

WiMax and Wi-Fi in Current World

Vikas Solomon Abel, Rodney Rambally

Abstract — This paper discusses two of the latest wireless technologies, namely Wi-Fi and WiMAX technology. The intent in this paper is to provide a brief description of each of these technologies as well as the benefits and risks involved in their implementation. Real world applications of these technologies are also briefly discussed.

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

1 Wireless Technologies

THE aim behind Wireless Broadband technology is the support of mobile clients within a certain range as well as the provision of a wireless network infrastructure in places where wired networks are not feasible or possible. The three most important broadband wireless technologies are IEEE 802.11, IEEE 802.16, and Wireless Mesh Network (WMN).

Wi-Fi or Wireless Fidelity, connects to the internet at high speeds. Wi-Fi enabled devices operate in unlicensed spectrum. They use radio technologies within the range of an access point for data communication as shown in Fig 1 [1].

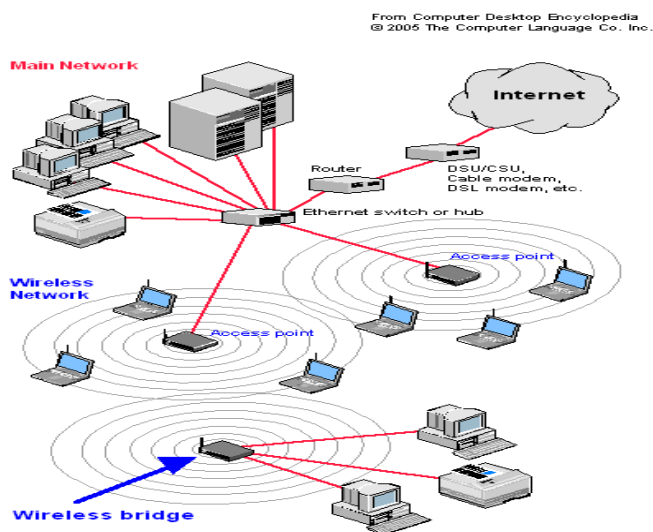
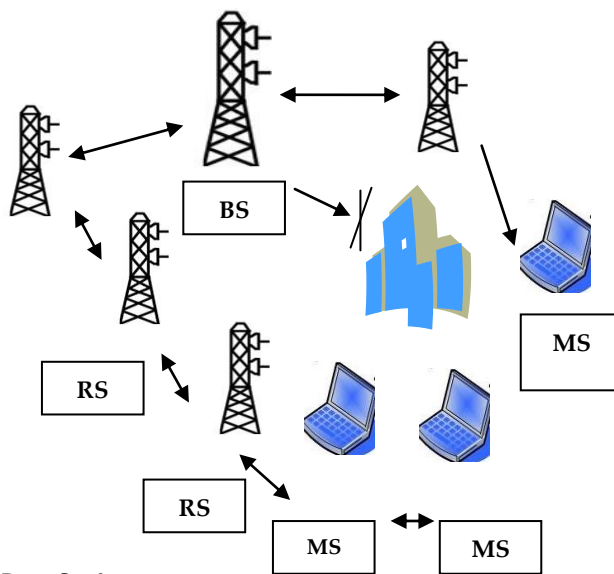


Fig 1. Wireless Fidelity

- Rodney Rambally is currently a Associate Professor in Information and Communication Technology Department in University of Trinidad and Tobago, Trinidad and Tobago, E-mail: rodney.rambally@utt.edu.tt
- Vikas Solomon Abel is currently a Senior Instructor in Information and Communication Technology Department in University of Trinidad and Tobago, Trinidad and Tobago, E-mail: vikas.abel@utt.edu.tt

WiMAX, an acronym for Worldwide Interoperability for Microwave Access, is a telecommunications technology that provides fixed and fully mobile internet access. The related sub-categories are:

1. 802.16-2004, also known as 802.16d, refers to the working party that has developed that standard. Since it has no support for mobility it is sometimes referred to as "Fixed WiMAX".
2. 802.16e-2005, also known as 802.16e, is an amendment to 802.16-2004. It introduced support for mobility, among other things, and is therefore also known as "Mobile WiMAX".
3. 802.16j-2009 is the Multihop Relay specification for 802.16 as shown in Fig 2 [2].



BS – Base Station
RS – Relay Station MS – Mobile Station

Fig 2. Multi-hop Relay Network architectures
Source : [3]

2 Wi-Fi

2.1 The Benefits of using Wi-Fi

1. Wi-Fi is a cost-effective and convenient alternative to a wired network.
2. Wi-Fi provides increased mobility to their users.

3. Cost associated with wiring cables and connectors is eliminated.
4. Ability to access Internet information in meeting rooms and other locations in the office gives ready information to the employees and increases the productivity.
5. Doctors, Lawyers, Airline travellers and other professionals view Wi-Fi as a very effective tool to get information readily. Members of a project can communicate with one other and keep one other informed of their progress in addition to also getting information from the Internet.
6. Wi-Fi helps in increasing revenues in Businesses like restaurants and other public places by creating hotspots to attract customers. This can be achieved at a low cost by a one time investment in the Wi-Fi infrastructure .
7. Connection to Wi-Fi by employees and guest visitors does not present any technical difficulty.
8. Wi-Fi is useful in space exploration, it is quite likely that space explorers may be carting around Wi-Fi-enabled PCs.

2.2 The risks of using Wi-Fi

If the Access Points (APs) are left unsecured, either to support free wireless access or because of lack of technical expertise, then security can be compromised [4].

A guest should not be able to misuse the bandwidth to an extent that the host is unable to sufficiently access the Internet. This could infect the network and the router itself [4].

Wi-Fi waves may propagate outside the walls of the building thereby causing intrusion by someone who is not authorized; the corporate network may also become susceptible to attacks.

2.3 ISP Perspective

The increase in the usage of laptops and development of wireless standards has made Wi-Fi a widely used technology . The computers need to have a wireless card and should be connected to a Wi-Fi access point or a

hotspot. Latest computers or laptops typically come with a built in wireless card.

Issues include security in Wi-Fi and its compatibility with other standards. For example 802.11a products are not compatible with 802.11b products, due to the different operating frequencies, and 802.11a hotspots would not help a 802.11b client [5].

3 WiMAX

3.1 The Benefits of using WiMAX

1. WiMAX technology can be quickly deployed to remote locations where the reach of copper networks is limited. It is relatively cheaper also.
2. When compared to GSM and 3G, WiMAX produces DSL like speeds and operates at greater distances at lower cost.
3. WiMAX offers uploading of large files .
4. WiMAX enables operators to offer triple-play services such as voice, data and video.
5. WiMAX provides features that businesses need. These include –
 - Quality of Service (QoS) which determines if a wireless technology can successfully deliver high value services such as voice and video
 - Toll-quality which is a voice call having quality comparable to that of an ordinary long distance call, originally placed over circuit-switched public telephone network .
 - Bandwidth at a low cost - WiMax provides fixed and mobile technology. WiMax promises a low cost, high bandwidth 4G technology.
6. NASA would like to utilize WiMAX relay stations, based on the evolving WiMAX 802.16j standard, to extend coverage and increase data throughput and to determine the feasibility of using IEEE 802.16 (WiMAX) as the communication protocol for lunar surface extra-vehicular activity (EVA) communications [6].
7. WiMax may be used to manage Application Layer Threats

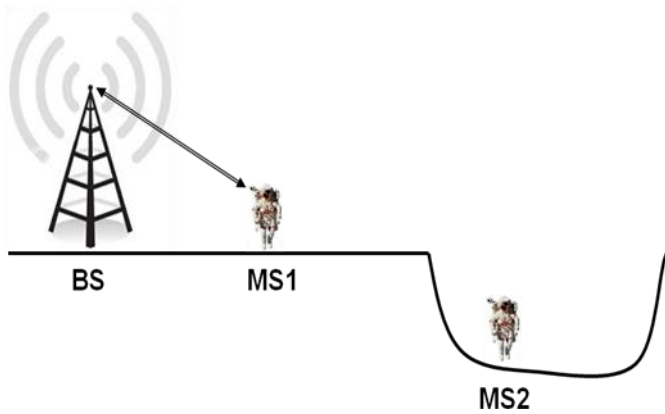


Fig 3. Lunar Scenario without 802.16j
 Source : [6]

In the scenario shown in Fig 3. Mobile Station 2 (MS2) is hidden by the crater and has limited or almost no communication with the Base station (BS) and has no communication with the Mobile Station 1.

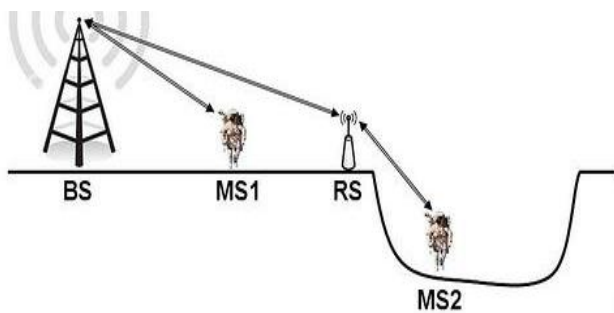


Fig 4. Lunar Scenario with 802.16j
 Source : [6]

In Fig 4. a Relay Station (RS) is introduced. Now the Mobile Station 2 (MS2) can communicate with the base station (BS) and has communication with the Mobile Station 1 because of the introduction of the Relay Station (RS).

3.2 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 [7].

2. Scrambling

Scrambling is another form of jamming, but for short intervals and is used to disorder targeted frames (mostly management messages) [7].

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 [7].

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 [7].

3. Denial of Service (DoS)

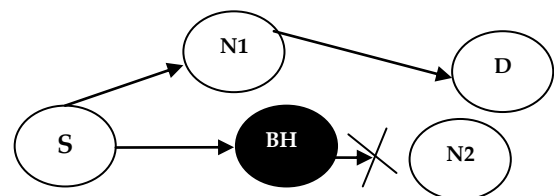
An attacker can force a BS to digest a large amount of handoffs and then launch a denial of service attack [7].

In an 802.16 mesh network deployment routers or gateways that reside between base station and client are susceptible to attacks in the application layer [7].

Network Layer Threats

1. Blackhole Attack

An attacker creates fake packets to target a valid node. A low cost route is advertised by the attacker. Subsequently the packets forwarded to it are dropped [7] as shown in Fig. 5.



S - Source
N1-Node1
N2 - Node2
BH - Blackhole
D - Destination

Fig 5. Blackhole Attack
 Source : [8]

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 [7].

3. Wormhole Attack

In a wormhole attack, an attacker creates a high quality out-of-band link and forwards packets and replays those packets at another location in the network through that out-of-band link [7]. This is demonstrated in Fig. 8.

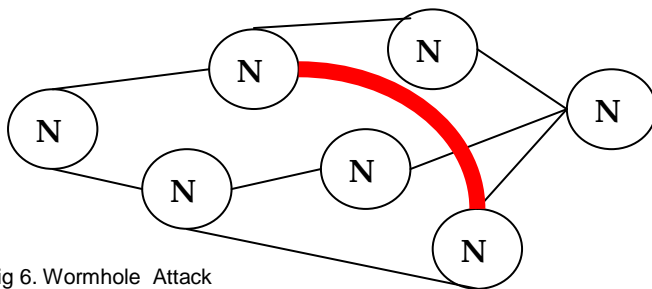


Fig 6. Wormhole Attack
Source : [2]

The attacks may be present as there is a “ad hoc 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 [7].

3.3 ISP Perspective

In high-density urban area there may be multiple networks like MPLS, Metro Ethernet, fibre networks, ADSL. There may also be many competing suppliers [9].

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/wi-fi/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>