ISSN:0975-9646

Survey on Security Mechanisms in Wireless Mesh Networks

Priti Gupta , Suveg Moudgil

CSE Department, KUK University,

Haryana, India

***Abstract*— Wireless Mesh Networking is an emerging technology in order to provide a possibility to build a network that can grow in terms of coverage to offer service access (i.e. internet access) for a large number of people with different needs. Security has become the main concern to provide safe communication between different mesh nodes. The aim of this research is to study various security mechanisms and authentication models. The objective is to study various scheduling mechanisms such as distributed scheduling and centralized scheduling, possibility of wormhole attack in adhoc networks, threshold authorization model with clustered certificate authority and a high efficiency wormhole detection algorithm.**

.

***Keywords*— Wireless Mesh Networks, Security Mechanisms, Authorization models, wormhole attack, GPS, Wormhole Attack Prevention**

I. INTRODUCTION

The wireless mesh networking has emerged as a promising technology for future broadband wireless access. A wireless mesh network (WMN) [1] consists of mesh nodes which form the backbone of the network. WMN also consist of mesh clients, mesh gateways, and mesh routers. The nodes are able to configure automatically and re-configure dynamically to maintain the mesh connectivity which gives the mesh "self-forming" and "self-healing" characteristics. The need for centralized management [2] is removed due to this self sufficient relationship between the mesh nodes. Intelligent routing allows mesh nodes to route data packets for nodes that may not be within direct wireless range of each other. Thus over multiple hops information can be routed from source to destination. Especially for backhaul communication, this has a big advantage in terms of network reliability over traditional single hop networks. A wireless mesh node consists of a wireless router and an antenna. It could be installed indoors or in a weather-proof enclosure outdoors. The antenna could be the standard indoor omni-directional antenna or it could be an externally mounted omni directional or directional antenna. It communicated with end clients and mesh nodes.

In wireless mesh networks (WMNs) wireless mesh routers form densely interconnected multi-hop topologies. For local communication and routing to a wired access network the routers automatically configure a wireless broadband backbone. Three kinds of wireless mesh networks can be identified:

1) In infrastructure WMNs [3] (Figure 1.1) mesh routers form a network offering connectivity to clients. The network is meant to be self-configuring and self-healing and to offer gateway functionality for connections to wired networks.
2) Client WMNs are ad-hoc networks formed by clients amongst themselves. None of the dedicated routers or infrastructure exists, so that the clients have to be self-configuring and act as routers for the traffic in the client WMN (if mobility is there then Client WMNs are very similar to MANETs). In this type of architecture, client nodes constitute the actual network to perform routing and configuration functionalities as well as providing end-user applications to customers.
3) Hybrid WMNs [3] combine the advantages of the two other WMNs. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. The infrastructure provides connectivity to other networks such as the Wi-Fi, Internet, cellular, and sensor networks and inside WMNs the routing capabilities of clients provide improved connectivity and coverage.

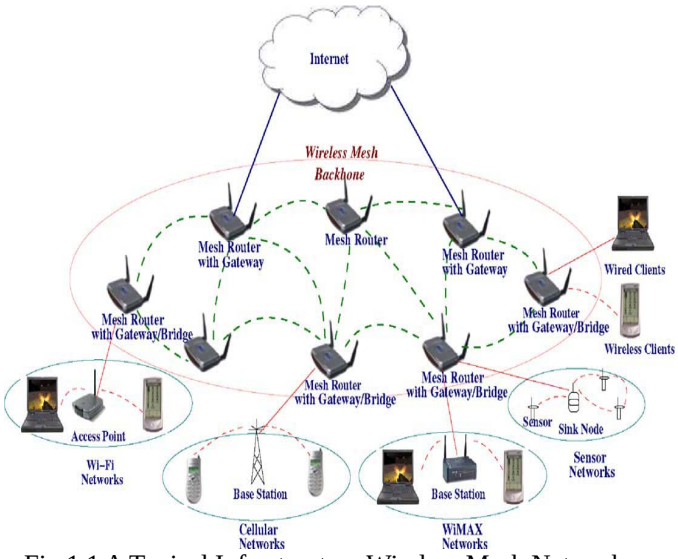

Fig.1.1 A Typical Infrastructure Wireless Mesh Network

II. SECURITY IN WIRELESS NETWORKS

As we look at Wi-Fi security [4], it is dangerous to concentrate on defending against a certain type of attack or to focus only on one security mechanism, such as data encryption. Also, it is wrong to ignore security weaknesses just because they have low consequences. The main difficulty in establishing a wireless network is being able to support effective security so that users can access network without fear of leaking mission-critical data through the

airwaves in or near the perimeter of office building. Security of WLAN remains an area of great debate and concern for the foreseeable future. The problem with most wireless LANs [5] is that security is often considered optional and is turned off by default on every system. The entire premise of a wireless network is a wonderful convenience; however it has no security out of the box. It becomes user's responsibility to determine how best to enable security so that people don't attempt to access your network without your knowledge. Why don't most people enable security by choice? This is an important question that has a simple answer. An 802.11b network, for example, with the best possible range and signal, has a maximum throughput of 11 Mpbs. Today people are finding wired 100 Mpbs LANs too congested for transferring files and other large objects over the network[4]. When you enable security on a wireless device, there is a certain degree of overhead that reduces the overall speed of your connection because it is effectively encrypting your network traffic on one end and decrypting it on another end. While the computer processes this information quite quickly, it cuts into your overall speed.

A. Security Attack

The main threats that violate the security criteria, which are generally known as security attacks are :-

1) *Denial of service attack***:** DOS attacks [6] are most common in networks which connect to internet and since WMNs are mainly designed for fast and long distance internets access this type of attacks are common in the network.
2) *Node capture attack***:** An attacker physically captures nodes and compromises them such that readings sensed by compromised nodes are manipulated or inaccurate [7]. In addition, the attacker may attempt to extract essential cryptographic keys (e.g., a group key) from wireless nodes that are used to protect communications in the very most wireless networks.
3) *Selective forwarding***:** In selective forwarding attack, instead of forwarding every message malicious nodes simply drop certain messages. Once a malicious node cherry picks on the messages, the latency is reduced and deceives the neighbouring nodes that they are on a shorter route. Effectiveness depends on following two factors:
   a) The percentage of messages it drops.
   b) Location of the malicious node, the closer it is to the BS (base station) the more traffic it will attract. When selective forwarder drops more messages and forwards less, the energy level is retained thus remaining powerful to trick the neighbouring nodes.
4) *Sybil attack*: It is the form of attack where a malicious node creates multiple identities in the network, each appearing as a legitimate node It can be used against topology maintenance and routing algorithms; it reduces the effectiveness of fault tolerant schemes such as distributed storage and disparity.

B. Routing Attack

1) *Wormhole attack* **–**In this type of attack [8] an attacker receives packets at one location in the network and tunnels them selectively to another location in the network. Then, the packets are resent into the network and the tunnel established between two colluding attackers is referred to as a wormhole.
2) *Sinkhole Black hole/ attack* **-** A malicious node uses the routing protocol to advertise itself as having the shortest path to the node. In this situation, the malicious node advertises itself to a node that it wants to intercept the packet.
3) *Byzantine attack*: In Byzantine attack [7], malicious node intention is to degrade the performance by doing malicious functionalities such as packet dropping, packet modification and injecting false packets.
4) *Routing table overflow attack* **:** an attacker attempts [7] to create routes to nonexistent nodes with intention to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. This attack could also lead to DoS attack or resource exhaustion.

III. RELATED STUDY

Shin-Ming Cheng [2] proposed the Combined Distributed and Centralized scheme (CDC) to combine the distributed scheduling and centralized scheduling mechanisms so that the minislot allocation can be more flexible, and the utilization is increased. In the 802.16 mesh mode, allocation of minislots can be handled by the centralized and distributed scheduling mechanisms. For the centralized scheduling mechanism - two scheduling algorithms named Round Robin(RR) and Greedy, are proposed as the base-line algorithms.

V.S .Shankar Sriram [8] proposed architecture and analyzed the possibility of wormhole attack along with a countermeasure to avoid such an attack. The proposed work involves the shared information between communicating access points to prevent Rouge Access Points from masquerading as false neighbours. The author's defence greatly diminishes the threat of wormhole attacks and requires no location information or clock synchronization. As initial research focused that wormhole attack is possible only on adhoc networks, but now-a-days wormhole attack is possible on infrastructure based wireless LANs also.

Divya Bansal [9] proposed a new approach using threshold authorization model with Clustered Certificate Authority which caters to the best of both the centralized and distributed architecture. As various wireless networks evolve into the next generation to provide good services, a key technology, wireless mesh networks (WMNs),has emerged recently. There are number of issues in the deployment of WMNs. Security is quite a serious issue amongst them. Authenticating the users and devices is a key point of network security in the network.

Monika [6] studied to mesh routers which are stationary and implemented both Gray Hole attack and black hole attack in mesh routers and study the delivery ratio of the network with and without the presence of attack routers. DoS attacks are most common in networks which connect to internet and since WMNs are mainly designed for fast and long distance internet accesses this type of attacks are common in the network. Wireless mesh networks consist of both mesh routers and mesh clients.

Huaiyu Wen and Guangchun Luo [11] proposed a high efficiency wormhole detection algorithm based on 2-hop neighbor in WMNs, which is called Wormhole Detection based on Neighbour's Neighbour scheme (WDNN) to enhance the efficiency and facility of wormhole detection .Then a simple Random Walk Route scheme (RWR) is proposed to prevent routes from wormholes in which the route is chosen without using the low latency link which is created by wormholes.

P Subhash and S Ramchandram proposed a mechanism to prevent byzantine wormhole attack in WMNs. The proposed work relies on digital signatures and prevents formation of wormholes during route discovery process and it is designed for an on-demand hop-by-hop routing protocol like HWMP (Hybrid Wireless Mesh Protocol-the default routing protocol for WMN). This is also applicable to source routing protocols like DSR(Dynamic Source Routing). This is a software based solution and does not require additional (or) specialized hardware.

Mohammad N. Al-Mohidat and Fathi M. Salem [12], proposed an effective modification to the IEEE 802.11 MAC(Medium Access Control) layer by incorporating a multi-channel mode and shows significant improvement in many major network performance metrics compared to the literature and to the single channel mode. As the multi-hop nature of WMNs creates many new challenges, primarily in the MAC layer and specifically, the IEEE 802.11 Medium Access Control (MAC) layer is designed for a single hop wireless network.

IV CONCLUSION

Wireless LAN (WLAN) Technology is currently experiencing tremendous growth in popularity, offering secure, seamless mobile access into corporate environments, residential areas, and public spaces. Wireless technologies represent rapidly emerging area of growth and for providing ubiquitous access to the network for the campus community. Wireless is being adopted for many new applications. In this paper the various standards, protocols and mechanisms in order to provide the right Authentication and Key Management solution based on the principle of detection mechanism for a Wireless Mesh Network have been studied.

Table1: Comparison of Various Security Protocols

Protocol	Based on	Advantages	Disadvantages
FEEPVR,SEEEP	Geographical Information	Simple and efficient end-to-end protocol	Extra positioning device
Packet Leashes	GPS & Clock	Geographical or temporal information bound the distance or lifetime of an end to end transmission packet	Need GPS and Clock synchronization
Mutual Authenticated Distance-Bounding	Distance-Bounding	No need of Synchronized Clock	Has enormous computing consumption
ECHO	Ultrasound	Helps in relaxing the timing requirements	Needs extra hardware
Neighbour-Related Methods	Directional Antennas	Attacks become increasingly difficult to execute successfully	Purely centralized and is considerably susceptible to distance estimation
Key-Based Methods	Keys	Messages from authenticated neighbour are accepted and messages tunnelled from multi-hop-away locations are discarded	Needs extra hardware
WAP,TTM	Synchronized clock	No need of any extra hardware	Need synchronized clock

REFERENCES

[1] Ho Ting Cheng, Hai Jiang and Weihua Zhuang , "Distributed medium access control for wireless mesh networks" , Wirel. Commun. Mob. Comput. 2006;:845–864 Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.445

[2] Shin-Ming Cheng, Phone Lin, Di-Wei Huang and Shun-Ren Yang, "A Study on Distributed/Centralized Scheduling for Wireless Mesh Networks", IWCMC'06, July 3–6, pp 599-604, 2006, Vancouver, British Columbia, Canada

[3] Ian F. Akyildiz, Xudong Wang, Weilin Wang, Wireless mesh networks: A survey, in Computer Networks, IEEE , September 2005, 445-487

[4] Anjum Naveed, Salil S. Kanhere, Sanjay K. Jha, "Security in Wireless Mesh Networks", October 27, 2006

[5] William , Arbaugh, Narendar Shankar,Y.C. Justin Wan "Your 802.11 Wireless Network has No Clothes" University of Maryland, 2001

[6]Monika Department of computer science, "Denial of Service Attacks in Wireless Mesh Networks", International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012, pp 4516-4522

[7] Sachin Dev Kanawat, Pankaj Singh Parihar, "Attacks in Wireless Networks", International Journal of Smart Sensors and Adhoc Networks, Volume-1, Issue-1, 2011

[8] V.S.Shankar Sriram, Ashish Pratap Singh, G.Sahoo, "Methodology for Securing Wireless LANs Against Wormhole Attack", International Journal of Recent Trends in Engineering, Issue. 1, Vol. 1, May 2009

[9] Divya Bansal and Sanjeev Sofat, "Threshold based Authorization model for Authentication of a node in Wireless Mesh Networks",Int. J. of Advanced Networking and Applications Volume: 01, Issue: 06, Pages: 387-392 (2010)

[10] P Subhash and S Ramachandram, "Preventing Wormholes in Multi-hop Wireless Mesh Networks",Third International Conference on Advanced Computing & Communication Technologies,IEEE 2013

[11] Huaiyu Wen and Guangchun Luo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbour in Wireless Mesh Networks" Journal of Information & Computational Science 10:14 (2013) 4461–4476, September 20, 2013

[12] Mohammad N. Al-Mohidat and Fathi M. Salem, "IEEE 802.11 Based Wireless Mesh Networks: A Multi-Channel MAC Baseline Study":IEEE 2013

[13] Hyunok Lee and Donald C. Cox, "A Fully-Distributed Control Time Slot Assignment protocol for large Wireless Mesh Networks", 978-1-4244-2677-5/08/ 2008 IEEE