Security Aspects in Wireless Mesh Network

Sonal R. Jathe
ME(Final Year), Dept of CSE, SIPNA's College of Engineering, Amravati (MS) INDIA
sonal_jathe@rediffmail.com

Dhananjay M. Dakhane
Assistant Professor, Dept of CSE, SIPNA's College of Engineering, Amravati (MS) INDIA

ABSTRACT
Wireless Mesh Network (WMN) is an emerging technology. WMN represents whole new network concept, and has the nature of wireless and multi-hop, so security is a critical problem. A wireless mesh network (WMN) is a mesh network created through the connection of wireless access point installed at each network user's locale. Each network user is also a provider, forwarding data to the next node. The networking infrastructure is decentralized and simplified because each node need only transmit as far as the next node. This paper consist of the introduction of the computer network ,comparison of wired and wireless LAN network, wireless mesh network, advantages and characteristics of WMN, security problems and solutions for it .

Keyword: Network, MANET, Multi-hop, Mesh Network, Wireless Mesh Network .

1 INTRODUCTION
Wireless mesh networking [1] could allow people living in remote areas and small businesses operating in rural neighborhoods to connect their networks together for affordable Internet connections. Firstly, we see the types of computer network, mesh network, wireless mesh network, characteristics and advantages of WMN, attacks on WMN, and solution to security problem.

A) Computer Network

The types of network are categorized on the basis of the number of systems or devices that are under the networked area [2].

Networking is the process by which two or more computers are linked together for a flawless communication. By creating a network, devices like printers and scanners, software, and files and data that are stored in the system can be shared. It helps the communication among multiple computers easy.

1) LAN - Local Area Network - A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs.

2) WAN - Wide Area Network - A WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a Router connects LANs to a WAN.

3) Wireless Local Area Network - A LAN based on Wi-Fi wireless network technology.

4) Metropolitan Area Network – A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city.

5) Campus Area Network – A network spanning multiple LANs but smaller than MAN, such as on a university or local business campus.

6) Storage Area Network - Connects servers to data storage devices through a technology like Fiber Channel.

7) System Area Network - links high-performance computers with high-speed connections in a cluster configuration. Also known as Cluster Area Network.

B) Comparison of wired and wireless LAN network –

Local Area Network-

Computer networks for the home and small business can be built using either wired or wireless technology. Wire Ethernet has been the traditional choice in homes, but Wi-Fi wireless technologies are gaining ground fast. Both wired and wireless can claim advantages over the other; both represent viable options for home and other LAN.

Below we compare wired and wireless networking in five key areas[2]:

- ease of installation
- total cost
- reliability
- performance
- security

About Wired LANs -
Wired LANs use Ethernet cables and network adapter. Although two computers can be directly wired to each other using an Ethernet crossover cable, wired LANs generally also require central devices like hubs, switches, or router to accommodate more computers.

1) Installation -
Ethernet cables must be run from each computer to another computer or to the central device. It can be time-consuming and difficult to run cables under the floor or through walls, especially when computers sit in different rooms. The correct cabling configuration for a wired LAN varies depending on the mix of devices, the type of Internet connection, and whether internal or external modems are used. After hardware installation, the remaining steps in configuring either wired or wireless LANs do not differ much. Both rely on standard Internet Protocol and network operating system configuration options.

2) Cost -
Ethernet cables, hubs and switches are very inexpensive. Some connection sharing software packages, like ICS, are free; some

cost a nominal fee. Broadband routers cost more, but these are optional components of a wired LAN, and their higher cost is offset by the benefit of easier installation and built-in security features.

3) Reliability -

Ethernet cables, hubs and switches are extremely reliable, mainly because manufacturers have been continually improving Ethernet technology over several decades. Loose cables likely remain the single most common and annoying source of failure in a wired network. When installing a wired LAN or moving any of the components later, be sure to carefully check the cable connections. Broadband routers have also suffered from some reliability problems in the past. Broadband routers have matured over the past several years and their reliability has improved greatly.

4) Performance-

Wired LANs offer superior performance. Traditional Ethernet connections offer only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs little cost more and are readily available. Although 100 Mbps represents a theoretical maximum performance never really achieved in practice, Fast Ethernet should be sufficient for home file sharing, gaming, and high-speed Internet access for many years into the future.

5) Security-

For any wired LAN connected to the Internet, firewalls are the primary security consideration. Wired Ethernet hubs and switches do not support firewalls. However, firewall software products like Zone Alarm can be installed on the computers themselves.

2 MESH NETWORKING

Mesh Network[2] is a type of networking where each node must not only capture and distribute its own data, but also serve as a relay for other sensor nodes, that is, it must collaborate to propagate the data in the network. A mesh network can be designed using a flooding technique or a routing technique. When using a routing technique, the message propagates along a path, by hoping from node to node until the destination is reached. A mesh network whose nodes are all connected to each other is a fully connected network. Mesh networks can be seen as one type of ad hoc network. Mobile Ad hoc Network (MANET) and mesh networks are therefore closely related, but MANET also have to deal with the problems introduced by the mobility of the nodes.

Fig.1 A diagram of a typical Partial Mesh Topology Network

3 WIRELESS MESH NETWORK (WMN)

WMN[2] is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, cell phones and other wireless devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet.

A wireless mesh network can be seen as a special type of wireless ad-hoc network. A wireless mesh network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area.

3.1 Advantages of wireless mesh networks include:

- Decreased need for Internet gateways.
- Collaborative redundant backup technology, which insures data security in the event of disk failure.
- The ability to configure routes dynamically.
- Lower power requirements, which could potentially be met by low-cost or renewable energy sources.
- Increased reliability: Each node is connected to several other nodes and if one drops out of the network, its neighbors simply find another route.

3.2 The Characteristic of WMN

The brief summary of the characteristics of WMN is listed as;

- WMN employs the Ad Hoc Network and hence has the abilities of self-initialization, self-reparation and self-organization.
- WMN is a wireless multi-hop network based on the backbones as part of the wireless infrastructure.
- The mobility of terminals could be easily supported by the wireless infrastructure.
- WMN is not stand-alone and should cooperate and be compatible with other types of wireless networks.

3.3 Problems In Security Of Wmn

In the design of WMN, security is important problem. Some common threats In WMN are as follows:-

Physical Threat: - Routers in WMN usually spread outdoors like on roofs of building. So, physical protection to routers of WMN is very weak.e.g. tempering the information in the router., stealing the private key for authentication stored in router.

Authentication in WMN: - For preventing an unauthenticated node from connecting to WMN. Every nodes joins WMN should able to verify the identities of others.

In WMN for authentication asymmetric cryptography is problematic due to energy limitation.

3.4 Difficulties in providing Security in WMNs

There are some difficulties in providing the security in WMN which are describes as follows[3]:

1). Shared Broadcast Radio Channel -It is the security problem in the WMN; as the radio channel is same for the sending and receiving the data so there is the possible attack like MAC Layer eaves dropping or the reply back.

2). Lack of association -It is another security problem in WMN as the authentication is poor in the WMN. All of the authentication is done via sending the shared keys.

3). Physical Vulnerability - In this is the main problem lies in the WMN. The problem is like the replacement of the mesh router

4). Limited Resource Availability - In this, as the resource is limited in the WMN so there is limitation of mesh router and client and the communication overhead.

3.5 Attack types in WMN

WMN may be susceptible to routing protocol threats and route disruption attacks. These threats are unique to WMNs[4].

1).Black hole attack:-

The malicious node always replies positively to a Route Request although it may not have a valid route to the destination. Almost all the traffic within the neighborhood will be directed toward the malicious node, which may drop all the packets.

M replies positively to every route request

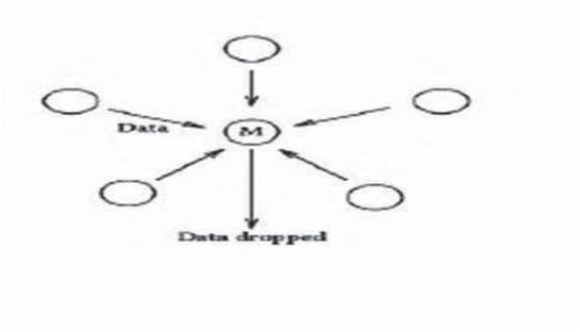

Fig 2. Black hole attack

2. Gray hole attack:-

An attacker creates forged packets to attack and selectively drops, routes or inspects network traffic.

3. Worm hole attack:-

Routing control messages are replayed from one network location to another, which can severely disrupt routing.

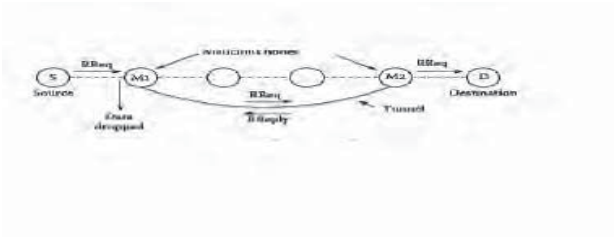

Fig.3 Worm hole attack

If an attacker connects node M1 and M2 using wormhole link then the route becomes S-M1-M2-D. M1and M2 are malicious nodes, could start dropping packets and cause network disruption.

4.Rushing attack:-

In On Demand routing protocol,attacker sends a lot of routing request packets across network in short interval of time keeping other nodes busy from processing legal routing request packets.

4 SOLUTION TO SECURITY PROBLEMS ON ROUTING PROTOCOLS :-

Routing protocol is important part of WMN and and it directly determine the implementation of network function and it's efficiency.

Some secure Routing Protocols are[5]:-

A) SRP(Secure routing protocol):-

SRP extends on demand routing protocol with ability of identifying discarding false routing information and eliminates attacks of tempering,forging.SRP ensures acquiring coorect topological information. Prerequisite condition of SRP is key shared between Source and destination.

B) Ariadne [6]:-

Suitable for DSR,using Tesla technology. TESLA is verification mechanism, which verifies the data packet by messenger authentication code(MAC). Source sends messenger and MAC first, and sends key for the verification of MAC. And at destination receiver stores messenger first and then verifies it using key. Prerequisite condition is, Source and destination have shared key and every node in network possess the initial verification value of other node.

C) ARAN:-

ARAN is suitable for on demand routing protocol. It uses public key certificate for verification of routing information. Prerequisite condition of ARAN is establish a certificate server responsible for issuing and maintaining the public key certificate of every node.

D) SLSP:-

Secure link state routing for MANET. SLSP is a secure protocol based on link states. Prerequisite condition of this protocol is every node has a pair of public and private key.

SLSP has two functions:-

- It could prevent IP address tempering.
- It could record the packets sending frequency of neighbors. And if it is higher than given value.

5 CONCLUSIONS

In summary, WMN is dynamically self organization and self configuration network by sending up MANET, for its internal nodes to obtain connectivity of nodes.

WMN is hybrid network of WLAN and MANET.WMN combines the advantages of WLAN and MANET providing large-capacity, high-speed and wide-covered network connection and is ideal model to solve the last-mile problem in wireless network distribution.

In the design of WMN routing protocols encounters many problems like mobility and security. For WMN, there are no. of attacks.

Routing protocol from MANET applied to WMN and problem of mobility solves but security problem are critical. Various secure routing protocols solve the security problems. So, in WMN it is important to find the proper way to solve security problem.

6 REFERENCES

[1] Mesh Networking by,en.wikipedia.org/wiki/Mesh Networking.Wireless Mesh Network by, en.wikipedia.org/wiki/Wireless Mesh Network

[2] Bradley Mitchell Wired versus Wireless Networking and Computer Network.

[3] Anil Kumar Gankotiya and Sahil Seth, Gurdit Singh, 'Attacks and their Counter Measures in Wireless Mesh Networks', Department of Computer Science, PEC University of Technology, Chandigarh, India

[4] A. Gerkis, 'A Survey of Wireless Mesh Networking Security Technology and Threats'.

[5] Ping Yi1, Tianhao Tong, Ning Liu, Yue Wu, Jianqing Ma, 'Security in Wireless Mesh Networks: Challenges and Solutions', Information security national engineering laboratory, School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai.

[6] Yih-Chun Hu, Adrian Perrig, David B. Johnson,' Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks', Proceedings of the MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA

Author Biographies

Ms. Sonal R. Jathe is a student of Sipna College of Engineering and Technology, Computer Science and Engg.[M.E.] Amravati, Sant Gadge baba Amravati University. She has published 2 papers in National Conferences. Her area of interest is network security and database.

Prof. Dhananjay M. Dakhane is working as a Associate Professor in Department of Computer Sci & Engineering, Sipna College of Engineering and Technology, Amravati, Sant Gadge baba Amravati University. He has Published 17 papers in National and International Conferences. He has Guided 8 M.E. Students and 35 BE students. Presently he is doing its research at Sant Gadge baba Amravati University. His area of interest is open source security, network security and information and web security.