Benefit and security issues in wireless technologies: Wi-fi and WiMax

Gurveen K.Sandhu , Gurpreet Singh Mann, Rajdeep Kaur

(*Assistant Professor, Dept. of Information Technology, Baba Farid college of Engineering and Technology, Bathinda,India)*

(*Assistant Professor, Dept. of Information Technology, Baba Farid college of Engineering and Technology, Bathinda, India)*

(Lecture, Dept. of Information Technology, Baba Farid college of Engineering and Technology, Bathinda,India)

Abstract— Option way out to the trouble of accessing information in remote areas where wired network are inaccessible is offered by Wireless Networking Technology. Wireless Networking has changed the way people communicate and share information by eliminating the boundaries of distance and location. Although Wireless Networking is regarded as Networking Future but still there are some unsolved issues which is preventing the wide adaption of Wireless Technologies.In this paper we have tried to discusses two latest wireless technologies: Wi-Fi and WiMAX. The objective in this paper is to briefly describe the technologies as well as the benefits and risks involved in their implementation.

Index Terms — *Wi-Fi, WiMax, Wireless Security, Wireless Benefits*

Wireless Technology

The use of wireless technology is quickly becoming the most popular way to connect to a network. Wi-Fi is one of the many available technologies that offer us the convenience of mobile computing. The thought of working anywhere and sending data to and from a device without physical connection is becoming increasingly attractive for many consumers and businesses (Stephen Haag 2007). In this paper we will define what Wi-Fi technology is, briefly how it works and its advantages and disadvantages.

In 1999 a new technology called Airport was introduced by Apple Computers. The technology enabled a mobile user to establish and maintain a connection to a network without being physically linked to it by some sort of cable. This technology was then adopted and developed by the rest of the IT industry, then changed to the name we are all familiar today, Wi-Fi stands for wireless fidelity' (Dynamic Web Solutions 2007).

The name of a popular wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections. The Wi-Fi Alliance, the organization that owns the Wi-Fi (registered trademark) term specifically defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards." Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation.

How Wi-Fi Works

If you've been in an airport, coffee shop, library or hotel recently, chances are you've been right in the middle of a wireless network. Many people also use wireless networking, also called WiFi or 802.11 networking, to connect their computers at home, and some cities are trying to use the technology to provide free or low-cost Internet access to residents. In the near future, wireless networking may become so widespread that you can access the Internet just about

anywhere at any time, without using wires.

Fig. 1.One wireless router can allow multiple devices to connect to the Internet.

Benefits of using WiFi

WiFi has a lot of advantages. Wireless networks are easy to set up and inexpensive. They're also unobtrusive -- unless you're on the lookout for a place to use your laptop, you may not even notice when you're in a hotspot.

A wireless network uses radio waves, just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens:

1. A computer's wireless adapter translates data into a radio signal and transmits it using an antenna.
2. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.

The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.
The radios used for WiFi communication are very similar to the radios used for walkie-talkies, cell phones and other devices. They can transmit and receive radio waves, and they can convert 1s and 0s into radio waves and convert the radio waves back into 1s and 0s. But WiFi radios have a few notable differences from other radios:

They transmit at frequencies of 2.4 GHz or 5 GHz. This frequency is considerably higher than the frequencies used for cell phones, walkie-talkies and televisions. The higher frequency allows the signal to carry more data.

They use 802.11 networking standards, which come in several flavors:

- **802.11a** transmits at 5 GHz and can move up to 54 megabits of data per second. It also uses **orthogonal frequency-division multiplexing** (OFDM), a more efficient coding technique that splits that radio signal into several sub-signals before they reach a receiver. This greatly reduces interference.
- **802.11b** is the slowest and least expensive standard. For a while, its cost made it popular, but now it's becoming less common as faster standards become less expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum. It can handle up to 11 megabits of data per second, and it uses **complementary code keying** (CCK) modulation to improve speeds.
- **802.11g** transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.
- **802.11n** is the newest standard that is widely available. This standard significantly improves speed and range. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. The standard is currently in draft form -- the **Institute of Electrical and Electronics Engineers (IEEE)** plans to formally ratify 802.11n by the end of 2009.

Security issues in WiFi

Wireless networks are inherently less secure than wired networks.

- The signal is broadcast, the network is shared and any network device can listen to network traffic for any other network device in range. This means that maintaining network security is potentially difficult.
- The signal spreads outside buildings so physical security is ineffective and it could be very difficult to locate unauthorized devices.
- The current wireless networking standards have very poor encryption facilities which cannot be regarded as secure.
- Efficient operation of wireless networks depends on coordinated management of the available spectrum. Unauthorized wireless equipment may interfere with and degrade the performance of authorized services.

WiMAX

WiMAX is a wireless digital communications system, also known as IEEE 802.16, that is intended for wireless "metropolitan area networks". WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the WiFi/802.11 wireless local area network standard is limited in most cases to only 100 - 300 feet (30 - 100m). With WiMAX, WiFi-like data rates are easily supported, but the issue of interference is lessened. WiMAX operates on both licensed and non-licensed frequencies, providing a regulated environment and viable economic model for wireless carriers. WiMAX can be used for wireless networking in much the same way as the more common WiFi protocol. WiMAX is a second-generation protocol that allows for more efficient bandwidth use, interference avoidance, and is intended to allow higher data rates over longer distances.

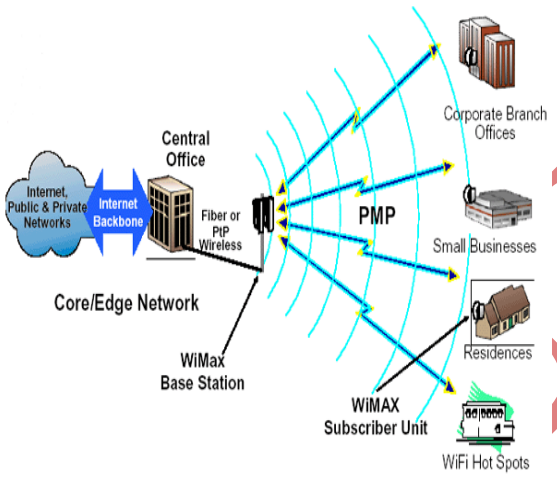
The IEEE 802.16 standard defines the technical features of the communications protocol. The WiMAX Forum offers a

means of testing manufacturer's equipment for compatibility, as well as an industry group dedicated to fostering the development and commercialization of the technology. WiMax.com provides a focal point for consumers, service providers, manufacturers, analysts, and researchers who are interested in WiMAX technology, services, and products. Soon, WiMAX will be a very well recognized term to describe wireless Internet access throughout the world.

Benefits of WiMAX

The bandwidth and range of WiMAX make it suitable for the following potential applications:

- Connecting Wi-Fi hotspots to the Internet.
- Providing a wireless alternative to cable and DSL for "last mile" broadband access.
- Providing data and telecommunications services.
- Providing a source of Internet connectivity as part of a business continuity plan. That is, if a business has a fixed and a wireless Internet connection, especially from unrelated providers, they are unlikely to be affected by the same service outage.
- Providing portable connectivity.



The risks of using WiMAX

Some of the attacks conducted at the various layers of WiMax are -

Physical Layer Threats

1. Jamming

Jamming is the process of introducing a strong source of noise powerful enough to significantly reduce the signal to noise ratio.

2.Scrambling

Scrambling is another form of jamming, but for short intervals and is used to disorder targeted frames (mostlymanagement messages).

Mac Layer Threats

1. Eavesdropping

During basic and primary connection, MAC management messages are sent in plaintext and are not properly authenticated which can be used by an attacker to launch an attack.

2. Masquerading threat

Identity theft occurs in which a fake device can use the hardware address of another registered device by intercepting the management messages and launch an attack.

3. Denial of Service (DoS)

An attacker can force a BS to digest a large amount of handoffs and then launch a denial of service attack.In an 802.16 mesh network deployment routers orgateways that reside between base station and client are susceptible to attacks in the application layer.

Network Layer Threats

1. Blackhole Attack

An attacker creates fake packets to target a valid node. A low cost route is advertized by the attacker. Subsequently the packets forwarded to it are dropped.

2. Greyhole Attack

Grey Hole is a node that can alter from behaving correctly to behaving like a black hole where packets are dropped. This is done to avoid detection.

3. Wormhole Attack

In a wormhole attack, an attacker creates a high quality outof-band link and forwards packets and replays those packets at another location in the network through that out-of-band link. This is demonstrated in Fig. 8.The attacks may be present as there is a "adhoc feature" in the current WiMax technology (eventhough this is not the case during its initial plan - a direct transmission from sender to base station).

Application Layer Threats

When routers or gateways act as intermediaries between client and base station, there is an increased potential of security vulnerabilities, as the intermediary routers that reside between base station and client are presentable and susceptible to attacks.

WiFi vs. WiMax

Comparing WiMax to WiFi is akin to comparing apples to oranges. Initially it's easy to see why the comparison would exist, as most people think WiMax is merely a more robust version of WiFi. Indeed they are both wireless broadband technologies, but they differ in the technical execution and ultimately their business case is very different. In addition to the technical differences that exist, the marketplace difference is that equipment is more or less non-existent for WiMax and certainly not geared towards a residential environment with very high pricing to be expected. It will take at least 2 years to see equipment of mass market uptake pricing.

WiMax will not be commercially available until the second half of 2005, and even then at a very controlled level. This is primarily due to standardization issues. In fact, it won't be until 2006 that a robust production and implementation will happen due to the ramp-up period for manufacturers. This is certainly one challenge to the widespread adoption of WiMax. Additionally, WiMax will have issues of pricing, and will remain far more expensive than WiFi. WiMax will be primarily adopted by businesses to replace or displace DSL, and offices that want to cover a lot of territory without entering the world of endless repeaters that are necessary with the 802.11 technologies. It will take some time (2 years) for WiMax to significantly reduce its price-point for residential uptake. WiMax will not displace WiFi in the home because WiFi is advancing in terms of speed and technology. Each year brings a new variant to the 802.11 area with various improvements.

Additionally, for commercial deployment, frequency allocation will be an issue. With the three dominant communications players controlling the best frequencies, it will be hard to get the type of traction needed with the remaining companies operating in the frequencies available. WiMax will become extremely robust and displace WiFi as the deployment of choice for commercial deployments, but that won't even begin until the end of 2006. Based upon the number of public hotspots already deployed, WiMax will not be chosen to replace those as they are up and running adequately and personnel involved understand how to work with the technology. The business case does not exist at the hotspot level. Where it may exist is for wider free use deployments such as city deployments (free ones) and other government sponsored or carrier sponsored (with ultra inexpensive pricing for consumers) deployments. If this happens then its not only WiFi that will be displaced, but cable and DSL will also lose a percentage of their subscriber base. What will cause the displacement is the consumer's proven desire for a bundled package.

Wireless Networking Equipment

Antennas

There are 2 types of antennas. . . omni-directional and directional. Omni-directional antennas have 360° coverage [or almost]. Directional antennas only go one direction, and have varying beam widths and areas they cover. Why would you use a directional antenna over an omni? Paths of signals only covering a smaller beam width are less susceptible to noise, and tend to go really far. Also, directional antennas are usually cheaper. Basically, if your signal needs to go to more than one place, you should have an omni directional antenna. If you're going the directional route, buy or build a yagi. [Rediculously directional]

The next factor in choosing an antenna, is how much gain do you need? Gain is measured in Decibles [dB]. Your signal doubles in strength every 3 dB, so if you're putting out 32mW and you have a 6 dB gain antenna, you will be outputting 128mW. Likewise, if you have a cable that attenuates 3 dB after an initial output of 32mW, you will be outputting 16mW at the end of the cable. So how much gain do you really need? There are many things that affect a signal, so it's hard to say. Your best bet is to get the highest gain you can, but there is rarely a need for anything greater than 16 or 18 dB. Anything past that, and you start running into safety issues [2.4 GHz waves are used to cook your food in microwaves, and they will melt your eyes with long term exposure], and problems with cards not being able to push that much power.

Transceivers

Need a PCMCIA card? Get an Orinoco Gold. Best you can buy, well worth the price, and they have a nifty external antenna connector on them already.Need a PCI or ISA card? Don't ask me, I haven't used any, but what I'd do is get one of those PCI to PCMCIA adaptor thingys, and plug an Orinoco Gold into it. AP's and Bridges? The Linksys WET11 Ethernet Bridge is excellent. It's also extremely fast. As for access points, I'd probably also recommend linksys, unless you are an ISP or something, and have some money to throw around. I haven't tried Cisco's stuff, but I see no point in it. You'd just be buying a name with them. 3Com's equipment is also nice, and is usually affordable.

Cables, Connectors, and Other Doo-hickies

First off, you'll probably need a pigtail. this is nothing but a short little adapter cable that plugs into your 802.11 card, or other device, and has an N type connector on the other end. [It doesn't have to be type N, but that's the standard, so you might as well use it]. Next thing you need is a chunk of coax. Get LMR-400 if you can. Note, that it sometimes goes under other names. You'll need N connectors on both ends of that coax. Yes, you can put your own on, but sometimes it's just easier to buy a 20' section of it with the ends already on. Keep in mind when getting coax. . . . the shorter the cable run, the less signal loss you have. Don't use more than you have to.

After Setup

A few things you need to do after you get done hooking this all up. If this stuff is outside, go to the hardware store, and invest in a roll of this rubber tape stuff made by 3m. [Some places don't have it, but it's worth looking around for. Normal electrical tape is not the best for waterproofing] It's expensive, but worth it. Wrap the stuff around all the connections that are out in the elements. If water were to get into your connection, it'd be really really really hard on your radio, which could eventually fry the thing. As for antenna pointing, pointing it right at the other antenna isn't always best. Sometimes aiming right off the side depending on the radiation pattern might help your signal. Experiment, change only one direction at a time and see if it gets any better.

Conclusion

In high-density urban area there may be multiple networks like MPLS, Metro Ethernet, fibre networks, ADSL. There may also be many competing suppliers . WiMAX is a technology for providing high speed access to rural areas. It can provide DSL like speeds. Other considerations include making a business plan, terrain maps for the area, studying the coverage area (number of base / relay stations), tower rent, population of the region, bandwidth requirements, mobility etc. Acquiring Spectrum is also a consideration. Various terrain types such as hills with a rather high density of trees, moderate tree density,flat area with a low tree density can dictate the use of WiMAX technology Radio Waves are unpredictable and may go beyond the coverage area of the premises. Some parts of the coverage area may not get the radio waves.

References

[1]V. Gunasekaran, F. Harmantzis, "Emerging wireless technologies for developing countries ", Technology in Society 29 23–42, 2009.

[2]V.Abel, "Survey of Current and Future Trends in Security in Wireless Networks", International Journal of Scientific & Engineering Research (ISSN 2229-5518), April 2011

[3]V. Abel, A. Mnaouer, "On the Study of the WiMAX Security Threats and Current Solution Trends", Journal of the Caribbean Academy of Sciences, 2010.

[4] N.Sastry, J. Crowcroft, K. Sollins, "Architecting Citywide Ubiquitous Wi-Fi Access"

[5]http://www.tutorialspoint.com/wifi/wifi_major_issues.htm

[6]R.Barton,S.Hwu,M.Khayat,A.Schlesinger, "Lunar Surface EVA 802.16 Radio Study", NASA – Johnson Space Center, October 13, 2008

[7]V.Abel,R.Rambally, "An Analysis of WiMax Security Vulnerabilities", International conference on wireless networks and embedded systems WECON 2009

[8]V.Abel, "Survey of Attacks on Mobile Adhoc Wireless Networks", International Journal on Computer Science and Engineering, ISSN : 0975-3397, Vol. 3 No. 2, 2 Feb 2011.

[9]M. Lemm,"Business Prospects Of Wimax -- An ISP point of View", http://EzineArticles.com/243958