International Journal of Research in Science and Technology http://www.ijrst.com
(IJRST) 2012, Vol. No. 2, Issue No. III, Jul-Sep **ISSN: 2249-0604**

THE STUDY OF STRUCTURAL & PLANNING DESIGNAND APPEARANCE ENHANCEMENT OF ROUTINE NETWORKS

Modh Jatinkumar C.

ABSTRACT

An emerging technology is the wireless mesh network. It may bring the dream of seamlessly connected world into reality. The main purpose of a Wireless Mesh Network is to provide high speed Internet access for end users. The design of the network architecture is a fundamental issue for a WMN and is critical in determining the network performance and providing QoS for end users, and thus should be addressed carefully. In this paper, issues related to security and authentications of wireless mesh networks are analyzed.

Key words*: WMNs, QoS, end users, authentication*

INTRODUCTION

Information travels across the Internet by being bounced automatically from one router to the next until it reaches its destination. In the last few years there is a rapid development of wireless technologies and their usage. There is also fast growing demand for high bandwidth communications from the users.

Wireless mesh networks offer a low cost and flexible deployment as compared to traditional network. By replacing conventional cables it provides a cost-effective alternative of high-speed internet connectivity to mobile users. It provides services like messaging, voice, e-mail, news, weather, stocks, e-commerce, health-care, various information services etc. In a wireless mesh network, the network connection is spread out among dozens or even hundreds of wireless mesh nodes that "talk" to each other to share the network connection across a large area. It can also support applications requiring high bandwidth communications e.g. video conferencing, video broadcasting and multimedia services. Wireless mesh networks provide the solutions where current model will experience limitations. Wireless devices can communicate directly without going through a central point internet gateway. By using mesh topology, traffic can be flow using the optimal path. Wireless mesh networks can be created without the need for an Internet Gateways at all.

WIRELESS MESH NETWORK ARCHITECTURE

WMN is an upcoming technology that visualizes supplementing wired infrastructure with a wireless back bone by providing Internet connectivity to mobile clients (MCs) in residential areasand offices.

In a Wireless Mesh Network, a Mesh Client (MC) can access the Internet through a wireless backbone formed by wireless MRs (Mesh Routers). Some special Mesh Routers provide Internet accessibility, called as the Internet Gateways (IGWs). Mesh Routers are interconnected in a multi-hop fashion to constitute a wireless backbone while Internet Gateways act as the communication bridges between the wireless backbone and the Internet. To increase thenetwork capacity, both the MR and IGW have the ability to simultaneously use multiple non- overlapping channels for packet reception &transmission.

Wireless mesh network is a promising wireless technology for various applications such as community and neighborhood networks, enterprise networking, metropolitan area networks, broadband home networking, transportation systems, building automation, health and medical systems, security surveillance systems, etc. It is gaining significant attention as a possible way to provide reliable wireless broadband service access with minimal up-front investments. It also provides an alternative broadband solution for areas where it's not easy to install the Wireless LAN access points, or some scenarios where there network connection are only required for a temporary period. For example, a wireless mesh network could be quickly deployed in the disaster site and is easy to be removed after the disaster event. Wireless mesh networks also provide an efficient way for enterprises which need temporary network connection in a working area. Another benefit is within a building that doesn't have an existing data cabling for access points since the costs of installing cable are relatively high.

There are multiple paths from source to a destination by Wireless Mesh Network and its intelligent routing algorithms allow each node to take the decision about the path for the forwarding of the packets. It selects the path which enhances the performance. Wireless mesh networks are having the capability of self-configuration. So it can be deployed incrementally as needed, one node at a time. The adaptive routing scheme will automatically select an alternate route to bypass the congested paths. The routing scheme will automatically select an alternate route in case some mesh routers goes down. The connectivity and reliability for the mesh networks increases when more mesh routers (MRs) are installed.

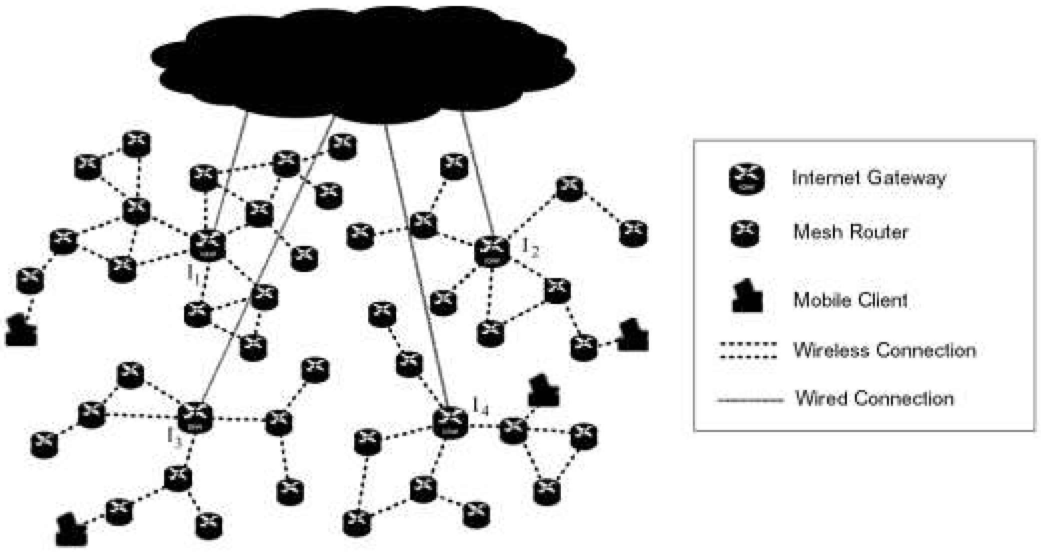

Figure 1: WMN Network Architecture

In Figure 1, the Wireless mesh network is shown. MRs (Mesh Routers) is wirelessly connected in a multi-hop fashion. Mesh Routers form a wireless backbone to enable everywhere Internet connectivity for Mesh Clients. Through the internet gateways, the wireless backbone is again tightly integrated with the Internet. Each MR (Mesh Router) may be equipped with single or multiple interfaces, which have the ability to deploy multiple non-overlapping channels (e.g., 12 for IEEE 802.11a and 3 for IEEE 802.11b/g) with which MR can simultaneously transmit and receive packets among different neighboring Mesh Routers (MRs). Each Internet Gateway (IGW) is configured with wired and wireless links and acts as the gateway between the wireless backbone and the Internet. The wired links connects to the other wired networks or Internet,while the wireless links enable the Internet Gate Way (IGW) to communicate with its neighboring Mesh Routers / MRs.

AUTHENTICATION IN WIRELESS MESH NETWORK

In a wireless network such as WMN, its security can more easily be compromised due to several reasons factors: dynamic change of network topology, distributed network architecture, the vulnerability of channels and network nodes in the shared wireless medium. Thus, a highly structured authentication mechanism is required to guarantee that only legitimate users to have access to the network service. The source of the incoming messages should be specifically identified to prevent malicious nodes gaining network access. Authentication of network devices is also important to ensure the authenticity of access points for users.

Authentication scheme is generally considered along with the key establishment. A key establishment protocol enables two entities to share a common session key which can be used for subsequent cryptographic algorithms (example symmetric key cryptosystems and message authentication codes). An authenticated key establishment scheme (AKES) in a WMN enables two entities (e.g., an MC and a MR, or two MCs) to share common session keys in an authentic way over open wireless links while providing mutual identity authentication between these two parties.

KEY ESTABLISHMENT IN WIRELESS MESH NETWORKS

Key establishment is a process by which two (or more) parties could establish a shared secret key to communicate securely. There are three different scenarios that two entities establish such a session key. One is the key transport approach, in which one party generates a session key on its own and securely transmits it to the other party. Another approach is called the key agreement, in which both parties contribute their information respectively to derive a joint secret key. The third one is key pre-distribution, in which shared keys are completely determined prior to deployment and is typically used in wireless sensor network.

A key agreement protocol is able to provide implicit key authentication if one party is assured that only the specifically identified second party could gain access to the particular secret key. A key agreement protocol that is able to provide implicit key authentication is called the authenticated key agreement protocol.

SECURITY ATTACKS (AUTHENTICATION RELATED)

If a WMN fails in protecting itself, the open wireless channel and the multi- hop nature of communication give many opportunities to malicious intruders, who can disrupt the network activities by conducting a number of security attacks.

Wireless mesh network attackers may come from three sources: External Attackers, Dishonest Customers and Dishonest operators. From these attacking sources, the attacker may gain illegal and unaccountable network access, intrude the privacy of legitimate network users, or launch denial-of-service (DoS) attacks against network resource availability. There are several types of attacks that are related to authentication.

UNAUTHORIZED ACCESS: It is the attacker access to the service provided by the wireless mesh network (i.e., the Internet Access). Further, the attacker may access to customer data and private information.

DENIAL-OF-SERVICE (DoS): A malicious attacker can conduct a DoS attack by sending a flood of packets to the MR. This results in denial of service to legitimate mesh clients.

REPLAY ATTACK: a malicious attacker caches a legitimate authentication request and replays it at a later time. Thus, if a MR fails to recognize authenticity of the request, it could be granting access to malicious attackers.

COMPRISED OR FORGED OR FAKE MR: The adversary can compromise and control a number of users and Mesh Routers subject to his choices. For example, the attackers may comprise existing MRs by physical tampering or logical break-in. The adversary may also set up rogue MRs to conduct a variety of attacks. The attacks may be implemented by attacking on wireless links (e.g., eavesdropping, jamming, replay and injection of message and traffic analysis).

Advanced attacks can also be implemented as the attacker can advertise itself as a genuine MR, using some forged messages or duplicate beacons procured by eavesdropping on a genuine MR. When a multi-hop MC hears these fraudulent beacons from a malicious MR, it assumes that it is within the radio coverage of a genuine MR and initiates a registration procedure. After registering, the MC assumes that it has obtained the Internet connection and disconnects its communication from the genuine MR. Slowly; the forged M1R could entice a number of MCs to disconnect from the genuine MRs. This attack is possible in situations where the MR is not authenticated by the MC and breaks a genuine Internet connection or causes unwarranted registration delay. The forged MR that acts as the relay can seize the data packets or capture sensitive personal (e.g., password) of MCs and other MRs.

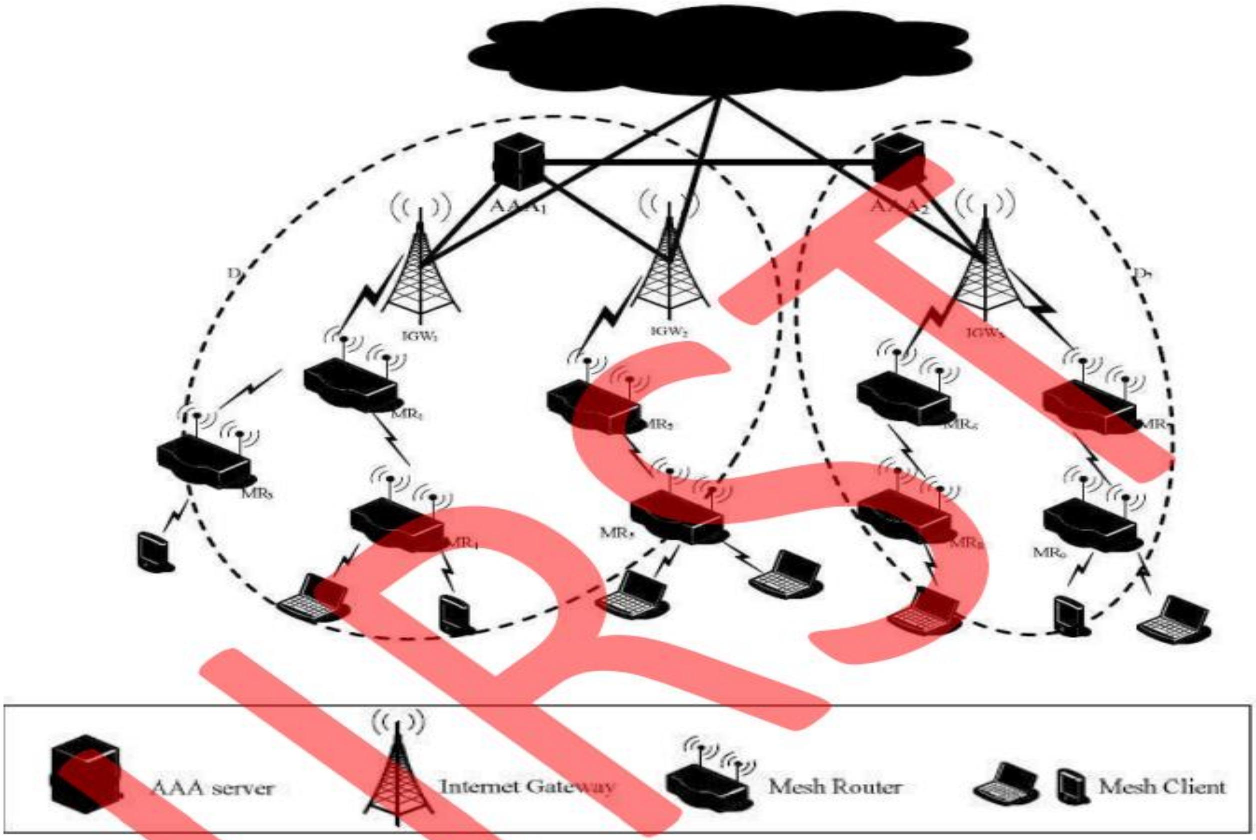

Figure 6.1: WMN Security Architecture

FEDERATED NETWORK ARCHITECTURE

In a WMN shown in Figure 6.1, every MR has the functionality of aggregating traffic from MCs. Unlike a pure ad hoc network where traffic is randomly generated between peer nodes, the traffic in WMN is IGW oriented, i.e., the traffic of a MR is predominantly directed either towards the IGW or from the IGW to the MR. In spite of different MR implementation on the radio and link layers, an IGW provides the Internet access for a couple of MRs located in its nearby area, resulting in similar network structures and common security issues for applications.

In a large network coverage area, there may exist more than one service providers (e.g., ISP) to provide coverage in different parts of the area. Each ISP could maintain and manage some IGWs along with attached MRs, which is denoted as the administrative mesh domain of an ISP (i.e., ISP domain in brief). To get the Internet access form the WMN, MCs will be initially registered into some ISP domain, which is called the home domain.

Similar to RADIUS protocol used in wireless LAN, each ISP maintains one administrative center with the function of authentication, authorization, and accounting (AAA) to manage different entities (i.e., for customers like MCs, network devices like MRs and IGWs) in its domain. We use the AAA server here to denote such a central administrative center. The AAA server assigns authorization policies for different entities, defining their role, permissions, and may be used for accounting. We denote an ISP domain as Di, which includes multiple IGWs, MRs, and registered MCs.

CONCLUSION

Wireless Mesh Network is emerging as a capable networking technology to offer users with high-bandwidth Internet accessibility with a lower cost, as compared to traditional wireless networks. To support practical use of it, robust authentication and access control schemes are required in many application scenarios to prevent security attacks and offer reliable network services for the authentic users. All the network resources such as radios and channels have to be properly protected from malicious access and attacks. In this paper, we investigate these issues in Wireless mesh networks, and illustrate the possible types of security attacks in the networks.

REFERENCES

1. *N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal, "Wireless Mesh Networks: Current Challenges and Future Directions of Web-In-The-Sky," IEEE Wireless Communications, vol. 14, pp. 79-89, 2007.*

2. *D. P. Agrawal and Q. Zeng, Introduction to Wireless and Mobile Systems. Thomson Learning, Inc., 2003.*

3. *I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," Comput. Netw. ISDN Syst., vol. 47, no. 4, pp. 445 487, 2005.*

4. *R. Draves, J. Padhye, and B. Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks," in Proceeding of ACM MobiCom, September 2004.*

5. *B. Neuman and T. Ts'o, "Kerberos: an authentication service for computer networks," Communications Magazine, IEEE, vol. 32, no. 9, pp. 33-38, Sep 1994.*

6. *L. Santhanam, B. Xie, and D. P. Agrawal, —Load balancing routing for wireless mesh networks: An adaptive partitioning approach,‖in Proceeding of 33rd IEEE Conference on LocalComputer Networks (LCN), Montreal, October 2008, pp.966 -972.*

7. *L. Chen and C. Kudla, —Identity based authenticated key agreement protocols from pairings,‖ in Proceedings of 16th IEEE Computer Security Foundation Workshop, 2003,pp.219-233.*

8. *S. Baek, S. Pack, T. Kwon, and Y. Choi, "A Localized Authentication, Authorization, and Accounting (AAA) Protocol for Mobile Hotspots," in WONS 2006: Third Annual Conference on Wireless On-demand Network Systems and Services. Les Menuires (France): INRIA, INSA Lyon, Alcatel, IFIP, 01 2006, pp. 144-153, http://citi.insa-lyon.fr/wons2006/index.htmlSession5*

9. *H. Zhu, X. Lin, S. Member, R. Lu, P. han Ho, and X. Shen, "Slab: Secure localized authentication and billing scheme for wireless mesh networks," IEEE Trans. Wireless Communication, pp. 3858-3868, 2008*