

An Overview of Security Issues on a Converged WiFi and WiMAX Network

Tonderai Muchenje*, Hippolyte Muyingi
Telkom Centre of Excellence (CoE) in Developmental
E-Commerce.
Computer Science Department
University of Fort Hare, Alice, P.Bag X1314, 5700
South Africa
Cell:+27720887508,+27(40) 602 2464
(tmuchenje3@gmail.com, hnmuyingi@ufh.ac.za)

Abstract- Wireless networking has offered an alternative solution to the problem of information access in remote inaccessible areas where wired networks are not cost-effective. They have changed the way people communicate and share information by eliminating worrisome factors of distance and location. But there are still unsolved issues that prevent wide spread adoption of broadband wireless communication. This paper provides an overview of security issues on a converged WiFi and WiMAX networks. It also seeks to provide a comparative overview of other alternative wireless convergence scenarios which can be used depending on suitability, applications requirement capabilities, and availability of coverage. This research was conducted to investigate and evaluate the wireless technologies security and also to analyze how the convergence of WiFi and WiMAX address confidentiality, integrity and availability (CIA) in a rural setting, Dwesa/Cwebe that was selected as the test bed for our project. Our findings reveal that inherent WiFi and WiMAX networks protocols could not achieve a robust and seamless converged wireless network.

Index Terms — authentication, availability, confidentiality, convergence, integrity, network performance, rural environment, security, Wi-Fi, WiMAX

1. INTRODUCTION

Wireless networks can be regarded as an important technological development in this modern age. Many individuals, companies and institutions of research have benefited from them, by increasing productivity and sharing information without undue concern about location and position, as long as users are within the wireless signal range; and they are considered by many as the way forward for rural Africa connectivity and its digital bridge to the

world. Though the wireless network has passed recognized benefits on its adopters, its security issues still remains an open question. Until the wireless network security has reached the equivalent security level provided by the wired networks, IT managers and Chief Information Officers will not continue adopting wireless networks as an alternative solution.

The 802.11 networks standards came to existence in 1999, with the 802.11b being the most deployed. The 802.11 wireless standards suffered some security flaws whereby their standard security method – the Wired Equivalent Protocol (WEP) mechanism – was cracked [1, 2]. Since concerns regarding security attacks on wireless networks are becoming costly, so there is a need for a high level of knowledge and skill to provide a robust network solution. The Institute of Electrical and Electronics Engineers (IEEE), Internet Engineers Task Force (IETF) and the Wireless Fidelity (WiFi) Alliance have come up with some interim and approved standard mechanisms to secure the 802.11 wireless networks, while 802.16 and the WiMAX Forum are looking to Worldwide Interoperability for Microwave Access (WiMAX) broadband wireless network specifications. These two bodies are in their development trying to address the short coming experienced in the 802.11 wireless networks. The WiMAX has many capabilities ranging from backhauling WiFi, cellular connectivity, rural connectivity, residential and enterprise mobile support connections [3].

This paper presents an overview of the security issues in converged WiFi and WiMAX wireless networks. The paper also outlines a comparison of possible convergences scenarios, and evaluates them on their capability in providing suitable and cost-effective solution to a rural setting. For our investigation and experimental purposes, we chose Dwesa\Cwebe as example of a rural setting in the Eastern Cape coast region of South Africa. The aim of our investigation is to come up with the best practices in

securing rurally deployed converged wireless networks for the fore-mentioned rural community.

2. CHALLENGES IN WIRELESS NETWORKS

As much as the wireless networks have brought about major development in the way the information is shared between individual-to-individual, individual-to-business and business-to-business scenarios, they still face challenges, which are yet to be solved. Security is among the major concerns as illustrated in the Figure 1.

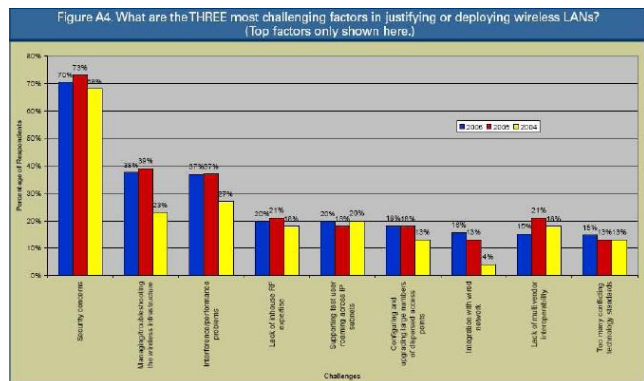


Figure 1: WiFi Challenges according to market survey [2004] [23]

We define security as protection of data being transmitted over a converged wireless networks. It is important to understand the full range of problems that security systems need to address. These needs are confidentiality, integrity and authentication (CIA), and can be defined as follows:

Confidentiality

Allowing only that the intended legitimate recipients to read encrypted messages (information).

Integrity

Can be referred to as ensuring that another party has not altered messages after it has been sent.

Authentication

This is making sure that parties sending messages or receiving messages, are who they say they are, and have the right to undertake such actions.

On wired networks it has been exhaustively researched and there are many mechanisms available to provide confidentiality, integrity and authentication of information (CIA). Virtual Private Networks (VPNs), Internet Protocol Security (IPSec), Intrusion Detection Systems (IDS) and firewalls are just examples among various security mechanisms that has been proposed to address security issues in wired networks.

The major problem when securing the wireless signal is in its mode of transmission [4]. The wireless signal is transmitted through electromagnetic waves, which cannot be physically contained. Being communicated through the air makes them easy to intercept by anyone with the right transceiver equipment.

The IEEE had ratified the 802.11 wireless protocols with basic methods to secure such a network, namely disabling SSID, Media Access Control (MAC) address filtering and the WEP mechanism [5]. These were mechanisms thought to provide the CIA elements on the wireless networks. Advances in technology and software development later compromised these mechanisms leaving the network vulnerable to malicious attacks; even recent mechanisms still exhibit weak protection of management messages [6]. WiMAX builds on the experience of security problems of 802.11 wireless networks. It was developed to solve most of the wireless LAN shortcomings especially security, and also quality of service, high-speed data rates and long distance connectivity coverage [3]. WiMAX, as a new technology on the market still undergoing experimentation, seems not to have fully solved the security flaws of wireless LAN. WiMAX still lacks mutual authentication, and is susceptible to replay attacks, spoofing of MAC address of the Subscriber Station (SS) and the PMK authorization vulnerabilities. Ever since the initial release of WiMAX in early 2004 (802.16d), the IEEE and the WiMAX Forum have been improving the standard incorporating some other capabilities to enhance security and mobility [7]. Another major drawback in the deployment of WiMAX for connectivity is the large initial expense involved.

Addition to that, there is also a need to consider the security protocols and mechanisms within the context of the applications in a converged wireless network. Especially in a rural setting, where resources are at a premium, the impact of security protocols needs to be weighed against the requirements of the users. There one needs to consider end user needs in terms of lack of qualified network management, limited bandwidth, and specialized applications.

Confidentiality, in wireless networks is a fundamental concern for a secured transmission. The intended recipient should only receive the information transmitted. The message authentication provides integrity to both the message sender and receiver. The wireless link should always be available and not be susceptible to malicious attacks, which rob the end-user of availability (denial of service attacks) [7].

There are many attacks, which can be launched to compromise authentication mechanisms or protocols. Two common attacks that are especially effective against wireless networks are the message replay attack and the man in the middle attack. The message replay attack acts principally on the authentication and authentication key formation protocols, while the man in the middle (MiTM) attack usually occurs when the security mechanism implemented does not provide mutual authentication. Other attacks known to occur include session hijacking, reflection

attacks and other attacks due to misuse of cryptographic services. These security issues must be addressed for wireless network to reach equivalent security provided by wired networks.

3. DEFINITION OF WIRELESS CONVERGENCE

The term convergence within the context of this paper refers to the combination of the two similar wireless networks, namely Wi-Fi (802.11) and WiMAX (802.16). The emergence of wireless networks is thought to be a crucial tool in “bridging the digital divide” [8]. It enables many more people to become connected to online resources without the worry and cost of a wired connection. While wireless technologies had been broadly adopted by homes, organizations and research institutions in developed countries, the idea of extending existing wireless technologies to offer a cost effective solution to the rural communities arose. Wi-Fi was the first commonly accepted wireless protocol to add flexibility and mobility to the Ethernet network thereby opening a whole set of new use cases for Ethernet technology [9]. Although Wi-Fi extended the capabilities of Ethernet; it did not solve networking issues concerning security, high-speed access, manageability, and wide area coverage. In 2004 the IEEE 802.16 wireless standard was ratified to address the problems, which had been identified in Wi-Fi technology. Besides improved security and parallel communications, 802.16 should operate in a 50km line of site radius. The 802.16 standard is seen mainly as a broadband wireless technology, which can support high-speed transmission of data, voice and video. To solve the rural connectivity in a cost effective manner, the University of Fort Hare conceptualized a convergence of the two wireless technologies at Dwesa/Cwebe rural setting. The IEEE 802.16 wireless standards provides for backhaul rural connectivity while Wi-Fi is the end user access technology, owing to the widespread adoption of this technology in cheap end-user devices. To date there is no 802.16 wireless standard-enable end user devices with broad adoption on the market. The converged wireless networks are thought to offer a number of benefits [10], which are:

- Significantly reduced costs
- Effective communication
- Productivity Enhancements
- Simplicity
- Cost control
- Flexibility and scalability
- Increased Security

Some drawback of the convergence may be the weak level of reliability of data, complexity of maintenance, low service and infrastructure upgradeability to suit rapid change in technology.

4. ALTERNATIVE WIRELESS CONVERGENCE

This section provides a comparative discussion of other convergence scenarios and their unsuitability in achieving wireless convergence in providing services to mobile users and wireless Internet connectivity, without focusing on related security issues.

4.1 WiFi vs. Bluetooth

Bluetooth and WiFi-based devices use the same 2.4GHz unlicensed radio spectrum. Bluetooth is defined by IEEE 802.15 standard. There are important communication technologies that provide different functionalities to different indoor wireless applications [11]. Bluetooth is a short range (~10metres) a wireless technology suitable for data file from one device to another in a close proximity. The Bluetooth exist in various devices such as phones, printers, personal digital assistance and modems and computers. Due to low bandwidth and coverage of Bluetooth, it is not effective to set up a network for remote applications. Therefore WiFi technology’s is a better networking consideration for accessing files [12]. The 16 bit Personal Identification Number (PIN) used for Bluetooth authentication and data encryption is not robust compared to the 80211i security enhanced protocol used in WiFi [11, 13].

4.2 WiMAX vs. UTMS

Though the mobile technologies provide ability for users to use it as an access technology, its data rates speeds do not give competition to WiMAX. Theoretically the mobile technologies have data speeds from 115kbps for General Packet Radio Service (GPRS), 384 Kbps for Universal Mobile Telecommunications System (UTMS) and 14.4Mbps for High-Speed Downlink Packet Access (HSPDA) while WiMAX offer high data speeds of up to 70Mbps for coverage of 50km. As much as the HSPDA can provide a much faster theoretical maximum data rate of 14.4Mbps with a kilometer making it only suitable for short distance access technology [14]. Similarly to other mobile technologies WiMAX have the same capabilities to transmit data and voice. The choice of using mobile technologies in transmitting voice is more expensive with VoIP/WiMAX as compared to WCDMA/HSDPA. The HSDPA uses a users’ Subscriber Identification Module (SIM) card for authentication, while the WiMAX supports the strong modern cryptographic algorithms which is more robust to protect secret data transmissions [15]. The overall cost for the WiMAX equipment is much lower as compared to the UMTS, especially due to less usage of high tower structures. The main advantage of using the UTMS cellular system is that, its infrastructure for 3rd Generation mobile network (3G), HSPDA, GPRS and Evolutionarily Distinct and Globally Endangered (EDGE) is already there while the WiMAX requires a new infrastructure setup for it to operate. More people prefer UTMS for mobile communication compared to WiMAX since it can be easily available. But the emerging of WiMAX-enable end user

devices and the on going wide spread trials and commercial deployments of WiMAX should favor its availability.

4.3 WiFi vs. UTMS

Many of the above features on WiMAX vs. UTMS apply to WiFi vs. UTMS; with the advantage of both offering mobility to end users. The low coverage of WiFi limits its application around hotspots areas, but it enables user-friendly interface to be used as IP-based broadband access devices. In fact WiFi and UTMS work rather better as complementary access technology, though the advent of Gigabit WLAN (WIGWAM project) [23] might completely favor WiFi in the near future.

4.4 WiFi vs. WiMAX

These two wireless technologies have common components in their operations with a major difference in the communication range. There is a need for many WiFi access point in order to cover the same distance covered by one WiMAX base station. Hence it is costly to deploy WiFi for greater distances. WiFi is an access technology suitable for indoor use due to its short ranges as an extension to LAN technology while the WiMAX was designed for long distance, backhauling and optimized for Metropolitan Area Network (MAN). As much as the WiFi has an advantage of providing end user access capabilities, it only support a limited number of users (not more than 12 per base station) whereas the WiMAX base station can support an average of about five hundred users. The WiMAX base station has a scheduling algorithm (First-In First-Out) which allocates a variable channel for each subscriber station to minimize the congestion and degrading throughput other than the random queue assignment based on MAC address in WiFi where as. The WiMAX uses a licensed and unlicensed spectrum where as the WiFi uses unlicensed spectrum with a limited channel bandwidth of 20 MHz. Due to the fact that WiMAX can support high bandwidth, low cost of ownership and provides backhaul capabilities it therefore can be considered as the future broadband access technology to bridge the 'digital divide'. The WiMAX is more reliable and have better QoS as it was designed with security as a major priority since the frailness of WiFi [16]. Despite the similarity in equipment cost, WiMAX technology requires a costly infrastructure while the WiFi can be easily install using low cost access points. In conclusion, WiFi has been adopted as an extension for Ethernet some years ago making it a mature technology as compared to the WiMAX which is currently license assignments and infrastructure deployment.

5. 802.11 WIRELESS LAN (WLAN)

The first 802.11 wireless network standards were developed in 1997 as an extension to the Local Area Network (LAN) [1]. It was known as wireless Ethernet that only supported a maximum speed up to 2 Mbps. Frequency

Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) were the modulation techniques supported.

There are three well known 802.11 wireless family standard widely used today.

5.1 802.11 wireless standard family

802.11b

The 802.11b is a refined standard for the original 802.11 and was successful due to its high data rates. 802.11b is the most widely deployed wireless network within the 802.11 wireless families [1, 2]. 802.11b supports data rates of up to 11Mbps and uses the DSSS modulation technique that is more reliable than the FHSS.

802.11a

The IEEE 802.11a operates in the 5 GHz band with a maximum data rate of 54Mbps [17]. This standard was ratified almost at the same time as was 802.11b, but its hardware was only made available in 2001 due to lack of availability of the frequency band components [18, 19,20]. The major disadvantage in deploying 802.11a with the other 802.11 standards b and g, is that they cannot co-exist, as they operate on different frequency bands. 802.11b/g operates on the 2.4 GHz spectrum [18]. There are some wireless card and access points which are compatible to all the three standards thereby supporting the 2.4GHz and 5GHz frequencies e.g. Orinoco 11a/b/g [21].

802.11g

The IEEE 802.11g wireless standard also operates on the 2.4 GHz band and has similar range and characteristics as the 802.11b. It has a raw data rate of 54Mbps. The 802.11g has backward compatibility with 802.11b and differs only on the modulation technique; it uses Orthogonal Frequency Division Multiplexing (OFDM). This then makes the 802.11b devices not able to pick the signal from the 802.11g devices [19]. **Figure 2** illustrates the development of IEEE 802.11 standards.

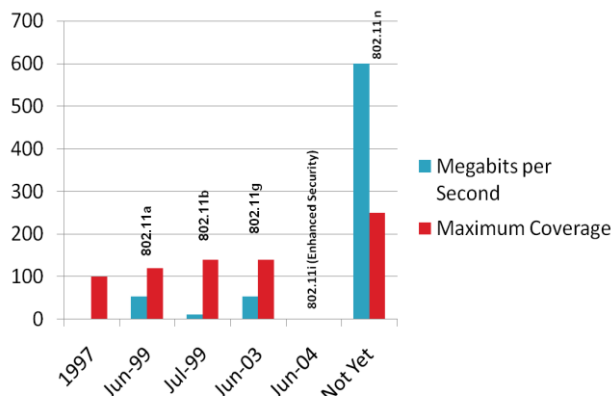


Figure 2: The 802.11 Family Standard evolution

5.2 Security issues on WLAN

Security is considered to be one of the biggest challenges when deploying a wireless network. Despite the introduction of the more effective 802.11i security standard, existing WLANs are not being secured properly [22]. According to a survey undertaken in Johannesburg, South Africa, in July 2006 only two of two hundred and seventy two networks used 802.11i mechanism in securing their wireless networks [23].

In accordance with the IEEE and the Wi-Fi Alliance there are a number of recommendations and best practices that were put forward to assure security of WLAN. WEP was the first protocol that was developed to provide confidentiality, integrity and authentication for data in transmission. The aims of WEP were not long lived due to a number of vulnerabilities [24] thereby letting unauthorized people to gain access to the wireless network. The WEP mechanism has not been considered to be a solution for securing WLAN ever since it was compromised. Wi-Fi Protected Access (WPA) was then introduced in 2003 as an interim solution to WEP. WPA has two implementation flavors, WPA-PSK which is similar to the WEP with better authentication and encryption and WPA Enterprise mode, which uses the 802.1X protocol, RADIUS server as a back-end authentication protocol and Temporal Key Integrity Protocol (TKIP). A Message Integrity Check (MIC) is used to monitor information tampering by a hacker [2]. **Table 1** illustrates a comparison of WPA technologies.

WPA Personal Mode	WPA2 Personal Mode
Authentication: PSK	Authentication: PSK
Encryption: TKIP/MIC	Encryption: AES-CCM
WPA Enterprise Mode	WPA2 Enterprise Mode
Authentication: 802.1X/EAP	Authentication: 802.1X/EAP
Encryption: TKIP/MIC	Encryption: AES-CCM

Table 1: Protocols of the WPA and WPA2 technologies

WPA was developed in 2003 as a short-term solution in fixing the security problem awaiting the ratification of the 802.11i in 2004. The 802.11i security standard for wireless local networks is similar to the WPA though it was designed with some improvements in terms of encryption mechanism. The 802.11i architecture contains the following components: 802.1X for authentication [23] (entailing the use of EAP and an authentication server), Robust Security Network (RSN) for keeping track of associations, and AES-based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to provide confidentiality, integrity and origin

authentication [2]. It also uses the same 802.1X port-access control protocol for better key management and a four way hand shake. This means that centralized security complements proven session key exchange technology in the latest standard.

Although there are specified mechanisms that have been postulated to be used in the securing of wireless LANs, organizations are still trusting virtual private networks (VPN) and firewalls to protect their highly sensitive data [25]. VPN may seem to be an attractive solution in securing wireless networks but there are a number of issues, which have to be considered before implementing the solution. When the organization has a VPN in place, it becomes easy and cost effective to extend it to wireless networks; though the extra overhead due by encryption needs to be evaluated against the required QoS. There are two most common ways in which VPN can be implemented namely; IPSec and SSL

6. THE 802.16 WIRELESS NETWORK STANDARDS

WiMAX is the industry name for the 802.16 set of standards. It is an emerging technology that delivers carrier –class, high speed, wireless broadband at a much lower cost than the cellular services while covering large distances than Wi-Fi. It has been designed to be a cost-effective way to deliver broadband over a wide area. WiMAX has standardized broadband-wireless-access technology and is intended to handle high-quality voice, data and video services while offering a high quality of service (QoS). WiMAX is classified as in the Wireless Metropolitan Area Network (WMAN) that operates in between 10 and 66 GHz Line of Sight and 2-11GHz Non Line of Sight [3]. **Figure 3** below shows the frequency band other 802.16 standards define.

	IEEE802.16	IEEE 802.16 Rev'd	IEEE 802.16e
Completed	Dec 2001	May 2004	Est. Mid-2005
Spectrum	10-66GHz	2-11GHz	2-6 GHz
Application	Backhaul	Wireless DSL and Backhaul	Mobile Internet
Channel Condition	Line of Sight only	Non-Line of Sight	Non-Line of Sight
Bit Rate	32-134 Mbps at 28 MHz Channelization	Up to 75Mbps at 20 MHz Channelization	Up to 16Mbps at 5-MHz Channelization
Modulation	QPSK, 16 QAM and 64 QAM	OFDM 256, OFDMA 2048 QPSK, 16 QAM, 64 QAM	Same as 802.16d, Scalable OFDMA
Channel Bandwidth	20,25 and 28 MHz	Selectable Channel Bandwidth between 1.5 and 20 MHz	Same as 802.16d

Figure 3: The evolution of IEEE 802.16 standard [3]

IEEE 802.16 was developed after the security failures that weighted down the progress of IEEE 802.11 networks. The IEEE 802.16 Working Group in their design for a robust mechanism incorporated DOCSIS a pre-existing standard to solve last mile problems for cables. Recognizing the importance of security, the 802.16 working groups are busy designing several mechanisms and protocols to protect the service provider from theft of service, and to protect the customer from unauthorized information disclosure [26].

7. WIMAX SECURITY ISSUES

In this section an overview of the security issues in WiMAX is presented. The overview will provide how WiMAX tends to address confidentiality, integrity and authentication.

7.1 Authentication

Authentication is a very important process which has been present to restrict network users from utilizing the services which are only allowed. From the 802.16 MAC protocol stack, physical layer is below the security sub-layer where a secure transport communication process exists. This means then the physical layer communication is sent on clear text which makes it vulnerable to attacks such as jamming of the radio spectrum, water-tourte attack and scrambling [27,28]. These attacks are made possible since there are no sufficient techniques available to protect physical layer. Ever since the development of WiMAX, mutual authentication has been a major problem. The Base Station (BS) is the only entity which authenticates the Subscriber station, leaving the Privacy and Key Management (PKM) vulnerable to forgery or replay attacks. The only way this problem can be managed is to include an authentication mechanism which provides mutual authentication. The IEEE 802.16 Working Group solved the problem with an amendment added to the current 802.16e to support Extensible Authentication Protocol to WiMAX networks for more details on EAP [28].

7.2 Confidentiality

In WiMAX scenario the first management messages are not encrypted. This can provide vital security cipher suite information to a person intending to get confidential user information. An attacker can passively (eavesdropping user traffic) listen to the communication between the BS and the SS. The PKM protocol uses the Temporal Encryption Key (TEK) sequence space to encrypt messages. The use of the sequence number to differentiate messages is subject to replay attacks. Since the early version of 802.16 uses the DES in CBC for data encryption, it can only provide a robust security up to 2^{32} of the 64 blocks [27,28], making the security diminish as the data rate goes

over 6.36Mbps. The introduction of the 802.16e standard tried to solve the data encryption and key management failure in the WiMAX initial standards. The 802.16e data encryption incorporates the AES-CCM which could encrypt the payload of the MAC PDUs. The advantage of using the AES-CCM compared to DES-CBC is in its encryption of the authenticated data and protection of the Generic MAC header (GMH). The 802.16e designers thought of using the AES-CCM for a based on a wide consideration such as co-exists with the 802.11i security standard [27].

7.3 Integrity

The initial 802.16 standard did not include the data traffic protection mechanism. This meant that forgery and data modification attacks were prevalent. Hence the 802.16 introduced a CBC-MAC as a component of the AES-CCM for protecting the integrity of the payload of the MAC PDUs [28].

8. DWESA/CWEBE COMMUNITY SETTING

This research paper is providing background information to the ongoing investigation of a novel generation of a multipurpose communication platform at Dwesa and Cwebe, two rural districts located on the Eastern Coastline of the Transkei, within the Eastern Cape Province of South Africa. Dwesa (32° 17' 60" S, 28° 49' 60" E) is on the southern side of Mbashe River, while the Cwebe (32° 13' 0" S, 28° 55' 0" E) is on the northern side.

Figure 4 shows a section of the network currently in place at the Dwesa/Cwebe site. The rural area is isolated from the rest of the world not only by its remote location, but also through the "digital divide". The University of Fort Hare and Rhodes University, sponsored by the Telkom Centre of Excellence (CoE) programme are jointly deploying a multipurpose Information Communication Technology (ICT) infrastructure intended to help people in the area to gain interactive and participative access to products and services, as well as acquiring important information technology knowledge and skills, and sharing local indigenous knowledge [25]. Numerous projects are underway to fulfill these goals and to place the total ownership of the projects in the hands of the community. Service contents are localized culturally as well as linguistically.

The IP converged wired and wireless network itself was designed and deployed as shown in Figure 4 [29]. Our research on how security issues are managed in such a converged network.

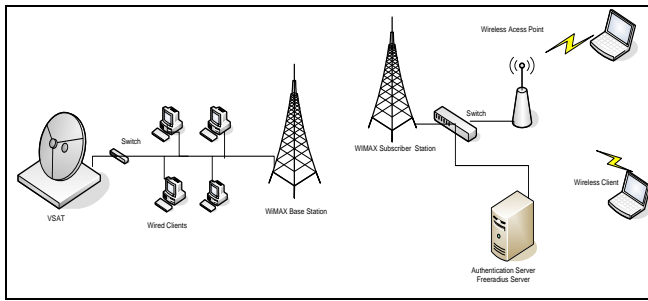


Figure 4: IP Converged wired and wireless network in Dzwesa /Cwebe, using Alvarion BreezeMAX 3500 WiMAX system [30]

9. SECURITY CONSIDERATIONS

The applications under trials and deployment at Dzwesa/Cwebe telecommunication platform test will provide the following services:

- VoIP (as the area has poor coverage from cellular networks like Vodacom, MTN and few Telkom land lines)
- An e-commerce platform with shopping mall, e-government, e-learning, e-health, e-judiciary
- An African knowledge ontology base
- Internet services: email, SMS, file sharing etc.
- New approach on billing services for rural Internet.

Our first step was thus securing each segment of the network using the inherent mechanisms considering the performance cost and effectiveness.

The major security consideration was on the interactions of the wireless networks devices taking the vulnerabilities and threat impact through impact analysis; e.g. shared resources between the wireless networks link and users such as RADIUS servers. We also considered network independent mechanisms such as IPSec or VPN.

Finally we need to optimize the security on the network according to the application requirements.

10. INITIAL FINDINGS

The security mechanisms of each of the wireless technologies that comprise the network have already been discussed. As we have seen, the weakest link of the chain can be the WLAN segment. WLAN should be implemented using the 802.11i standard. This will probably not be possible right away in this project because of hardware incapacities of the Cisco Aironet 1100 AP to support 802.11i protocol standard. Another solution may have to be implemented which might be a WPA Enterprise mode using the TKIP for encryption.

We expect that IPSec and VPN should not be implemented, as they will impact on the cost of implementation and performance [30, 31]. The only main advantage of using IPSec /VPN is that they can be implemented independently

of a particular network, so they will be suitable for some applications like the e-commerce platform. However they are not suited to other applications like accessing the Internet [36].

According to WiMAX security findings, the initial 802.16d though a provided high-data speeds and a larger wireless coverage as compared to the WiFi technology, it had some security flaws which needed addressing. This initial 802.16d had a weaker data encryption mechanism, 3DES which later was replaced by AES-CCM in the mobile WiMAX (802.16e). The authentication and PKM enhanced access control by introducing PKM-EAP.

As the security mechanisms of these two wireless networks still could not provide robust and seamless security, therefore an access concentrator implementing Point-to-Point Protocol tunneling with MPPE security infrastructure was recommended. Currently, there are test underway in evaluating Point-to-Point Protocol over Ethernet (PPPoE) running 128bit Microsoft Point-to-Point Encryption (MPPE) tunneling over this converged wireless network [32].

We expect that the security within the WAN will impose insignificant bandwidth penalties, so that we will be able to provide basic security for all applications on the network, even though this may not be required for the application.

Further we have found that the industry standards are moving very quickly so that, hardware supported converged WiMAX and WiFi networks will probably available for end user devices or at least relays in the near future. In this case, the security best practices we will highlight must be built-in [33]

11. CONCLUSION

In conclusion, we believe that the converged wireless network is an ideal choice for building inexpensive IP based communication networks that carry data, voice and video. Furthermore, the convergence of Wi-Fi and WiMAX wireless technologies may offer a solution to high-speed rural Internet connectivity. It may even provide ICTs a cost effective way of bridging the digital divide in the near future, by mixing the cheapest components for Wide-Area and Local-Area connectivity. Although these wireless technologies offer tremendous benefits to individuals, businesses, educational institutions and rural communities Internet connectivity, security is still a major concern. Confidentiality, integrity and authentication must be achieved on the converged network. From the initial findings the inherent security mechanisms in WiFi and WiMAX still could not manage to offer a robust network solution in a converged infrastructure. Therefore, a testing of the PPPoE running a 128bit MPPE is under investigation to evaluate its effectiveness and effects on network performance. In future after the final implementation and testing of the proposed security mechanisms, a best practice for deploying a converged wireless network will be presented.

12. ACKNOWLEDGMENTS

The authors wish to acknowledge invaluable contribution from Fort Hare University Telkom Centre of Excellence, CoE, namely. The principal author would like to thank Ronald Wertlen, Director at e-KhayaICT, for the editing, relevant advice and information, and the Zimbabwean Government through the Presidential Scholarship for the sponsorship of my studies.

3. REFERENCES

1. Black Box (2005),, *802.11: Wireless Networking*, White Paper White Paper, http://www.blackbox.com/Tech_Support/White-Papers/802.11-Wireless-Networking2.pdf
2. Cam-Winget.N, Housley. R, Wanger. D and Walker.J, *Security Flaws: In 802.11 Data Link Protocols*, *Communication of The ACM*, May 2003/ Vol .46.No 5
3. Westech Communication Inc (2005), *Can WiMAX Address Your Application*, White Paper, accessed on 3 October 2006, www.wimaxforum.org/technology/downloads/Can_WiMAX_Address_Your_Applications_final.pdf,
4. Griffin (2005) "Creating a Secure Network for Your Business", "White-Paper", accessed on 24 June 2006, <http://www.aometrosystems.com/whitepaper.htm>
5. King J.S ()*An IEEE 802.11 Wireless LAN Security White Paper* www.wifi-plus.com/images/Whitepaper-8.pdf, Retrieved on the 11 April 2007
6. Page. K. H. Kismet. <http://www.kismetwireless.net/>, 2006. Retrieved 18 December 2006.
7. Xu. S., Matthews, M., Huang, C (2006)., *Security Issues in the Privacy and Key Management Protocols of the IEEE 802.16*, retrieved on 1st May 2006 from <http://www.cse.sc.edu/huangct/acmse06cr.pdf>
8. Best M.L., Maclay C.M., *Community Internet Access in Rural Areas: Solving the Economic Sustainability Puzzle*, Ch. 8 in *The Global Competitiveness Report 2001-2002*, WORLD ECONOMIC FORUM
9. Dymond .A, Oestmann. S, *A Rural ICT Toolkit for Africa, infoDev Program of the World Bank*, 2003, <http://www.infodev.org/projects/telecommunications/351africa/RuralICT/Toolkit.pdf>
10. Computer Science Corporation,(2005) *Converged Networks*, article , Retrieved on the 2 January 2007
11. Groupe Ingenico (2007): *WiFi vs. Bluetooth Two Outstanding Radio Technologies for Dedicated Payment Application*, White paper, accessed 23 April 2007, http://www.ingenico.com/INGENICO_GALLERY_CONTENT/Documents/corporate/whitepaper/Whitepaper-Wi-fi-vs-Bluetooth.pdf
12. TeleDynamic Communication, *Bluetooth vs. WiFi in today's business environment*, accessed on 23 May 2007, http://www.teledynamic.com/resources/Wireless/Blue_Tech_Over.pdf
13. Crookston R (2004): *Bluetooth vs. WiFi*, accessed on 23 August 2007,http://www.verifonedevnet.com/VeriFone/Attachment/20040804/RetailTechnolog_407_28_316.pdf
14. Vile D (2006): *WiFi Hotspots vs. 3G/HSDPA vs. WiMAX*, accessed on July 2007, <http://www.it-analysis.com/technology/mobile/content.php?cid=8587>
15. Lurie S (2006):*HSDPA vs. WiMAX: Comparing Characteristics and Prospects of Datacom Technologies*, accessed on 23 August 2007, <http://www.digit-life.com/articles2/mobile/wimax.html>
16. Mylavarapu R (2005): *Security Considerations for WiMAX-based Converged network* accessed on June 23, <http://rfdesign.com/mag/508RFDf1.pdf>
17. IEEE. *IEEE Supplement to IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band*, *The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA, June 2003. Institute of Electrical and Electronics Engineers, Inc. (IEEE)*
18. Gast M. *1st Gast The Definite Guide*. O'Reily, 1st edition, 2002.
19. Morrow R. *Wireless Network coexistence*. McGraw-Hill, 1st edition, 2004.
20. Wikipedia. *IEEE 802.11*. <http://en.wikipedia.org/wiki/802.11>, 2006. Retrieved April 12, 2006.
21. ProCurve Networking, *Hewlett-Packard Development Company, L.P. Planning a Wireless Network - White Paper*. www.hp.com/rnd/pdfs/802.11technicalbrief.pdf, 2006. Retrieved 8 December 2006.
22. *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*. Institute of Electrical and Electronics Engineers, Inc. (IEEE), March 2001

23. Rensburg.J.J, Investigation of the deployment of 802.11 wireless networks, MSc thesis from University of Rhodes, 2006,
24. J. Wexler. 2004 WLAN State of the Market Report. *Webtorials*, 2004
25. Mujinga. M, *Evaluation of the IPSec Performance on a Dual Stack IPv4/IPv6*, Masters Thesis from the University of Fort Hare, 2005
26. Barbeau M (2005)WiMaax/802.16 Threat Analysis, accessed on 20 March 2007, www.scs.carleton.ca/~barbeau/Publications/2005/iq2-barbeau.pdf
27. D. Johnson and Walker. J, "Overview of IEEE 802.16 Security", *IEEE Security and Privacy*, 2004
28. Ansari. N, *WiMAX Security Privacy Key Management*, Proceeding form Sendai International Workshop on Network Security and Wireless Communication, January 24, 2007
29. Whittington .B, *A low cost, IP-based access loop for consumer telephony in rural community*, Proceeding of the Southern Africa Telecommunication Network Application Conference, 2005
30. Wireless Security Corporation, *VPN and IPSec: Imperfect Solution for Wireless Security*
31. Wongthavarawat, K. (2005). *IEEE 802.16 WiMAX Security*, retrieved on 1st May, 2006 from http://www.nectec.or.th/nac2005/documents/20050328_SecurityTechnology-05_Presentation.pdf
32. Steven J. Vaughan-Nichols, "Achieving Wireless Broadband with WiMax," *Industry Trends*, IEEE Computer, June 2004.
33. Cisco IOS Release 12.0(5)XE5: *PPTP with MMPE*, accessed on 11 September 2007, <http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xe/120xe5c/pptp.pdf>
34. Dwesa/Cwebe project, online available, www.dewsa.com/ accessed on 27 September 2007.
35. Meenakshi, S. P.; Raghavan, S. V. *Impact of IPSec Overhead on Web Application Servers* Advanced Computing and Communications, 2006. ADCOM 2006. International Conference on Volume, Issue, 20-23 Dec. 2006 Page(s):652 -657

Hippolyte Muyingi (PhD PE Engineering VUB, Brussels) is with the Department of Computer Science, University of Fort Hare. Among his areas of academic interest are PLC communications, Network security, and ICT for development. Prof Muyingi has a long experience in teaching and research and he is the Head of the Fort Hare Telkom Centre of Excellence in Developmental eCommerce, one of the prime sponsors of the Dwesa project.

Tonderai Muchenje was born in Mt Darwin, Zimbabwe. He obtained a Bachelor of Science in Computer Science and Geographical Information System (2004), Bachelor of Science Honors in Computer Science (2005) from the University of Fort Hare and an Advanced Business Analysis Certificate (2006) from University of Pretoria. Currently, studying towards MSc in Computer Science at University of Fort Hare.