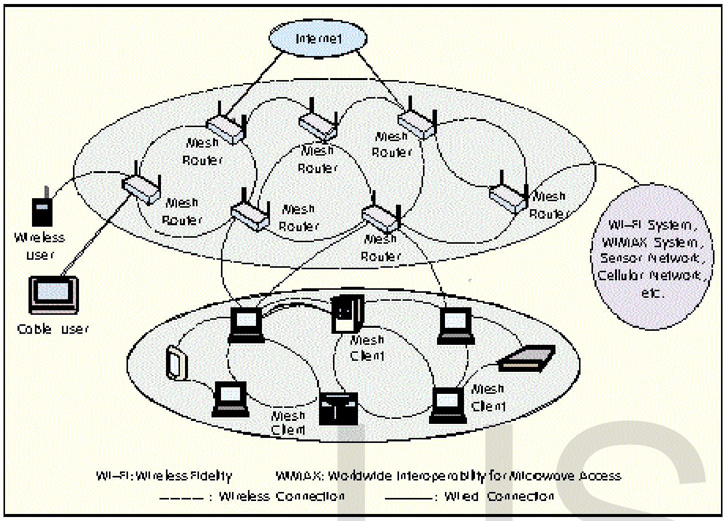

Figure 2:

Hybrid wireless mesh network: As its name indicates it is combination of infrastructure and client wireless mesh network. It has property of both infrastructure/backbone and client wireless mesh network. Mesh client also connect with mesh router infrastructure by which client can access the internet. It is also support the different type of network such as Wi-Fi, Cellular and sensor network etc.

Security services of wireless mesh network:

Confidentiality

Integrity

Availability

Access control

Non repudiation

Confidentiality: It is service of WMNs security. It promises that any unauthorized person cannot access the important information of packets, because wireless mesh networks are used in Military to send important message from one place to another place and it is also used in banks.

Integrity: It is also service of WMNS security. It promises that only authorized person can change, modify, insert or delete something from the original packet of information.

Availability: It is a service of WMNs security. It promises that each resource is available for only authorized users.

If above security services are followed by WMNs, then we can call that WMNs are secured.

Access Control: It provides protection against unauthorized access to packet.

Non repudiation: This service protects against repudiation by either sender node or receiver node of the packet.

Security Attacks in WMNs: There are some threats that violate the security criteria of wireless mesh networks which are known security attack. In wireless mesh network, attacks are easily possible because wireless mesh network infrastructure made by wireless routers and attacker can easily capture to the wireless mesh router. An attacker can extract the packet of information and it performs unauthorized action as an authorized user.

Attacks are two types-

Active attack: In active attack attacker can perform any operation like insertion, deletion or alteration. An active can be easily detected.

Passive attack: This type of attack is very dangerous because in this attack, attacker only access the information. Attacker cannot perform any action with the information. So it is very difficult for detection.

These are different type of attack

Denial of service attack: It is very common attack in network. In this attacker sends many requests to a targeted node. Network crash will occurs because of the flooding, i.e. overloading nodes.

Sybil attack: In Sybil attack, a malicious node pretends the identity of several nodes. By doing so undermining, the effectiveness of fault-tolerance schemes, such as redundancy of many routing protocols. By using Sybil attack, an adversary can act in more than one place at the same time.

Selfish and greedy behavior attack: A node increases its own share of the common transmission resource by falling to adhere to the network protocol by tempering with their wireless interface.

Selective forwarding attack: In this attack certain messages will be dropped by malicious node.

Sinkhole attack: It is also known as black hole attack, attacker surprisingly announces the short path to sink in order to attract traffic and when attracts the messages drops them or run selective forwarding attack.

Routing table overflow: In this attack, an attacker try to create routes to imaginary nodes with intension to create enough route to avoid routes from begin created or to overcome the protocol implementation.

Conclusion: In this paper we have discussed about the wireless less mesh network and its Characteristics and also discuss about security services and security attacks. We conclude security attacks in wireless mesh networks. In WMNs most attacks are much harder to count because the attacker is aware of the network secrets and protocols. An attacker drops only few packets, due to congestion or poor wireless congestion. However current security approaches may be effective to a particular WMNs, but still lack of mechanism to prevent from attack in different protocol to prevent. Wireless mesh networks are very useful for future because it provide many facilities for users.

References

1. **Rabbi, Md. Taufiqur Rahman, Md. Afser Uddin,G.M. Abdullah Salehin An Efficient Wireless Mesh Network : A New Architecture**
2. **Muhammad Shoaib Siddiqui,Choong Seon Hong Security Issues in Wireless Mesh Networks 2oo7 IEEE**
3. **Na Wangs, Hengjun Wang A security architecture for wireless Mesh Network 978-0-7695-3972—0/10$26.00@2010 IEEE.**
4. **IAN F. AKYILDIZ,GEORGIA INSTITUTE OF TECHNOLOGY XUDONG WANG KIYON, INC.A SURVEY ON WIRELESS MESH NETWORK**
5. **Samir R. DAS stony Brook University, SUNY Wireless mesh networking**

6. Ben salem,J.-p.Hubaux,"Securing wireless mesh networks,"wireless communication IEEE2006 .

7. Indre Egners,Ulrike Meyer "Wireless Mesh Network Security: State of Affairs"on