

Wireless Networks for Mobile Devices

Rahul Agarwal

Wireless networks are overtaking wired access at the network edge. This is largely due to availability of highly mobile devices at low cost. Wireless networks offer flexibility, rapid installation, scalability and ease of movement of devices, and are becoming increasingly popular among all kinds of users. As their popularity increases security has become a major concern. All risks presented by wired networks are still there, in addition since communication is over thin air threats are magnified many fold as any receiver can tap into the communication. New sets of protocols and attack techniques need to be studied.

There are many wireless network standards for data communication available for mobile devices. Many devices support multiple standards and ways to communicate. I have classified the networks based on the size of area of availability of the network.

1. Wireless Personal Area Networks (WPANs)

Wireless personal area networks are generally seen as a cable replacement technology. These networks operate on an unlicensed frequency (generally 2.4GHz) and cover a range of about 10 meters (30 feet), providing bandwidth up to 4 Mbps (20 Mbps for certain new versions!). Some points to note about WPANs:

- Extremely short range: Typically up to 10 meters, it may be lowered if you choose to use lesser power on your devices
- Relatively low cost: Lower cost as an infrastructure setup is not required and ad hoc networks are setup
- Low power consumption by devices as the signals are for short distances: The signal strength to use is generally configurable on the device
- Personal space communication: Connecting your personal devices such a PC, PDA, Mobile phone and entertainment devices.
- Security and Privacy implications: Since your personal devices interact in this space you information may be at risk. For example are using a Bluetooth headset with your phone in your office, someone a few cubicles down may be able to listen in to your communication without requiring any special equipment if the communication is not secure!
- Interoperability of devices by different vendors may be an issue: Many vendors use propriety protocols and do not allow interoperability

1.1 Bluetooth and IEEE 802.15

Bluetooth¹ and IEEE 802.15² standard aim to provide a standard to short communication and both operate on the unlicensed 2.4GHz frequency providing bandwidth of up to 20

¹ <http://www.bluetooth.com/>

² <http://grouper.ieee.org/groups/802/15/>

Mbps in a range of 10 meters. 802.15 protocols specifically aim to interoperate with other 802.11 networks using the standard MAC protocols.

Devices can operate in discoverable, limited discoverable and non-discoverable modes. These basically determine if other devices in proximity can be detected or not. Bluejacking³ is an instance of use/abuse of such features. Connected devices form what is known as a piconet and there can be a master-slave relation among communicating devices. These technologies support both voice and data communication and are slowly being adopted widely. Security is a major concern as highlighted before.

1.2 Infrared (IrDA)

Promoted by the Infrared Data Association (IrDA)⁴, the protocols are suited well for certain applications and being an old standard many devices have infrared support. Some special points about infrared data communication

- Typically only up to 1 meter (3 feet)
- Line of sight required
- Point-to-Point communication only

It is typically used to 'beam' information as the line of sight restriction makes other practical uses of this technology hard. It is used widely on almost every remote control and is very cost effective.

2. Wireless Local Area Networks (WLANs)

Local Area Networks are cost effective and widely deployed. There many wired technologies [Kurose 3E] and LANs are almost essential now in any computing environment. Wireless LANs go a step further and save costs as cables are not needed. It also makes it easy to move networked devices and still be connected to the network; however there are additional security and privacy concerns that will be looked into detail later.

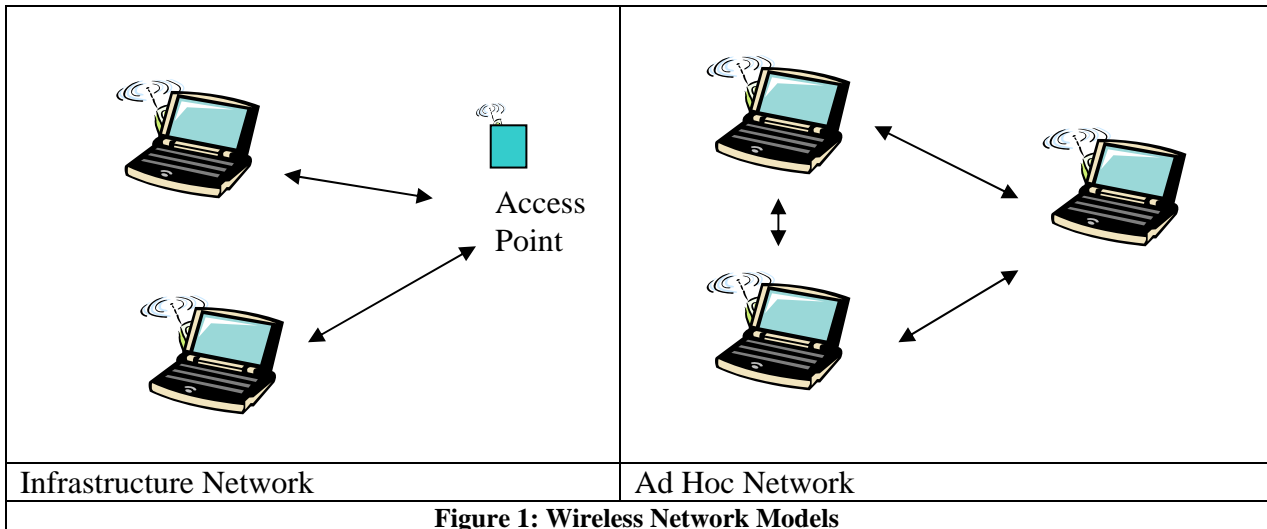
WLANs can be setup as one of the following network models:

An **infrastructure network** consists of a central access point or base station and a number of communicating devices. The access point is generally connected to a wired network and these networks typically run using the 802.11x protocols.

An **Ad Hoc network** dynamically connects wireless devices in the vicinity without any central coordination. Typically 801.11x and 802.15 (Bluetooth) are deployed. These two modes present unique challenges and issues with both are studied.

³ <http://news.bbc.co.uk/1/hi/technology/3237755.stm>

⁴ <http://www.irda.org>



2.1 IEEE 802.11x

The IEEE 802.11x family of protocols uses Carrier Sense Multiple Access (CSMA), Medium Access Control (MAC) with Collision Avoidance (CA). Wireless networks are different from wired networks primarily at the Physical Layer however this requires significantly different protocols at the Link Layer due to signal attenuation, fading, hidden-terminal problem, multi-path propagation and easy interference from other signals at the physical level. These networks can typically be configured as an infrastructure based network or an ad hoc network.

802.11 networks have a range of 50 meters (802.11a) to 100 meters (802.11b,g) and bandwidth of 11 Mbps (802.11b) to 54 Mbps (802.11a,g). They operate on the unlicensed 2.4 GHz (802.11b,g) and 5GHz (802.11a) frequencies.

Other protocols in the family focus on many desirable features. 802.11e aims providing Quality of Service (QoS), 802.11f aims at vendor interoperability, 802.11h aims for higher speed physical layer and 802.11i aims at enhancing MAC layer security.

More details suggested at Wikipedia⁵.

3. Wireless Wide Area Networks (WWANs)

Wide area networks and Satellite networks provide coverage in very large areas and global coverage in the case of satellite networks. However these networks require significant capital investment and maintenance. Cellular phone networks for example require communication towers for each cell and an underlying backbone of wired communications network. Further these operate on licensed frequencies that are usually auctioned at high prices. Most new networks are digital and packet switched providing 'always on' network availability to mobile devices. Cellular networks have to deal with

⁵ http://en.wikipedia.org/wiki/Wireless_LAN

additional complexities of roaming users and handoff (continuing uninterrupted user communication as user moves from one cell to another).

Technology availability and bandwidth restrictions are important to note when developing for mobile devices.

Some important technologies are listed.

3.1 GSM

The Global System for Mobile Communications (GSM⁶) is the most popular 2G network and used widely across the world. Different GSM networks operate over 900 MHz, 1800 MHz and 1900 MHz in different geographies and there are tri-band phones available that are compatible across this spectrum. GSM is circuit switched and provides data transfer up to 9.6 Kbps.

3.2 CDMA

CDMA is another 2G technology and was introduced by Qualcomm. Like GSM it is circuit switched and operates in 800 MHz and 1900 MHz. It provides data transfer up to 14.4 Kbps.

3.3 GPRS

General Packet Radio System (GPRS) is a patch for current GSM networks enabling them to provide digital packet switched data services (typically 56 Kbps) and creating what is called a 2.5G network. Such data rates may be compared to a dial-up internet connection, paving way for the faster 3G networks. It provides a cost-effective way for telecom companies to be able to provide data services.

3.4 Future 3G Networks

Enhanced Data Rates for Global Evolution (EDGE) and Wideband CDMA (WCDMA) are new technologies pushing for 3G networks. EDGE operates over 200 kHz narrowband and therefore does not require a 3G license making it a cheaper alternative. However peak data rates are 384 Kbps (actually around 150 Kbps only). WCDMA offers varying data rates depending on mobility, 144 Kbps (highly mobile), 384 Kbps (mobile), and 2 Mbps (almost stationary).

⁶ <http://www.gsmworld.com>