

CPNI VIEWPOINT 04/2007

WIMAX OVER THE HORIZON

AUGUST 2007

Abstract

WiMAX is a standards-based technology enabling the delivery of last mile broadband wireless access as an alternative to wired broadband like cable and DSL. This Viewpoint discusses the key features of WiMAX, security considerations and typical architectures.

CPNI Viewpoints

CPNI Viewpoints are intended to provide a management level overview of emerging risks. A Viewpoint may not necessarily offer mitigation advice; other CPNI products are available for this purpose.

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

KEY POINTS

- **WiMAX** is defined by the WiMAX Forum as **Worldwide Interoperability for Microwave Access** - a standards-based technology enabling the delivery of last mile **broadband wireless** access as an alternative to wired broadband like cable and DSL.¹
- WiMAX operates in a similar way to Wireless Fidelity (Wi-Fi), but at higher speeds, over greater distances and for a greater number of users.
- The key benefits of WiMAX are **speed, coverage** and **cost**. In ideal circumstances, WiMAX is capable of speeds of up to 70Mbps over 30 miles. In practice, however, this is not likely to be achieved at the same time because range and bandwidth are inversely proportional.
- The two types of wireless service provided by WiMAX are: Line of Sight (LOS) and Non-Line of Sight (NLOS), where LOS is a straight, unobstructed line between two antennas. NLOS uses lower frequency transmissions that are not as easily disrupted by physical obstructions - they are better able to diffract, or bend, around obstacles.
- Due to the issues with security in Wi-Fi technology, the standards bodies have tried to incorporate security into WiMAX from the beginning. However, there are several vulnerabilities in WiMAX open to potential attack including: lack of base station authentication, unencrypted management frames, frequency jamming and disassociation frame flood attacks.²
- WiMAX could potentially cover suburban and rural areas that currently have no broadband Internet access.
- UK infrastructure comprises of legacy systems that make it difficult to introduce WiMAX as a replacement to fixed line technologies. This is similar for the broadband market, with the number of Internet Service Providers increasing due to relaxation in UK regulation.
- The mobile variant of the WiMAX standard (802.16e) could prove to be a real success if it is deployed in the UK, due to the increasing number of people working away from the office environment.
- WiMAX has widely been described as the high speed replacement to DSL and contender to 3G.

¹ **Broadband wireless** is defined to be the wireless transmission of data at high speed, usually at the generally accepted rate of 250Kbps and above, as well as the equipment and media that support the transmission.

² See NISCC Technical Note – The Security of 802.11 Wireless Networks accessible from the CPNI website:
<http://www.cpn.gov.uk/docs/re-20020814-00479.pdf>

INTRODUCTION

1. WiMAX has been widely described as the high speed replacement to DSL and is a realistic competitor to existing mobile technology, 3G. 3G is a current mobile phone technology delivering speeds of up to 2Mbps. WiMAX is still an emerging technology by comparison; it is however being piloted by a few companies in the UK.
2. In this paper, we will explore: what WiMAX is, how it works, security vulnerabilities, basic architectures, the WiMAX market in the UK, applications and compare it to Wi-Fi and 3G. Some knowledge of IT systems is assumed, but deep a technical background is not essential.
3. Acronyms are defined in the glossary at the end of this Viewpoint.

WHAT IS WIMAX?

4. **WiMAX** is defined as **W**orldwide **I**nteroperability for **M**icrowave **A**ccess by the WiMAX Forum, formed in June 2001 to promote conformance and interoperability of the IEEE 802.16 standard. Officially known as Wireless Metropolitan Area Network (MAN), IEEE 802.16 is the name collectively given to the suite of standards emerging from the IEEE Standards Authority.
5. The Forum describes WiMAX as “a standards-based technology enabling the delivery of last mile **broadband wireless** access as an alternative to wired broadband like cable and DSL. It provides fixed, nomadic, portable, and mobile wireless broadband connectivity without the need for direct Line-of-Sight (LOS) with a base station”, where LOS is a straight, unobstructed line between two antennas. LOS and Non-Line-of-Sight (NLOS) are covered in more detail later in this paper.³
6. As a broadband wireless access technology, WiMAX can provide the ‘last mile’ of the communications link. However, its extended capabilities in terms of radio range and data throughput widens the number of applications that it could potentially address.
7. The ability to actively manage the radio connection to ensure the highest possible link quality and the Quality of Service (QoS) management functions to offer either ‘guaranteed’ or ‘best effort’ services to enterprise or domestic customers alike, are two of the advanced features of WiMAX.
8. The key benefits of WiMAX are;
 - **Coverage and Speed:** As a technology, WiMAX, in ideal circumstances, is capable of speeds of up to 70Mbps over 30 miles. One single WiMAX connection, therefore, would have the equivalent capacity of a lot of ISDN-type lines. In practice, however, the maximum coverage and speed is not likely to be achieved at the same time.
 - **Cost:** An obvious advantage to a wireless technology, such as WiMAX, is the absence of cable compared to a wired infrastructure, which represents a significant reduction in initial capital expenditure. It also makes it easier to extend to suburban and rural areas.

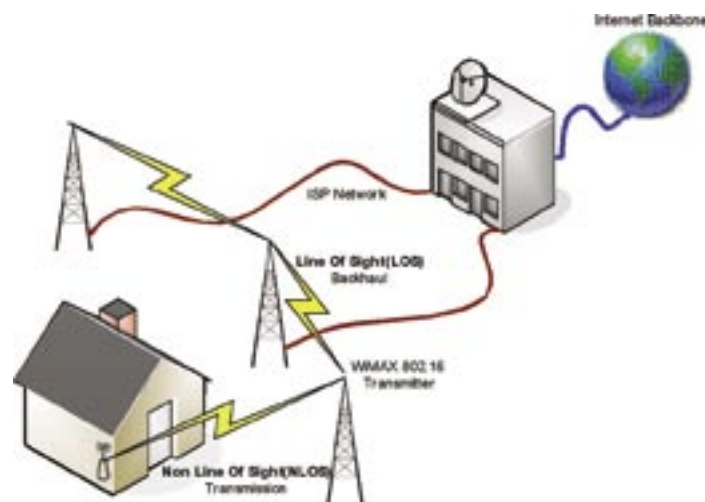
³ **Broadband wireless** is defined to be the wireless transmission of data at high speed, usually at the generally accepted rate of 250Kbps and above, as well as the equipment and media that support the transmission.

TECHNICAL DETAIL

HOW DOES IT WORK?

9. WiMAX operates in a similar way to Wi-Fi, but at higher speeds, over greater distances and for a greater number of users. Most, if not all, WiMAX systems consist of two parts:
 - **Transmitter:** Usually a tower-like structure supports the WiMAX antennas. This is similar in concept to a mobile phone mast which is typically connected to the network using a standard wired, high-speed connection. WiMAX typically uses a microwave link to establish a connection to the network. A single WiMAX tower can provide coverage to an area up to 8,000 square km.
 - **WiMAX receiver (or Customer Premises Equipment - CPE):** The receiver and internal antenna can be a small box or PCMCIA card, and they can be built into a laptop the way Wi-Fi access is today.
10. In general, the communications are described as follows:
 1. A subscriber sends wireless traffic at speeds ranging from 2Mbps to 155Mbps from a fixed antenna – usually on a building. In Figure 1, indoor CPE is used in conjunction with a fixed antenna.
 2. The WiMAX 802.16 transmitter disperses transmissions from multiple sites and sends traffic over wireless or wired links to a switching centre using the 802.16 protocol.
 3. The switching centre sends traffic to an Internet Service Provider (ISP) or the Public Switched Telephone Network (PSTN).

Figure 1. How WiMAX works



11. There are two types of wireless service provided by WiMAX. These are; Line of Sight (LOS) and Non-Line of Sight (NLOS) – both can be seen in Figure 1.

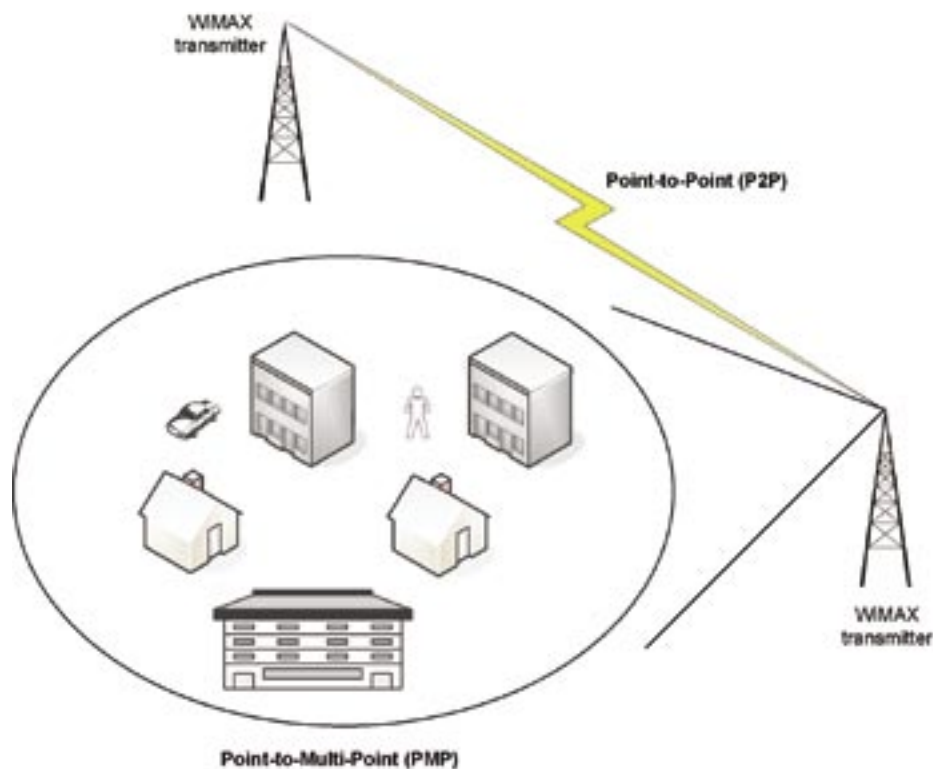
- **Line of Sight (LOS):** A fixed dish antenna points straight at the WiMAX tower from a rooftop or pole. The LOS connection carries a higher bandwidth with fewer errors. Line-of-sight transmissions use higher frequencies, with ranges reaching a possible 66 GHz. At these higher frequencies, there is less interference and lots more bandwidth. This makes them a popular choice for providing a backhaul service.⁴
- **Non Line of Sight (NLOS):** This is comparable to a Wi-Fi service, where a small antenna on a computer communicates to the tower antenna. In this mode, WiMAX uses a lower frequency range of 2GHz to 11GHz (similar to Wi-Fi). Shorter wavelength or lower frequency transmissions are not as easily disrupted by physical obstructions, they are better able to diffract, or bend around obstacles.

WHAT IS THE BASIC ARCHITECTURE?

Point-to-Multipoint (PMP)

12. The most typical WiMAX-based architecture includes a base station mounted on a building, which communicates on a **Point-to-Multi-Point (PMP)** basis with a subscriber station (SS) (or CPE) located in business offices and homes. As seen in Figure 2, PMP is synonymous with distribution. One base station can service hundreds of dissimilar subscribers in terms of bandwidth and services offered.

Figure 2. PMP & P2P/PTP



⁴ Backhaul is the communications infrastructure that connects the access network equipment (base stations and wireless access points) to the core network (switching or routing devices)

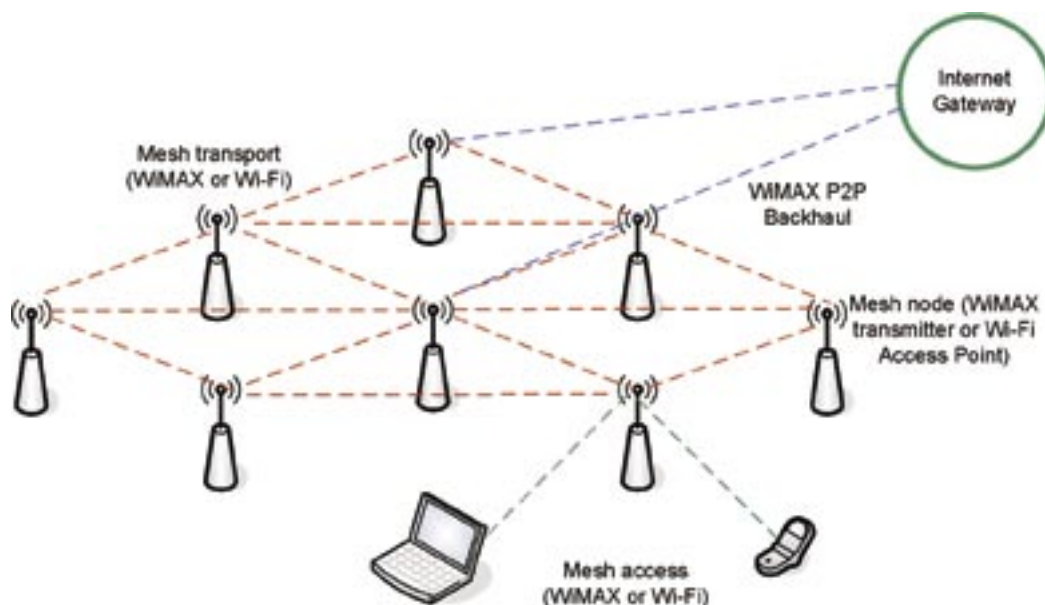
Point-to-Point (P2P or PTP)

13. **Point-to-Point (P2P)** is used where there are only two points of interest: one sender and one receiver. This is also a scenario for backhaul or the transport from the data source (data centre, central office etc) to the subscriber or for a point for distribution using PMP architecture. As the architecture calls for a highly focused beam between two points, range and throughput of point-to-point radios will be higher than that of PMP products. This is an example of a LOS service.

Mesh Architecture

14. In a mesh network, each node (i.e. base station or access point) connects to several neighbouring nodes and on to an Internet gateway (i.e. a base station that aggregates the mesh network traffic and routes it to the Internet) – see Figure 3. Since each node has many routes to a mesh gateway, there is built-in resilience in a mesh network.
15. The combined system solution of using WiMAX for backhaul, Wi-Fi or WiMAX mesh and Wi-Fi or WiMAX for user access gives operators the ability to cost-effectively deliver wireless (WiMAX or Wi-Fi) Internet access over considerable outdoor distances and in a range of network environments. Costs are reduced through the rapid provisioning and simplified management of Wi-Fi and WiMAX services.
16. Wi-Fi mesh is limited in certain respects. Indoor coverage is not as good as it could be and it is susceptible to interference by devices such as microwave ovens. Trees and buildings can also block the signals.

Figure 3. Wi-Fi Mesh Network



WIMAX IN THE UK

17. The licensed band for WiMAX in the UK (also for Western and Eastern Europe) allotted by the European Telecommunications Standards Institute (ETSI) is 3.5 GHz (3.3 GHz – 3.8 GHz), originally used for the wireless local loop (WLL).
18. In the UK, licensed WiMAX spectrum is currently held by two companies: UK Broadband Ltd. (3.4 GHz) and Pipex (3.5 GHz) – the latter of which has recently been sold to an Italian firm, Tiscali. The frequencies they currently own, however, sit directly in the middle of the WiMAX frequency range – ideal for running a broadband service. Both UK Broadband Ltd. and Tiscali offer WiMAX-based broadband and have already launched limited services.
19. WiMAX requires a new infrastructure, but rolling out a large network involves large capital expenditure if covering sizeable areas. Organisations like UK Broadband Ltd. and Tiscali do not own their own infrastructure, therefore, have to buy or lease infrastructure from other operators, which is the biggest cost in the network.
20. Unlicensed WiMAX systems in the UK operate in the 5.8 GHz (5.25 GHz – 5.85 GHz) band, where the 802.11a standard is defined to operate. The majority of countries globally have also embraced the 5GHz spectrum for license-exempt communications providing economies of scale for manufacturers of chipsets. Some governments and service providers, however, are concerned that interference resulting from the availability of too many license-exempt bands could affect critical public and government communication networks, such as radar systems.⁵
21. The key features of a WiMAX system in a licensed or unlicensed band can be seen in the table below.

Licensed WiMAX System	Unlicensed WiMAX System
<ul style="list-style-type: none"> • High cost to entry – coupled with exclusive ownership of a band, enables service quality improvements and reduces interference • More power • Better coverage • Less interference – but not entirely exempt from interference, which occurs within an organisation’s own network • Lower frequency band – this is better for NLOS (mobile) use • Exclusive rights service – more predictable and stable solution for large metropolitan deployments and mobile usage • Co-channel interference • System planning required 	<ul style="list-style-type: none"> • Low or no entry cost • Reduced range due to power restrictions • Faster roll-out, reduced time to market • Globally common band means economies of scale for chipset manufacturers • Accelerating broadband in developing markets • Possible uncoordinated interference • Careful system design required to avoid interference

⁵ **Unlicensed** or **license-free** spectrum as it is sometimes called simply means a spectrum band that has rules pre-defined for both the hardware and deployment methods of the radio in such a manner that interference is mitigated by the technical rules defined for the bands rather than it being restricted for use by only one entity through a spectrum licensing approach.

Any person or entity that does not infringe upon the rules for the equipment (which in practical terms is all pre-certified by the manufacturer) or its use can put up a license free network at any time for either private or public purposes including commercial high speed Internet service.

22. The regulator, Ofcom, hopes to release more spectrum – two x 100MHz bands in the 10GHz range could be available sometime in 2007. At the top-end of the frequency range, the bands have very poor characteristics for WiMAX i.e. the radio signals will not penetrate buildings; therefore, all of the infrastructure will have to use LOS.
23. There is the possibility that spectrum could be made available in the 2GHz band – specifically, 2.5 – 2.6 GHz; 2.01 – 2.025 GHz and 2.29 – 2.3 GHz, but this is currently allocated to 3G use. It could be a long time before it gets released as parts of Europe are using it for 3G; there are interference issues to consider.
24. WiMAX trials (indoor and outdoor) are being held all over the UK. Pipex UK announced results for one of its WiMAX trials in Stratford-upon-Avon. Speeds in excess of 2Mbps (uplink and downlink) were achieved indoors at a range of 1.2km (0.75 miles) from the base station with no direct line of sight. Drive tests using the indoor antenna in a vehicle at various distances from the base station showed symmetric speeds of 5Mbps. Speeds of 10Mbps down and 9Mbps up were achieved to external antennas at the test house at 1.2km from the base station. Longer range tests with external antennas achieved 6Mbps down and 4Mbps up at a range of 6km from the base station.
25. Intel is one company promoting WiMAX and is investing heavily in its development. The organisation intends to release chipsets with WiMAX capability to the general public in early 2008 in notebooks and PDAs. Equipment is rumoured to comply with 802.16e only to fit in with the theory that mobile WiMAX will be better accepted into the UK's infrastructure. Intel's venture capital arm partnered with Pipex in 2006 to form the UK-based company Pipex Wireless.

THE WIMAX MARKET

WIMAX APPLICATIONS

Broadband replacement

26. WiMAX can be used to provide a wireless alternative to cable and DSL for the 'last mile' of broadband access. The 'last mile' is the final leg of delivering communications connectivity to a resident or customer. Usually referred to by the telecommunications and cable industries, it is typically seen as an expensive challenge because 'fanning out' wires and cables is a considerable fiscal and physical undertaking.

Rural broadband

27. The distance and remoteness often mean that rural broadband is an expensive proposition for the service provider. Houses in rural areas are often located a long way from a supply point.
28. A service provider Point of Presence (PoP) will be the local exchange building or a radio mast – the equipment supplying broadband services are range limited in their operation. Typically DSL services require the CPE to be within 5km of the PoP.
29. The 'last mile' issue is only part of the problem; the backhaul connection from the PoP to the Internet interconnection must also be considered. In urban areas, these connections are not readily available, but when accessible they are also heavily used making them cost effective to operate. The rural community distributed over wide geographical areas contains fewer

subscribers whose use of the Internet services may not be as frequent or demanding as those of the urban businesses or residential users (i.e. MAN residents). The rural subscriber must therefore bear the additional cost of providing the backhaul service to the rural PoP; this is not cost effective as the connection is often under utilised.

30. From a distance and remoteness perspective, WiMAX has the potential to provide both the backhaul transmission and broadband solution due to its extended range.

Mobile backhaul

31. Mobile operators are required to deploy thousands of base stations in order to gain the required coverage and capacity which means the most complex and often the most expensive part of their networks is the backhaul connection.

Wi-Fi backhaul

32. The number of Wi-Fi hotspots being installed around the world is growing at an ever increasing rate. The cost of buying and installing a wireless Access Point (AP) may be negligible to a business, however an Internet connection is still required. A public access Wi-Fi hotspot may attract a high volume of traffic therefore the backhaul connection needs to support this capacity. Transmission rates of 2Mbps or in increments, a leased line solution could be used but this may be expensive, particularly in city centre areas.

Business Continuity

33. WiMAX can provide a diverse source of Internet connectivity as part of a business continuity plan. That is, if a business has a fixed and a wireless internet connection they are less likely to be affected by the same service outage. However, it will still be necessary to ensure that the connections do not share any facilities at any point. Natural disaster areas may benefit from this type of deployment.

Wireless Voice over IP (VoIP)

34. VoIP is a technology that has been around for many years, though applications tended to be restricted to enterprise VoIP over LAN solutions. More recently, it has been popularised by Internet-based applications like Skype and Vonage.⁶
35. Broadband subscribers are signing up for VoIP services very rapidly, the attraction being 'free' or very cheap calls. The cost-effective nature of the service is itself very attractive to a large fixed telecoms provider or mobile operator.
36. The next step for many subscribers is wireless VoIP, 'free' or cheap calls whilst on the move. Current cellular technologies struggle to meet the needs of a VoIP connection, therefore mobile operators are not in a position to immediately offer VoIP services. WiMAX is particularly suited to voice transmissions due to;

⁶ For more information on VoIP, see the NISCC Viewpoint – "Voice over IP", accessible from the CPNI website: http://www.cpni.gov.uk/docs/vp_01_2006.pdf
CPNI also intend to release a Viewpoint on Enterprise VoIP, which will be available on the main website.

- the wide data bandwidth it can offer (802.11g 54Mbps)
- WiMAX's ability to provide carrier grade connection even in a NLOS environment and manage the quality of individual connections.

37. By 2009, In-Stat (the communications industry market researcher) forecasts there will be 4.4 million Voice-over-WiMAX (VoWiMAX) subscribers, worldwide.

4G

38. The IEEE has started work on a 1Gbit/s version of WiMAX, which could seize the coveted '4G prize', and replace both cellular and WiMAX. The IEEE says it will have the 802.16m standard ready during 2009, and it will use current Orthogonal Frequency Division Modulation (OFDM) and Multiple-Input Multiple-Output (MIMO) technologies, with which some companies have already demonstrated Gigabit wireless speeds.^{7 8}

It will also have backwards compatibility with the current mobile WiMAX standard, 802.16e, and will also be suitable for fixed as well as mobile links.

39. Before getting to this position, there are technology issues to resolve, such as, packing the multiple antennas which the technology requires into a mobile device.

40. The larger problem is a political one. If this standard is to merge the two worlds of 3G and WiMAX, then an IEEE standard must be accepted as the next step in the cellular roadmap, which is currently determined by the ITU telecoms standards body, with the operator-led 3GPP group.

41. Other applications of WiMAX might include;

- Asynchronous Transfer Mode (ATM) backhaul⁹
- Online gaming
- Security and surveillance
- Telematics and telemetry

HOW DOES WIMAX COMPARE TO WIFI AND 3G?

42. Wireless Fidelity (Wi-Fi) (IEEE 802.11x)

- **Range:** WiMAX offers a greater range
- **Bandwidth:** WiMAX is more bandwidth-efficient and ultimately may be used to provide connectivity to entire cities
- **Mobility:** WiMAX can be incorporated into laptops to give users an added measure of mobility

7 Orthogonal Frequency Division Modulation (OFDM) – A method used for carrier modulation in digital transmissions. A spread spectrum technique, it combines good noise resistance, immunity to reflections and efficient use of the spectrum.

8 MIMO (Multiple-Input Multiple-Output) – A technique that uses multiple antennas to increase throughput, phenomena such as multipath propagation to increase throughput,

9 Asynchronous Transfer Mode (ATM): A high bandwidth, high speed (up to 155 Mbps), controlled-delay fixed-size packet switching and transmission system integrating multiple data types (voice, video, and data).

- The WiMAX specification provides symmetrical bandwidth over many kilometres and range with stronger encryption (3DES or AES) and typically less interference. Wi-Fi is short range (approximately 10s of metres) has WEP or WPA encryption and suffers from interference in metropolitan areas where there are many users.
- Wi-Fi Hotspots are typically backhauled over ADSL, therefore Wi-Fi access is typically highly contended and has poor upload speeds between the router and the internet.

43. 3G

- 3G is third-generation technology in the context of mobile phone standards. Services associated with 3G include wide-area wireless voice telephony and broadband wireless data, all in a mobile environment.
- 3G is capable of speeds ranging from 384Kbps to 2Mbps, which may not be as high as WiMAX, but are sufficient for video telephony.
- The low cost of Broadband Wireless Access (BWA)/WiMAX spectrum compared to 3G is a clear driver for service providers to enter the field of wireless services with WiMAX.
- The price paid per Hz for WiMAX spectrum is as much as 1,000 times lower than for 3G spectrum. North America is currently the leading region in terms of the number of BWA/WiMAX licenses awarded with a total of 394 BWA/WiMAX license holders, against 186 licensees in Europe, 97 licensees in Asia, and 49 licensees in the Caribbean and Latin American region.
- WiMAX and 3G are not necessarily mutually exclusive. There are benefits in finding the right mix of the two technologies. WiMAX can provide the necessary support to help augment 3G.

SECURITY CONSIDERATIONS

44. Standards bodies have attempted to prioritise security in WiMAX as a lesson from the security flaws discovered in WEP in the 802.11 Wi-Fi technology. However, despite good intentions, there are several known potential attacks open to adversaries, including:
- Denial of Service (DoS) attacks
 - Rogue base stations
 - Session hi-jacking
 - Network manipulation with spoofed management frames
 - Disassociation flood attacks
 - Man-in-the-middle attacks
 - Other attacks including WiMAX protocol fuzzing this may enable attackers to further manipulate a Base Station (BS) or Subscriber Station (SS).¹⁰

¹⁰ Protocol fuzzing is a testing methodology that manipulates protocols and targets systems in an iterative fashion by sending intentionally flawed network traffic in an attempt to expose weaknesses that may be used as a venue for security breaches.

Confidentiality

45. The absence of security at the physical layer means that a rogue BS can impersonate a legitimate BS. This makes session hijacking possible and the attacker could gain access to sensitive information.
46. Fuzzing (testing the robustness of a program by sending malformed packets to a program's interfaces) has become a popular hobby for hackers, and it is unclear whether WiMAX implementers will address this problem by following secure coding standards.
47. A fundamental principle in 802.16 networks is that each SS or CPE must have an X.509 certificate that will uniquely identify it. The use of X.509 certificates should make it more difficult for an attacker to spoof the identity of legitimate subscribers. However, mutual authentication between the BS and SS is not provided, which leaves the identity of the BS open to spoofing.

Integrity

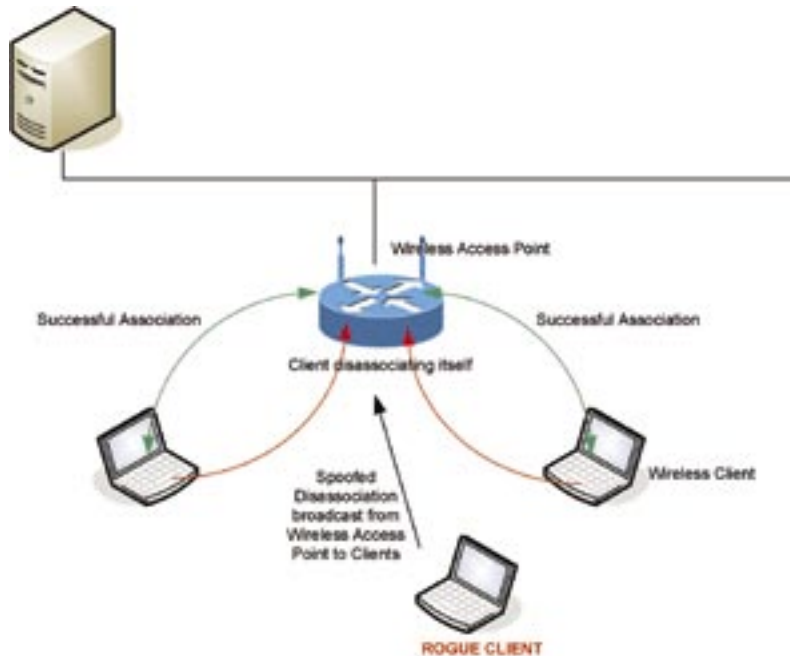
48. With the 802.16e amendment, support for the AES cipher is available, providing strong support for confidentiality of data traffic. However, like the 802.11 specification, management frames are not encrypted, allowing an attacker to collect information about subscribers in the area and other potentially sensitive network characteristics. When AES is not used, data traffic modification is possible. WiMAX is also capable of supporting 3DES.
49. The 802.16e amendment has added support for the Extensible Authentication Protocol (EAP) to WiMAX networks. Support for EAP protocols is currently optional for service providers.
50. As noted above, a fundamental flaw in the authentication mechanism used by WiMAX's Privacy and Key Management (PKM) protocol is the lack of BS or service provider authentication. This makes WiMAX networks susceptible to man-in-the-middle attacks, exposing subscribers to various confidentiality and availability threats. A man-in-the-middle attack is an integrity issue.

Availability

51. WiMAX deployments using licensed Radio Frequency (RF) spectrum give some measure of protection from unintentional interference. It is reasonably simple, however, for an attacker to use readily available tools to jam the spectrum for all planned WiMAX deployments resulting in DoS.
52. In addition to physical layer denial of service attacks, an attacker can use legacy management frames to forcibly disconnect legitimate stations, resulting in a DoS scenario. The attack is similar to the disassociation flood attacks used against 802.11 networks.
53. A disassociation flood attack is a form of DoS attack that forces a client to the disassociated/authenticated state by spoofing disassociation frames from the access point to a client. Typically, client stations would re-associate to regain service until the attacker sends another disassociation frame. An attacker would repeatedly spoof the disassociation frames to keep the client out of service. See Figure 4.

54. The gaps in WiMAX security, specifically in user terminals, intrusion detection and connectivity service networks, present opportunities for security companies, but risks for users.

Figure 4. Disassociation flood attack



CONCLUSIONS

55. WiMAX could potentially erase the suburban and rural blackout areas that currently have no broadband Internet access because phone or cable companies have not yet run the necessary high-capacity wires to those remote locations. Because WiMAX does not depend on cables to connect each endpoint, deploying WiMAX to an entire community or campus can be done in a matter of days, saving significant amounts of manpower.
56. The UK infrastructure comprises of legacy systems that make it difficult to introduce WiMAX as a replacement to fixed line technologies.
57. While approval of the 802.16e standard by the IEEE is a critical step, certification of the profile based on this standard, led by the WiMAX Forum, holds the key to its adoption. The mobile variant of the 802.16 standard could prove to be a real success should it be deployed in the UK, due to the increasing number of people working away from the office.
58. WiMAX has the potential to offer high speed broadband access to all, but in the UK there is little spectrum currently available. The release of spectrum is an ongoing issue and may potentially hinder the future success of the technology.
59. WiMAX has some security concerns, such as man-in-the-middle attacks, but the real test of WiMAX security will come when providers begin wide-scale network deployments, and researchers and attackers have access to commodity CPE equipment. Until then, the security of WiMAX is limited to speculation.

BIBLIOGRAPHY/REFERENCES

1. **Telecoms Academy, UK** "WiMAX Explained" course notes
2. **Wikipedia** Online Encyclopaedia http://en.wikipedia.org/wiki/Main_Page
3. The **Institute of Electrical and Electronics Engineers Inc.** <http://www.ieee.org>
4. **Office of Communications** UK Telecommunications regulator <http://www.ofcom.org.uk>
5. **Pipex Wireless** <http://www.pipexwireless.com>
6. **UK Broadband Ltd.** <http://www.ukbroadband.co.uk/index.html>
7. **TechWorld** UK Infrastructure and network knowledge centre for IT professionals <http://www.techworld.com>
8. **The Register** IT & Comms News <http://www.theregister.com>
9. **Urban WiMAX Plc** <http://www.urbanWiMAX.co.uk>
10. **The WiMAX Forum** <http://www.WiMAXforum.org/home/>
11. **WiMAX Industry** Broadband Wireless News & Marketplace <http://www.wireless-industry.com>
12. **Wireless Week** Wireless News <http://www.wirelessweek.com>
13. **ZDNet** Tech News, Blogs and Whitepapers for IT Professionals <http://www.zdnet.com>

GLOSSARY

3G	Third Generation (mobile communication). Generally used as reference to public mobile communication systems based on the UMTS standard.
3DES	In cryptography, Triple DES (3DES) is a block cipher formed from the Data Encryption Standard (DES) cipher.
4G	Providing high-speed mobile data and telecommunications services
ADSL	Asymmetric Digital Subscriber Line (ADSL) - a technology that allows more data to be sent over existing copper telephone lines, where the upload speed is different from the download speed. Usually the download speed is much greater.
AES	Advanced Encryption Standard - a security algorithm used increasingly as an alternative to DES. The algorithm must be used with key sizes of 128 bits, 192 bits, or 256 bits depending on the application security requirement.
Backhaul	Backhaul is the communications infrastructure that connects the access network equipment (base stations and wireless access points) to the core network (switching or routing devices)
Base Station (BS)	A low-power, multi-channel two-way radio in a fixed location.
CPE (or Subscriber Station – SS)	The Customer Premises Equipment (CPE) for DSL services is a DSL modem.
DES	Data Encryption Standard is a method of encrypting data using a shared 56 bit key.
Downlink (Uplink)	Technical term for data transmission in the direction from the network, the provider or the Internet provider to the subscriber. (The return channel is known as the uplink).
DSL	Digital Subscriber Line (DSL) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines. A DSL can carry both data and voice signals and the data part of the line is continuously connected.
ISDN	Integrated Services Digital Network (ISDN) is a type of circuit switched telephone network system, designed to allow digital (as opposed to analogue) transmission of voice and data over ordinary telephone copper wires, resulting in better quality and higher speeds than available with analogue systems.
LOS	Line of Sight (LOS) is a straight, unobstructed line between two antennas.
Metropolitan Area Network (MAN)	A data network designed for a town or city.
Mbps	Megabits per second
Mesh networking	A way to route data, voice and instructions between nodes. It allows for continuous connections and reconfiguration around broken or blocked paths by ‘hopping’ from node to node until the destination is reached. Mesh networks are self-healing: the network can still operate even when a node breaks down or a connection goes bad. As a result, a very reliable network is formed. This concept is applicable to wireless networks, wired networks and software interaction.

NLOS	Non-Line of Sight (NLOS) is where no line can be drawn between two transmitting devices. Best suited for mobile use.
P2P or PTP	Point-to-Point is used where there are two points of interest: one sender and one receiver. This is also a scenario for backhaul or the transport from the data source (data centre, central office etc) to the subscriber or for a point for distribution using PMP architecture.
PCMCIA card	The PCMCIA is the Personal Computer Memory Card International Association, an industry trade association that creates standards for notebook computer peripheral devices.
PDA	Personal Digital Assistant.
PMP	Point-to-Multi-Point (PMP) is most typical WiMAX-based architecture, which includes a base station mounted on a building, which communicates with multiple subscriber stations (or CPEs) located in business offices and homes.
PoP	A PoP (Point-of-Presence) is the location of an access point to the Internet. A PoP necessarily has a unique Internet (IP) address. Your Internet Service Provider (ISP) has a point-of-presence on the Internet. A PoP usually includes routers, digital/analogue call aggregators, servers, and frequently, frame relay or ATM switches.
Telematics	The integrated use of telecommunications and informatics, also known as Information and Communications Technology (ICT). More specifically it is the science of sending, receiving and storing information via telecommunication devices.
Telemetry	Telemetry is remote measurement or the remote collection of data. Telemetered data can be physical, environmental or biological data. Telemetry is typically used to gather data from distant, inaccessible locations, or when data collection would be dangerous or difficult for a variety of reasons. Telemetry can also mean radio signals from a spacecraft used to encode and transmit data to a ground station.
UMTS	Universal Mobile Telecommunications System (UMTS) - broadband, packet-based transmission of text, digitised voice, video, and multimedia at data rates up to and possibly higher than 2Mbps, offering a set of services to mobile computer and phone users no matter where they are located in the world.
WEP	Wired Equivalency Privacy is a security protocol for Wi-Fi networks.
Wi-Fi:	A brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks based on the IEEE 802.11 specifications.
Wireless Local Loop (WLL)	Also called radio in the loop (RITL) or fixed-radio access (FRA), is the use of wireless connection as the last mile for delivering plain old telephone service (POTS) to customers.
WPA	Wi-Fi Protected Access (WPA) is a data encryption specification for 802.11 wireless networks that replaces the weaker WEP. Created by the Wi-Fi Alliance before an 802.11i security standard was ratified by the IEEE, it improves on WEP by using dynamic keys, Extensible Authentication Protocol to secure network access, and an encryption method called Temporal Key Integrity Protocol (TKIP) to secure data transmissions.