An Overview of Wireless Network Concepts

Biju Issac
Swinburne University of Technology, Sarawak Campus, Malaysia

Wireless networks and the subsequent mobile communication are growing by leaps and bounds in the past years and the demand for connection without cables is certainly high. Nowadays, wireless networks are quite common and can be found on university campuses, corporate offices and in public places like hotels, airports, coffee shops and so forth. Not only are mobile devices getting smaller and cheaper, they are also becoming more efficient and powerful, capable of running applications and network services. This is causing the uncontrollable growth of mobile computing as we are witnessing today. Among the many number of applications and services that are executed by mobile devices, network and data services are in high demand. Brief descriptions of some selective wireless technologies that help mobile computing, like IEEE 802.11 networks (with infrastructure mode and ad-hoc mode), Bluetooth, HomeRF, WiMAX and cellular technologies are given below.

IEEE 802.11 INFRASTRUCTURE NETWORK

Wireless local area network (WLAN) which is also known as Wi-Fi (Wireless Fidelity) networks, requires an infrastructure network that could provide the services of accessing other networks, along with forwarding functions and medium access control. The Institute of Electrical and Electronics Engineers (IEEE) in 1997 initiated the first WLAN standard and they called it 802.11. But, 802.11 only supported a maximum bandwidth of 2 Mbps, which is quite slow for most applications. The IEEE 802.11 family consists of different standards. The initial standard was approved in 1997 and it backed wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications that supported 1 Mbps and 2 Mbps data rate over the 2.4 GHz ISM band.

In a wireless infrastructure setup, there are two basic components, access points and wireless stations. An access point or base station functions as a bridge by connecting to a wired LAN (Local Area Network) through Ethernet cables. It receives data, buffers and transmits data between the wireless and the wired network infrastructure. A single access point supports on average 20 users and has a coverage varying from 20 meters in areas with obstacles like walls, stairways, elevators, and so forth, and up to 100 meters in areas where there is clear line of sight. The design of infrastructure-based wireless network is rather simpler as most of the network functionality lies within the access point. Transmission and reception of wireless communication can happen in different channels.

A building may require several access points to provide complete coverage and allow users to roam seamlessly between access points. A wireless network adapter connects users via an access point to the rest of the LAN. A wireless station can be using a PC card in a laptop, an ISA or PCI adapter in a desktop computer, or can be fully integrated within a handheld device. Security of a WLAN is of great concern with WEP (Wired Equivalent Privacy) encryption as static WEP keys could be easily recovered because of a design flaw (Stubblefield, Ionnidis, & Rubin, 2002). RADIUS Server authentication which uses EAP protocol (Extensible Authentication Protocol) with TKIP (Temporal Key Integrity Protocol) encryption is proposed as interim solution in WPA (Wi-Fi protected Access) standard, with AES encryption option being looked into as long term solution (Gast, 2002). Figure 1 shows a simple wireless network that uses RADIUS server authentication.

There are different wireless LAN technologies that the IEEE 802.11 standard supports in the unlicensed bands of 2.4 and 5 GHz. They share the same MAC (Medium Access Control) over two PHY layer specifications: Direct-Sequence

Figure 1. The wireless network in an organization showing mobile laptops

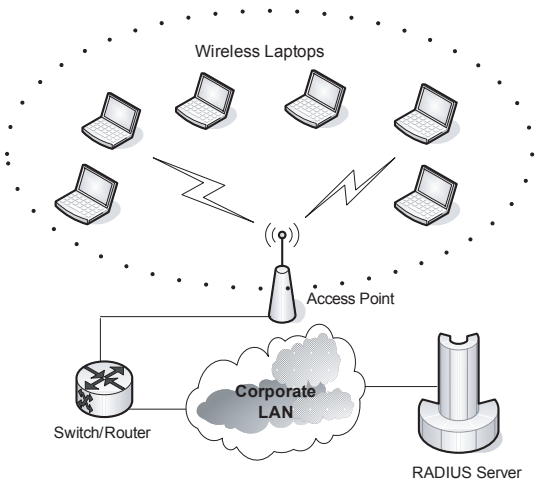

Table 1. Popular IEEE 802.11 comparisons

IEEE Standard	Maximum Speed	Frequency band	No. of nonoverlapping channels	Notes
802.11 (legacy)	1 Mbps to 2 Mbps	2.4 GHz	n/a	First standard (ratified in 1997). Uses FHSS and DSSS.
802.11a	54 Mbps	5 GHz	8 to 14 (or more in future)	Second standard (ratified in 1999). Uses OFDM.
802.11b	11 Mbps	2.4 GHz	3 (Channel 1,6 and 11)	Third and the most common standard (ratified in 1999). Uses DSSS.
802.11g	54 Mbps	2.4 GHz	3 (Channel 1,6 and 11)	Popular standard (ratified in 2003). Uses OFDM.

Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS) technologies. Infrared technology though supported, is not accepted by any manufacturer. Data rates of up to 2 Mbps were achieved initially by IEEE 802.11 systems operating at the 2.4 GHz band. Their wide acceptance initiated new versions and enhancements of the specification. The different extensions to the 802.11 standard use the radio frequency band differently. Popular 802.11 standards like 802.11a, 802.11b and 802.11g are listed in table 1.

As a strong and robust standard, 802.11i deals with the limitations of WEP encryption that was used with 802.11b and enhances the overall wireless security. The architecture uses 802.1x for authentication (with the use of EAP and an authentication server that uses 4-way handshake), includes improvements in key management and the Advanced Encryption Standard (AES) for encryption. Other 802.11 extensions include 802.11c that focuses on MAC bridges, 802.11d that focuses on worldwide use of WLAN with operation at different power levels, 802.11e that focuses on Quality of Service, 802.11f that focuses on access point interoperability and 802.11h that focuses on addressing interference problems when used with other communication equipments. Table 1 shows the comparison of the popular 802.11 standards (Held, 2003; Issac, Hamid, & Tan, 2006).

IEEE 802.11 AD HOC NETWORK

A wireless ad-hoc network is a network that uses wireless links where each node is willing to forward data to the other neighbouring nodes dynamically, based on the network connectivity. Types of wireless ad-hoc networks include Mobile ad-hoc networks (MANET), Wireless Sensor Networks (WSN) and Wireless Mesh Networks (WMN). A mobile ad-hoc network can be defined as a network of computer nodes that happens to be in proximity with each other, having no fixed infrastructure. A wireless sensor network (WSN) is a wireless network that makes use of distributed autonomous devices that uses sensors to measure or monitor environmental conditions like temperature, motion, sound, vibration, pressure and so forth, in a cooperative fashion. Wireless mesh networking (WMN) is mesh networking that is implemented on top of a wireless LAN in a decentralized (with no central server) way or centralized way (with a central server). Mesh networks are also extremely reliable with its redundant links, as each node is connected to several other nodes. If one node shuts down due to hardware errors or due to some other reason, its neighbours can easily find another route. Mesh networks can involve either fixed or mobile nodes.

Generally, in any ad-hoc network, each node can directly communicate with other nodes and so no access point or controlling station is needed. It is a self configuring network of routers along with associated hosts connected by wireless links. This union of network nodes or devices forms an arbitrary topology. This type of network provides great flexibility as it can be used for unplanned meetings, fast replacements of communication scenes far away from any infrastructure. Nodes or devices may look or rather search for target nodes that are out of vicinity by flooding the network with broadcasts packets that would be forwarded by each node. Wireless connections are even possible through multiple nodes forming a multihop ad-hoc network. Routing protocols then provide reliable connections even if nodes are moving around.

The routers are free to move randomly and organize themselves arbitrarily, making unpredictable changes in network's wireless topology. There is no need for access point and if one station working in ad-hoc mode is connected to wired network, stations forming ad-hoc network have a wireless access to Internet. IEEE 802.11 technology can be used to implement single-hop ad-hoc networks where the stations need to be in the same transmission radius to be able to communicate. But in multihop ad-hoc networking,