BIOINFO Security Informatics
ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 2, 2012, pp.-45-48.
Available online at http://www.bioinfo.in/contents.php?id=344

WIRELESS MESH NETWORK SECURITIES

WANKHEDE P.G.[1] AND CHAVHAN K.L.[2]

[1]Hi-Tech Institute Of Engineering And Technology, Aurangabad, M.S., India.
[2]Jawaharlal Darda Institute of Engineering and Technology, Yavatmal, M.S., India.
*Corresponding Author: Email– pranw.178@gmail.com, kiranlalitccc@gmail.com.

Received: March 15, 2012; Accepted: April 12, 2012

Abstract- Using Wireless Mesh Networks (WMNs) to offer Internet connectivity is becoming a popular choice for Wireless Internet Service Providers as it allows a fast, easy and inexpensive network deployment. However, security in WMNs is still in its infancy as very little attention has been devoted so far to this topic by the research community. In this paper, we describe the specifics of WMNs and we identify fundamental network operations that need to be secured. Wireless sensor networks are a new type of networked systems, characterized by every constrained computational and energy resources, and an ad hoc operational environment Network security to Wireless Sensor Networks is a very essential requirement because they are easily susceptible to many threats like Denial-of-Service attacks.

Citation: Wankhede P.G. and Chavhan K.L. (2012) Wireless Mesh Network Securities. BIOINFO Security Informatics, ISSN: 2249-9423 & E-ISSN: 2249-9431, Volume 2, Issue 2, pp.-45-48.

Copyright: Copyright©2012 Wankhede P.G. and Chavhan K.L. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Introduction

Wireless mesh networks (WMNs) have emerged as a promising concept to meet the challenges in next generation networks such as providing flexible, adaptive, and reconfigurable architecture while offering cost-effective solutions to the service providers. Unlike traditional Wi-Fi networks, with each access point (AP) connected to the wired network, in WMNs only a subset of the APs are required to be connected to the wired network.

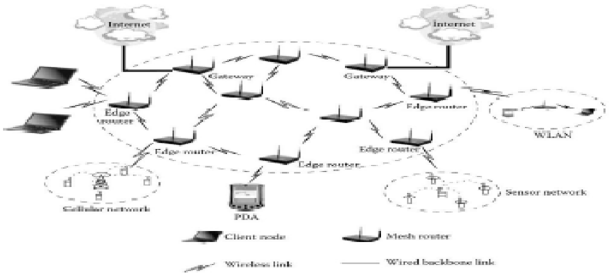

Fig. 1- The architecture of a wireless mesh network

The APs that are connected to the wired network are called the Internet gateways (IGWs), while the APs that do not have wired connections are called the mesh routers (MRs). The MRs are connected to the IGWs using multi-hop communication. The IGWs provide access to conventional clients and interconnect ad hoc, sensor,
cellular, and other networks to the Internet shown in Fig.(1).

Applications of Wireless Mesh Networks

Due to their versatility, WMNs can efficiently satisfy the needs of multiple applications. In this section, we will survey some of the most commonly encountered applications of WMNs. It is likely that other applications will emerge as the technology matures.

Broadband Internet Access

Today, most of the Internet broadband connections rely either on cable or digital subscriber lines (DSL) (satellite being a distant third). Unfortunately, a large percentage of the population (especially in rural environments, but also in large cities, even in developed countries) do not have the necessary broadband infrastructure (either TV cable or a good quality phone cable) to connect to the Internet. Furthermore, installing the required infrastructure (in particular, installing new cables) is prohibitively expensive for all but the largest Internet Service Providers (ISPs). WMNs offer considerable advantages as an Internet broadband access technology:

- **Low Upfront Investments-** Since there are no cables to install, the significant upfront investments typically associated with cable and DSL are largely bypassed. A bare-bones WMN providing minimal coverage can be used to service the first customers (an operation commonly known as "seeding"); as the number of customers increases, the network can be upgraded incrementally.
- **Customer Coverage-** Due to its multihop routing ability, line of sight to a single base station is not required; as long as a client has connectivity to any other client, it can obtain Internet access. It was shown that, especially for scenarios with significant obstructions (trees or high-rise buildings), a WMN can significantly improve the coverage in comparison with a point-to-multipoint (e.g., IEEE 802.16) solution.

Indoor WLAN Coverage- The popularity of IEEE 802.11 compatible WLANs exposed one of the most unpleasant aspects of the technology: in order to provide coverage of any but the smallest buildings, multiple access points (APs) are required. All of these access points have to be connected to a distribution system (a wired network), commonly an Ethernet network. Several companies leveraged the multihop capabilities of WMNs to eliminate the need for cables. In such a deployment, at least one of the WMN routers is connected to the external network and, hence, becomes a gateway. All of the other WMN routers double as APs and forward the data from the wireless clients to the gateway. Another form of WMN is formed by using the bridging features of some models of access points that can forward each others packets.

Characteristics of WMNs- Wireless Mesh Networks are mainly studied in the context of two distinct scenarios, namely single operator scenarios in which a single operator provides and maintains the infrastructure of the WMN and multi-operator scenarios in which multiple operators provide and maintain the infrastructure. Multi-operator scenarios can further be characterized by scenarios that only support roaming of MCs between the WMNs operated by different providers and scenarios that additionally support infrastructure sharing.

Single-Operator WMNs- In single-operator WMNs all infrastructure nodes are controlled by a single operator. Typical applications include intelligent transportation systems, public safety support, Internet access, smart metering, and building automation. The operator is responsible for the deployment of MRs, MAPs, and MGs, but not necessarily the MC's hardware. MR, MAP and MG hardware provided by the operator is typically homogeneous. The operator is able to influence the topology of the network except for the MCs.

Multi-Operator WMNs- In multi-operator WMNs, several operators provide and maintain infrastructure components, i.e., MAPs, MRs, and/or MGs. In the simplest case, each operator maintains a separate network but the clients registered with any of the operators may roam to WMNs provided and maintained by other operators. Possible applications of WMNs inter-operating like this include the previously introduced single-operator applications, e.g., Internet access or building automation. Here, access control needs to ensure that MCs of interworking operators are able to access a network without being registered to the operator of the network they currently want to access.

Communication Patterns- WMN have to support different communication patterns between the nodes in the network. These patterns are:

- Mesh Client - Mesh Client
- Mesh Client - Mesh Router
- Mesh Client - Mesh Gateway
- Mesh Router - Mesh Gateway
- Mesh Router - Mesh Router

MC-MC communication refers to communication between two clients (located in the same WMN). MC-MR communication refers to the communication between client and the associated mesh access point. MC-MG communication refers to traffic destined to leave the WMN through the gateway, e.g., to a destination on the Internet. This may also include management traffic, e.g., when communicating with a AAA Server located outside of the WMN. MR-MR communication refers to all traffic between MRs. MR-MG communication can be considered as special cases of MR-MR. It may include management traffic, but also forwarded user traffic.

Security Challenges in WMNs- Physical layer: The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. As with any radio-based medium, the possibility of jamming attacks in this layer of WMNs is always there. Jamming is a type of attack which interferes with the radio frequencies that the nodes use in a WMN for communication. A jamming source may be powerful enough to disrupt communication in the entire network. Even with less powerful jamming sources, an adversary can potentially disrupt communication in the entire network by strategically distributing the jamming sources. An intermittent jamming source may also prove detrimental as some communications in WMNs may be time-sensitive.

More complex forms of radio jamming attacks where the attacking devices do not obey the MAC layer protocols.

MAC layer

Different types of attacks are possible in the MAC layer of a WMN. Some of the major attacks at this layer are: passive eavesdropping, jamming, MAC address spoofing, replay, unfairness in allocation, pre-computation and partial matching etc. Some of these attacks are briefly described.

Passive eavesdropping- The broadcast nature of transmission of the wireless networks makes these networks prone to passive eavesdropping by the external attackers within the transmission range of the communicating nodes. Multi-hop wireless networks like WMNs are also prone to internal eavesdropping by the intermediate hops, whereby a malicious intermediate node may keep the copy of all the data that it forwards without the knowledge of any other nodes in the network. Although passive eavesdropping does not affect the network functionality directly, it leads to the compromise in data confidentiality and data integrity. Data encryption is generally employed using strong. encryption keys to protect the confidentiality and integrity of data.

Intentional collision of frames- a collision occurs when two nodes attempt to transmit on the same frequency simultaneously. When frames collide, they are discarded and need to be retransmitted. An adversary may strategically cause collisions in specific packets such as acknowledgment (ACK) control messages. A possible result of such collision is the costly exponential back-off. The adversary may simply violate the communication protocol and continuously transmit messages in an attempt to generate collisions. Repeated collisions can also be used by an attacker to cause resource exhaustion.

Network Layer

The main function of the networking layer is to transfer the packets from the source to the destination over multiple hops. In this respect, WMNs are radically different from 3G systems, WLANs and WMANs. All these technologies use a single wireless link, and hence have no need for a network layer. In contrast, for WMNs and MANETs the source and the destination can be several wireless hops away from each other, and hence the packets have to be routed and forwarded in the wireless network itself.

Routing- The routing protocol is an important factor in any network, but in WMNs it can mean the difference between failure and success. Several of the advantages of WMNs over competing technologies are enabled by the routing protocol alone:

- **Scalability/Efficiency-** If the routing protocol has a high overhead and requires global information, it will be impossible to scale it to a large number of nodes.
- **Reliability-** The routing protocol should be able to reroute fast around failed nodes, broken links, and upon the failure of a gateway it should be able to redistribute the orphaned clients among neighboring gateways. For this property, fast reconfiguration and support of multiple gateways is essential.
- **Mobile User Connectivity-** To ensure seamless mobile user connectivity, the routing protocol should enable fast hand-offs.

Special cases of WMNs

In order to make our presentation as easy as possible to follow, we have focused so far on the “classic” definition of WMNs. However, WMNs are in reality a much broader concept. In this section, we present two special cases of WMNs and we briefly describe the security challenges they introduce.

Vehicular Networks

So far, we have assumed the TAPs to be static. Vehicular networks represent a special case of WMNs that consists of a set of mobile TAPs (represented by the cars) and of roadside WHSs. The spectrum of applications offered by a vehicular network is wide ranging: It goes from safety related applications such as reporting important events (e.g., an accident, or traffic optimization through cooperative driving (e.g., deviate the traffic to avoid a traffic jam) to payment services (e.g., electronic toll collection) and location-based services (e.g., targeted marketing).

Multi-operator WMNs

So far, we have assumed the WMN to be managed by a single operator, but a mesh network can also designate a set of wireless devices belonging to different networks and controlled by different operators. These devices can be as various as access points, base stations, laptops, vehicular nodes or mobile phones.

Recent Security Proposals

In this section we evaluate recent security proposals for WMNs with respect to the characteristics and scenarios they support and with respect to the security requirements.

Mesh Networking- When discussing proposed security architectures for WMNs, it is of course important to consider upcoming standards as the IEEE 802.11s. If this standard is successfully passed, network equipment vendors will implement it and roll out their hardware with wireless mesh networking support. The standard is still in draft status. It currently supports access control for all types of nodes (MCs, MR/MAPs, MGs) based on two protocols: the Simultaneous Authentication of Equals (SAE) protocol and the Abbreviated Handshake protocol. The Abbreviated Handshake is used for authentication and key agreement between peers that already share a PMK, i.e., a pair of peers that have already successfully run SAE before. The Abbreviated Handshake protocol requires fewer messages to be exchanged between the nodes than the SAE protocol, which explains its name. The keying material generated during the Abbreviated Handshake protocol is subsequently used to encrypt and integrity and replay protect the communication between the nodes.

ARSA- Zhang et al. proposed an Attack Resilient Security Architecture for Multi-hop Wireless Networks (ARSA) that aims at providing secure roaming in multi-domain WMNs based on so-called passes that are linked to trusted brokers. They employ Identity Based Cryptography (IBC) in order to circumvent broadcasting lengthy X.509 certificates. IBC also enables self-authenticating public keys since they can be reproduced by anyone knowing the identity, e.g., based on the Network Access Identifier, of the entity and the domain parameters. Brokers issue signed passes to MCs. If a MC accesses a WMN, the operator will have to have an agreement with the broker in order to support the MC, i.e., for billing. Once the MC provides the pass issued by his broker, the included public key is used to encrypt a temporary network access pass issued by the respective operator. The client checks network legitimacy by verifying the signature on the operator’s domain parameters. Domain parameters are much like certificates in context of IBC, since they provide means to gather the cryptographic parameters necessary to perform validity checks. MC to MC authentication is based on temporary passes issued by the operator.

Conclusion

Wireless mesh networks leaped from the drawing boards into reality. Numerous start-up companies are pursuing the technology and use it to satisfy the needs of numerous application, providing broadband Internet access, WLAN coverage and connectivity. The technology has the potential to successfully compete with several traditional technologies (3G systems, WLANs and WMANs).

References

[1] *http://www.meshnetworks.com*.

[2] Raya M. and Hubaux J.P. (2005) *SASN*.

[3] Ben Salem N. and Hubaux J.P. (2006) *IEEE*.

[4] A.M. et al., *DIREN'02*.

[5] Skinnemoen H., Hansen S.K., Jahn A. and Berioli M., *AI-AAICSSC'07*.

[6] Portmann M. and Pirzada A.A., *IEEE Internet Computing*.

[7] Cheikhrouhou O., Laurent-Maknavicius M. and Chaouchi H., *SAR'06*.

[8] Martignon F., Paris S. and Capone A. (2008) *Q2SWinet*.

[9] Zhang Y., *Communications'06*.

[10] Tchepnda C. and Riguidel M. (2006) *20th Int. Conference on Advanced Information Networking and Applications*, 2, 33-38.

[11] Akyildiz I.F., Wang X. and Wang W. (2005) *Computer Networks and ISDN Systems*, 47(4).

[12] Salem N.B. and Hubaux J.P. (2005) *WiMesh*.

[13] William Stallings (2006) *Network Security Essentials(*3rd *edition).*