Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Wimax Technology: A Secure Broadband Connectivity for Governments, Military Services in Rural/Strategic Isolated Locations

Mr. Sanjeev Kumar Choudhary
Research Scholar
ASET,
Noida (U.P), India

Mr. Sanjay Kumar Dubey
Asst. Professor
ASET,
Noida (U.P), India

Mr. Ramesh Gupta
Lecturer
SET,
AIT Gurgaon (Hr.), India

Abstract - Considering the universal usage of mobile phones, in this paper we have proposed a solution to broadband facility in strategic isolated locations through implementation of WiMax technology. Thus ensuring the secure broadband services to Governments, military, Hospital, Transport services in rural and isolated locations. We have started by justifying the need for a shift towards WiMax technology by providing proper citations on disadvantages of existing technology and how WiMax surmounts them. Further, insights into the WiMax technology, its implementation and the corresponding hardware requirements in mobile owing to WiMax have been provided.

Key word: PAN, MAN, WAN, Wimax, Blue Tooth

I. INTRODUCTION

Governments, military, corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, strategies, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers. The confidential information about Governments planning, military strategies, a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to negative consequences. Protecting confidential information's is every agencies requirement, and in many cases it is also a legal requirement. Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take i.e electronic, physical, etc. Information Technology Security is information security applied to technology. It is keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems. Information assurance is the act of ensuring that data is not lost when critical issues arise. These issues include but are not limited to; natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arises. This paper presents a general overview of information security in WIMAX technology implementation.

II. Key Concepts

Confidentiality, integrity and availability are one of the core principles of information security.

1. Confidentiality

Confidentiality refers to preventing the disclosure of information to unauthorized individuals or systems. For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred. Confidentiality is necessary for maintaining the privacy of the people whose personal information a system holds.

2. Integrity

The data integrity is maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner.

3. Availability

The information must be available when it is needed to serve its purpose. Ensuring availability also involves preventing denial-of-service attacks.

4. Authenticity

In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties

involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

5. Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

6. Access control

Access to protected information must be restricted to people who are authorized to access the information. The foundation on which access control mechanisms are built start with identification and authentication.

7. Identification

Identification is an assertion of person who can be granted access to protected information. It will be necessary to verify the person.

8. Authentication

Authentication is verifying a person to grant access to the system on verification. There are three different types of information that can be used for authentication:

- PIN, a password, magnetic swipe card.
- Biometrics, palm prints, fingerprints, and retina (eye) scans.

9. Cryptography

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted can be transformed back into its original usable form by an authorized user, who possesses the cryptographic key, through the process of decryption. Cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit either electronically or physically and while information is in storage.

Cryptography provides information security with other useful applications as well including improved authentication methods, message digests, digital signatures, non-repudiation, and encrypted network communications. Older less secure applications such as telnet and ftp are slowly being replaced with more secure applications such as ssh that use encrypted network communications. Wireless communications can be encrypted using protocols such as WPA/WPA2 or the older (and less secure) WEP. Wired communications (such as ITU-T G.hn) are secured using AES for encryption and X.1035 for authentication and key exchange. Software applications such as GnuPG or PGP can be used to encrypt data files and Email.

Cryptography can introduce security problems when it is not implemented correctly. Cryptographic solutions need to be implemented using industry accepted solutions that have undergone rigorous peer review by independent experts in cryptography. The length and strength of the encryption key is also an important consideration. A key that is weak or too short will produce weak encryption. The keys used for encryption and decryption must be protected with the same degree of rigor as any other confidential information. They must be protected from unauthorized disclosure and destruction and they must be available when needed. Public key infrastructure (PKI) solutions address many of the problems that surround key management.

III. AVAILABLE WIRE LESS TECHNOLOGY

Each wireless technology is designed to serve a specific usage segment:

• Personal area networks (PANs)
• Local area networks (LANs)
• Metropolitan area networks (MANs)
• Wide area networks (WANs)

The requirements for each usage segment are based on a variety of variables, including:

• Bandwidth needs
• Distance needs
• Power
• User location
• Services offered
• Network ownership

1. Wireless Personal Area Networks (PAN)

The first usage segment is the wireless PAN,. Typical network coverage in the PAN is up to ten meters, but performance varies depending on the standard employed.

1.1 The IEEE 802.15.1 standard (also called Bluetooth) is primarily used for unwiring computing and communication peripherals, such as a computer to a printer or a handset to a headset. Bluetooth is rated up to 1 Mbps in performance data rates.

1.2 The second standard in this usage segment, the IEEE 802.15.3 standard (also called ultra-wide band), is designed for delivering multimedia services. UWB supports data rates over 400 Mbps, allowing for video of digital video disc (DVD) quality to be shared throughout the home. In this case the PAN becomes a high-speed personnel area network.

2. Wireless Local Area Networks
Standards based WLANs typically have these features:
• Service more applications and users than do PANs
• Cover a greater distance than PANs: up to 100 meters
• Aggregate PANs

The wireless standard associated with WLANs is IEEE 802.11.
Three major revisions to the physical layer have been released:
• 802.11a supports bandwidth speeds up to 54 Mbps
• 802.11b supports bandwidth speeds up to 11 Mbps
• 802.11g supports bandwidth speeds up to 54 Mbps

3. Metropolitan Area Networks
The wireless MAN aggregates LANs and typically covers areas up to 50 km. Both WiMAX and coppered wired technologies (such as DSL and DOCSIS cable) are used in this usage segment.

4. Wide Area Networks
WANs aggregate MANs across large geographic areas (over 50 km). WAN uses a variety of communication media to pass large amounts of traffic from the various MANs. However, the most common media used are fiber optic links. This set of high-speed, high-bandwidth interconnections is referred to as the core network. Performance of WAN networks is up to 10 Gbps and depends on the type of traffic the network handles: voice only or voice, video and data.

Today, the popularity, cost benefits and throughput associated with Wi-Fi networks have caused a growth in network deployments, use and adoption. This is due to the options available in achieving access to the last mile. WISPs (Wireless Internet Service Providers)
are pushing Wi-Fi to the limits to reach and cover MANs.

IV. MAJOR CHALLENGES IN PROVIDING CONNECTIVITY IN RURAL AND ISOLATED AREA

1. The major challenge in providing connectivity in rural and isolated area is cost. Any system/technology for providing connectivity in rural and isolated areas, will sustain only if it is affordable. Typically town places have Fiber point-of-presence(PoP) and are separated by a distance of 30-40 Kms. Town places are surrounded by small villages with distance between them around 3-4 Kms.

2. Another challenge in providing connectivity in rural and isolated area is information security. Due to sparsely populated area there are chances of theft of tempering of data which may give the owner of data a negative impact.

V. WIMAX PRODUCTS ASSOCIATED WITH THE BROADBAND ACCESS DEPLOYMENT

WiMAX is a worldwide certification addressing interoperability across IEEE 802.16 standards-based products. The IEEE 802.16 standard with specific revisions addresses two usage models:
• Fixed
• Portable

1 Fixed
The IEEE 802.16-2004 standard (which revises and replaces IEEE 802.16a and 802.16REVd versions) is designed for fixed-access usage models. This standard may be referred to as “fixed wireless” because it uses a mounted antenna at the subscriber’s site. The antenna is mounted to a roof or mast, similar to a satellite television dish. IEEE 802.16-2004 also addresses indoor installations, in which case it may not be as robust as in outdoor installations.

The 802.16-2004 standards is a wireless solution for fixed broadband Internet access that provides an interoperable, carrier-class solution for the last mile. The Intel WiMAX solution for fixed access operates in the licensed 2.5-GHz, 3.5-GHz and license-exempt 5.8-GHz bands. This technology provides a wireless alternative to the cable modem, digital subscriber lines of any type (xDSL), transmit/exchange (Tx/Ex) circuits and optical carrier level (OC-x) circuits.

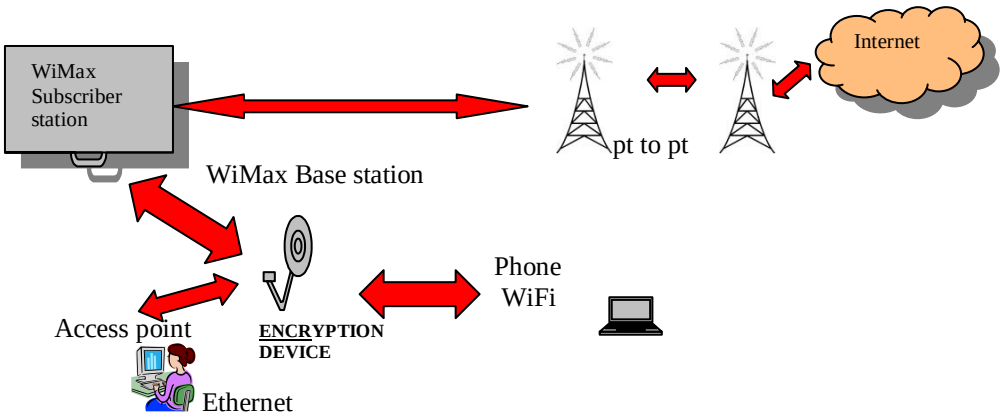

Fig 1 : WiMax Network Topology

2. Portable

The IEEE 802.16e standard is an amendment to the 802.16-2004 base specification and targets the mobile market by adding portability and the ability for mobile clients with IEEE 802.16e adapters to connect directly to the WiMAX network to the standard. The 802.16e standard is expected to be ratified in early 2005.

The 802.16e standard uses Orthogonal Frequency Division Multiple Access (OFDMA), which is similar to OFDM in that it divides the carriers into multiple sub carriers. OFDMA, however, goes a step further by then grouping multiple subcarriers into sub-channels. A single client or subscriber station might transmit using all of the sub-channels within the carrier space, or multiple clients might transmit with each using a portion of the total number of sub-channels simultaneously. The IEEE 802.16-2004 standard improves last-mile delivery in several key aspects:

• Multi-path interference
• Delay spread
• Robustness

Multi-path interference and delay spread improve performance in situations where there is not a direct line-of-sight path between the base station and the subscriber station. The emerging 802.16-2004 media-access control (MAC) is optimized for long-distance links because it is designed to tolerate longer delays and delay variations. The 802.16 specification accommodates MAC management messages that allow the base station to query the subscriber station, but there is a certain amount of time delay. WiMAX equipment operating in license-exempt frequency bands will use time-division duplexing (TDD); equipment operating in licensed frequency bands will use either TDD or frequency-division duplexing (FDD). Intel WiMAX products will support TDD and half-duplex FDD operation. The IEEE 802.16-2004 standard uses OFDM for optimization of wireless data services. Systems based on the emerging IEEE 802.16-2004 standards are the only standardized OFDM based, wireless metropolitan area networks (WMAN) platforms. In the case of 802.16-2004, the OFDM signal is divided into 256 carriers instead of 64 as with the 802.11 standard. As previously stated, the larger number of subcarriers over the same band results in narrower subcarriers, which is equivalent to larger symbol periods. The same percentage of guard time or cyclic prefix (CP) provides larger absolute values in time for larger delay spread and multi-path immunity. The 802.11 standard provides one-fourth of the OFDM options for CP than does the 802.16-2004 standard, which provides 1/32, 1/16, 1/8 and 1/4, where each can be optimally set.

The physical layers (PHYs) for both 802.11 and 802.16-2004 are designed to tolerate delay spread. Because the 802.11 standard was designed for 100 meters, it can tolerate only about 900 nanoseconds of delay spread. The 802.16-2004 standard tolerates up to 10 microseconds of delay spread more than 1000 times than in the 802.11 standard.

VI. Ethernet Encryption Overview

In a globally-interconnected world, governments, businesses and individuals exchange billions of online messages and transmit millions of megabytes of data every day…much of it high value, some of it high risk. The hundreds of millions of kilometres of optical fibre cable crossing the globe give us the freedom to communicate instantly with anyone, virtually anywhere. But this enabling technology is a double-edged sword: the benefits of instant communication through voice, video and data must be weighed against the time and cost to ensure the confidentiality of personally identifiable information (PII), corporate IP and secret government information travelling anywhere along the millions of kilometres of network fibre. As the global economic crisis continues, there are widespread reports of increased activity by cyber criminals and electronic hackers who can steal millions of dollars in seconds, but who also trade in user names, passwords and corporate intelligence captured from data hacked during transmission. The widely-held belief that optical fibre is inherently secure has been debunked – over two years ago It is demonstrated that a readily available device that clamps onto the fibre bending it sufficiently to extract a signal, could be used to capture information without damaging the fibre or disrupting communications. Encryption is the solution to totally securing optical fibre and other data networks. Encryption technology, proved over more than a decade, is now in use by governments, military, law enforcement and corporate networks worldwide. It employs 64, 128, 256 bit algorithms and high speed public and private key exchange technology to verify and then secure everything transmitted over the information network. In the event that

a hacker intercepts the communications, all information is encrypted and unusable, therefore protecting against threats to corporate productivity or reputation and individual loss.

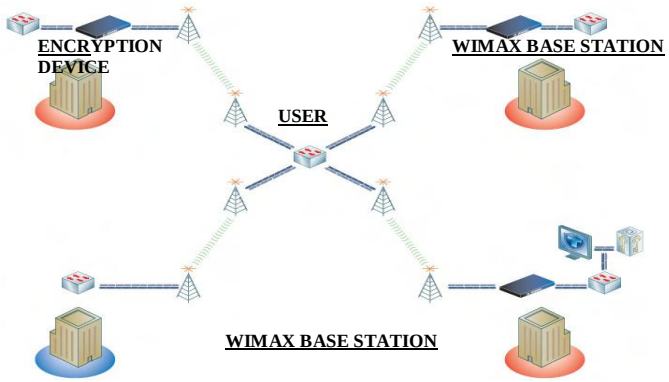

Fig 2 : WiMax Network Topology Encyption Solution to network protects the data between the Important Department sites, while all other traffic remains in the clear.

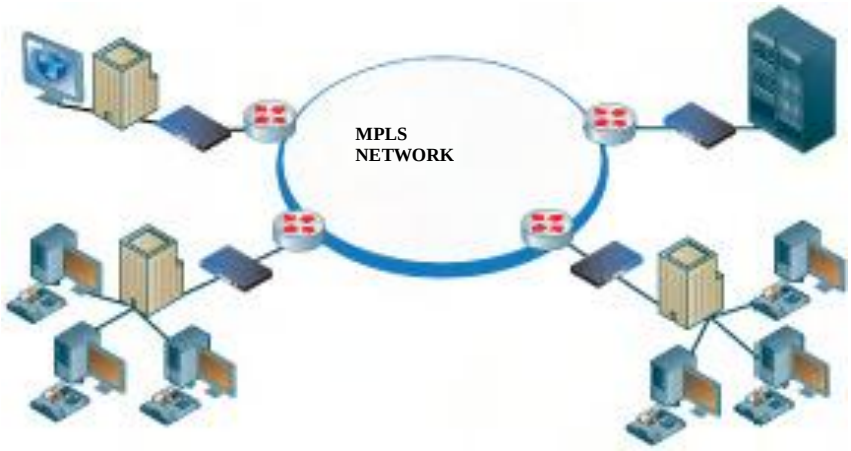

Fig 2 :Defined Security policies and encryption keys are dynamically distributed to all encryptors.

VII. Summery and Conclusion

This paper explores a viable business model for the deployment of a Wi-Fi access network that uses WiMAX backhaul systems to lower infrastructure costs. Use of Encryption device increased the security of data and made the many systems operational. In the short run, it is beneficial both for service providers and users, until mobile versions of WiMAX systems (IEEE 802.16e) become a reality. Since the backbone infrastructure is WiMAX, it should be easier to migrate to mobile WiMAX access in the future, by using the same infrastructure. The main advantage of this hybrid model (using both WiMAX and encryption) is that it turns the entire geographic area into a wireless hot zone in a very short period of time. Wi-Fi APs cost very little and can be easily mounted on lamp posts or stop lights at a significant cost than leasing tall towers to mount the BS and antennas. The advantage of using Wi-Fi as a last mile solution is that, despite the higher density of Wi-Fi APs, it is still more economical compared to alternative infrastructure costs. This is due to the fact that the capital costs of APs are much lower and that additional investment in APs should not impact the net profit. The main economic advantage of WiMAX infrastructure mesh architecture is its low backhaul cost, due to traffic aggregation. However, additional research and standardization work is needed to bring the full benefits of mesh architecture or infrastructure mesh to 802.16/WiMAX. A profitable business strategy for a WISP would be to serve a wide variety of customers with the same infrastructure. Another main advantage of this model is that residential and business users can access an on demand (on a daily or hourly basis) service along with their option of traditional monthly subscription. The result is one-time CapEx that can be leveraged across different customer bases, making this an optimal solution for broadband deployment. It was found that a higher operating profit can be achieved even with a smaller number of subscribers in the initial stages of the deployment. For a larger intake, the business case looks significantly better. Therefore, with lower backhaul costs and zero dollars on CPE subsidies and truck rolls, the combination of Wi-Fi with WiMAX to provide both voice and data services, represents an attractive solution for deploying city wide wireless broadband access.

References

[1] WiMAX Forum, www.wimaxforum.org
[2] http://www.telecomindiaonline.com
[3] www.intel.com

[4] WiFiRe: Medium Access Layer (MAC) and Physical Layer (PHY) Speci¯cation Center of Excellence for Wireless Technology (CEWiT)
[5] S, Iyer et al. Broadband wireless for rural areas - wifire: Medium access control (mac) and physical layer (phy) specifications Centre for Excellence in Wireless Technolgies, IIT Madras, Chennai, India, 2006.
[6] http://en.wikipedia.org/wiki/Information_ security
[7] http://www.certesnetworks.com/

