

Using WiMAX For Effective Business Continuity During And After Disaster

Elankayer Sithirasenan

School of Information and Communication Technology
Griffith University,
Gold Coast, Australia
+61 7 555 28252
e.sithirasenan@griffith.edu.au

Nasser Almahdouri

Office of His Excellency, the Minister Responsible
for Defense Affairs
Ministry of Defense, Sultanate of Oman
+96 8 243 12814
mod.om@omantel.net.om

ABSTRACT

Disasters occur in different forms and at different times. It can be man-made or natural. In either case businesses can suffer immensely due to interruption to various Information Technology (IT) services. With global warming natural disasters are predicted more often than before. Further, with freely available tools on the Internet more and more hackers are exploiting system vulnerabilities to craft unexpected system failures. With today's heavy dependency on IT, business success exclusively depends on the availability of IT services. Hence sustainability of IT services has become a major concern to organizations. Therefore, establishing network connectivity to an emergency site and enabling system availability will be of immense significance to the success of businesses under disastrous conditions. In this context, the applicability of mobile Worldwide Interoperability for Microwave Access (WiMAX) technology to establish network connectivity during and after a disaster is to be investigated. Although, there are many business continuity solutions dealing with other IT services, the problem of network failure and the ability to quickly establish network connectivity locally and remotely are to be explored in this study.

Categories and Subject Descriptors

C.2.1 [Network Operations]: Network management and Public networks.

General Terms

Management, Design, Reliability, Security.

Keywords

Emergency Networks, Business Continuity, Authentication.

1. INTRODUCTION

Disasters have negative impact on small or large businesses affecting the way it operates. Natural and man-made disasters could be destructive causing power failure, flooding, loss of

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. "IWCMC'10, June 28–July 2, 2010, Caen, France. Copyright © 2010 ACM 978-1-4503-0062-9/10/06/...\$5.00"

customer confidence, and the closure of many business-sectors that inhibit business continuity. However, most organizations develop and establish suitable techniques to prepare themselves to face these kinds of disasters. Such techniques may be different depending on the nature of the business such as IT usage, number of branches, size of business etc. The most common technique is the use of disaster recovery and business continuity plan which examines and assesses the threats that are expected and developing a strategy to mitigate the effect of these threats. Also, backup is a common technique used by many organizations that include daily, weekly, incremental, excremental backups. Site backup or mirror backup is used by large organizations in which they take separate backup in another location other than the original location. However, all these techniques will be useless if the network that serves the organization is no longer functional due to the disaster.

WiMAX is a wireless digital communications technology providing wireless transmission of data, voice and video over long distances. It is based on the IEEE 802.16 standard. WiMAX delivers point-to-point or point-to-multipoint connectivity. It uses Orthogonal Frequency Division Multiplexing (OFDM) which delivers spectral efficiency resulting in higher data rates and overall system capacity [1]. It is a promising technology that offers competitive advantages such as mobility, large area coverage (last mail), quality of services (QoS), and cost effectiveness over the other wireless technologies [2].

This paper is aimed at investigating the viability of employing WiMAX technology to mitigate the effect on businesses and to provide an optional approach for business continuity when organizational network is damaged. We propose to develop, implement and test an emergency network model that can be used during and after a disaster. The model will include all the necessary components to quickly and securely establish the lost network connectivity with the remote backup site. Details of how the existing wired network will be integrated to the swiftly established wireless network, authentication and authorization issues and the secure communication with the remote backup site will be investigated and implemented.

2. EMERGENCY OUTLOOK

In our daily life we experience different kinds of disasters that cause significant damage to property, and loss of life. These disasters have negative impacts on human life with a range of feelings that one might experience varying for different reasons. The degree of personal connection to the impact of disaster will

affect the way a person reacts to it. All disasters happen naturally or are caused by humans.

2.1 Natural Disasters

A natural disaster is a hazardous phenomenon that affects the environment, cause damages, destroys houses and buildings, leads to financial crisis, and loss of lives. The effect of the disaster depends on the type of the disaster and their strengths such as cyclone, earthquake, floods, hailstorms, fire, dust devils, etc. In the recent years the world has experienced many natural disasters. Some of them were very dangerous and caused the humanity a great deal such as the Haiti earthquake on 12th January 2010 that killed over 100,000 lives. The Hurricane Katrina on 29th August 2005 cost 1,800 lives and cost \$105billion for reconstruction.

Weideman and Frank Bacon [3] have examined the effect of Hurricane Katrina on oil companies' stock prices. They have studied and analyzed 15 oil firms in the Gulf of Mexico and examined the effect of disaster on stock price's risk adjusted rate return before and after 30th August 2005. It was revealed that the Hurricane Katrina had a significant and negative impact on the risk adjusted rate of return on selected oil company stock prices over the event study period and stock return dropping significantly in the disaster area. Also, the oil company stock price return started a significant downturn up to 25 days prior to 30th of August. Finally, in the short run, the disaster caused negative return on stocks for oil companies.

Kenneth Lacho [4] studied the impact of Hurricane of Katrina on the small businesses in Ruston, Louisiana about 400 miles from the impact area. He conducted personal interviews with 12 small business owners during the period from 14th to 27th of September 2005. Also, he interviewed the Ruston Chamber of Commerce and the director of the Small Business Development Center at Louisiana Tech University. The 12 firms that have been included in his study were from different perspectives (filed). The study found that due to influx of evacuees immediately after the Hurricane of Katrina, many small businesses in Ruston experienced an increase in sales.

2.2 Man-Made Disasters

Other than natural disasters there are man-made disasters which are caused by human beings. Human-made disasters occur when actions by people lead to different forms of threats to infrastructure. These kinds of disasters are created intentionally or by accident and can cause colossal harm to public. Also, sometimes they are directed by people or organizations to gain hidden benefits and may be influenced by religion or believe. The 9/11 attack is such a disaster where 19 terrorists from Al-Qaida hijacked 4 planes and intentionally crashed them into the Twin Towers of the World Trade Center and Pentagon, killing all the passengers and about 2,976 people in the buildings. Sasser worm is another example of man-made disaster which affects computers running Microsoft operating systems. This virus can exploit systems via network ports without user intervention.

Anat and John [5] studied how virus attack announcements impacts on the market value of firms. They selected market value as a measure of the economic impact of security breach (Virus

attack) announcements on companies. They collected data on virus attacks using a search of business news in Lexis-Nexis database and found 224 public announcements of virus attacks between 1988 and 2002. After analyzing the data, they found that virus attack announcements had no significant impact on share prices of the affected companies.

Jack Kondrasuk [6] conducted a study on the effects of 9/11 and terrorism on human resource management: recovery, reconsideration, and renewal. Employers were affected by 9/11 in numerous ways; crisis management teams and plans increased and disaster plans were either revised or developed. Jack has resulted that 9/11 attacks effected the human resources management in different organizations. 76% of the companies allowed employees to cancel or delay business travel, 62 % allowed employees to take time off if needed, and 45% cancelled meetings and events. However, he found that the above percentages had decreased by August 2002. Further, the crisis management plans and employee assistance programs increased in that year. The 9/11 attack affected the employment area of HRM centered on callus of military-involved employees, screening applications, equal employment opportunity, and layoffs of employees. Also, hiring and terminating of employees received more attention.

2.3 Business Continuity

To ensure business continuity, majority of organizations have examined and assessed their threats and established methods to avoid or mitigate the effects. As mentioned before, lately, most businesses have prepared disaster recovery and business continuity plans to mitigate the effects due to a disaster.

Khalid Salem et al. [7] studied about business continuity information network for rapid disaster recovery. They have presented a model for pre-disaster preparation and post-disaster business continuity / rapid recovery. This model is used to design and develop a web based prototype of Business Continuity Information Network (BCIN) system. The BCIN enables collaboration between local, state, federal agencies and the business community for rapid disaster recovery, by allowing disaster information exchange among participants and provide businesses with effective and timely disaster recovery information. The BCIN model provides different dashboards with support for map based, location specific, and disaster related data analysis. BCIN can support intelligent decision making and suggest possible preparation and recovery plans depending on latest damage status and historic disaster profiles.

Kimberly, et al. [8] conducted a study on designing for disasters. They have presented a data dependability solution (solver) which protects against several threats such as data loss, data corruption, and data inaccessibility. This solution uses recovery time objective (RTO) to specify the maximum time allowed until application services are restored after disaster, recovery point objective (RPO) to give maximum time for which recent updates may be lost, and penalty rates: the cost of service outages and data loss. Solver uses different data protection and recovery models with parameters such as tape backup, remote mirroring etc. As the solver is provided with input data, it will show the best scenario to protect and recover the business data.

3. WIMAX APPLICATIONS

Several countries around the world have already deployed WiMAX to take the competitive advantages and features that WiMAX offers to reach more and more user communities. WiMAX is used in different application areas such as internet, mobile phone, TV broadcast and monitoring. Other than commercial usage, WiMAX can be used in isolated areas by establishing WiMAX networks in the remote area and connecting it with the main WiMAX network via satellites [9]. During disasters these kinds of networks will help avoid significant damages or loss of lives in the disaster area, since WiMAX, once established can facilitate communication with aid agency to obtain urgent support [10]. Another use of WiMAX is environment monitoring such as Volcano, fire monitoring, and telemedicine applications [11]. Also, EU's Sixth Framework

Our proposed model is developed in two stages. First, as shown in Fig. 1, we have modeled the emergency network that depends on the WiMAX network to communicate between the swiftly established WiFi network and the backup site. Next, we modeled the authentication and security mechanism needed to securely connect the emergency network via the third party WiMAX network to the backup site. In this view, we have developed an authentication and authorization model that securely authenticates the wireless hosts in the emergency network with the AAA (authentication, authorization, and accounting) server [13] in the backup site.

Our proposed model enables quick and easy establishment of an

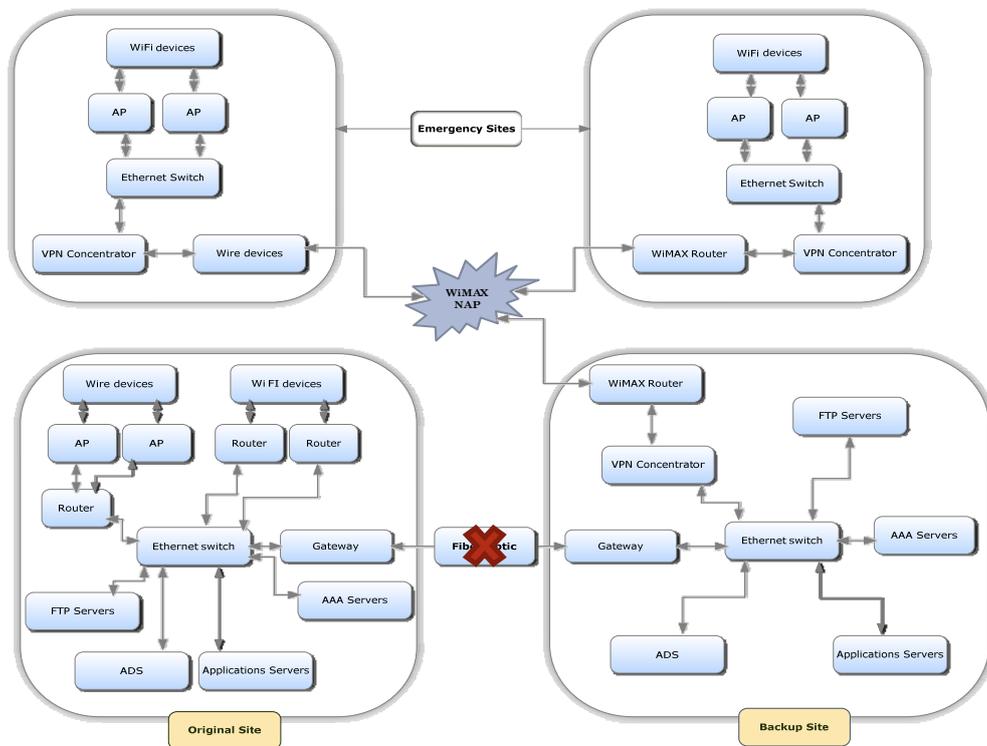


Figure 1. Original and Emergency Network Paradigm

Program Project WEIRD, using WiMAX advantages, is established in European countries to extend the connectivity of the pan-European data communication network to isolated and impervious area. Further, WiMAX can also be used to monitor areas such as seismic and volcanic zones and alert the population about the occurrence of natural catastrophes in these area [12].

4. PROPOSED MODEL

As a result of the disaster the servers located in the original site may have been destroyed or damaged and /or the network connectivity lost. Hence, to provide the lost IT services, users will have to be connected to the data and application servers located at the backup site.

emergency network when one or more of the original network is destroyed due to a disaster. In the case the normal operations network is destroyed, all servers from the original site will be inaccessible. Therefore our proposed emergency network will be using the servers in the backup site that are replicates of the original servers. Moreover, due to the disaster, if the fiber optic cable connectivity is no longer available to the backup site, the emergency network will mainly use the WiMAX connectivity subscribed through the WiMAX network access provider.

Further, network security and authentication are critical, especially for wireless communications with low infrastructure costs such as wireless local area networks (WLANs). Furthermore, when data is transmitted over the WiMAX network

its security must be guaranteed explicitly rather than depending on the WiMAX service provider's security options.

In our proposed model, the wireless hosts in the emergency network need to associate themselves with the access points (AP) either by listening to the AP's "Beacon" or advertising themselves by a "Probe Request". When both the AP and the wireless host agree on a common set of security parameters the first phase of association is deemed complete. In the next phase, the wireless host must authenticate itself to the AAA server in backup site. We propose to use EAP-TTLS authentication for this purpose since it has the advantages of very secure exchange of data, requires only the server side certificate, supported by a wide range of OS, username / password is not enough to gain access as the client side private key is still required, and supports session resumption [14]. The goal of this authentication is only to secure the data between the wireless host and the AP. The wireless host initiates EAP-TTLS authentication by sending a "Hello" message to the AAA server as shown in Fig. 2. Upon receiving this message, the AAA server will reply with a "Hello" message that includes the server's certificate, server key exchange and server request. At

However, this traffic encryption is only between the wireless host and the AP. Within the third party WiMAX network we have no guarantee on the confidentiality, integrity and authenticity of the data. The third party WiMAX network may use its own security mechanism to protect data within their network. In our model, we assume that the security mechanism used by the WiMAX Network Access Provider (NAP) is unknown and hence we do not risk transmitting the organizational data over the third party network. Therefore, in our proposed model we introduce our own solution to ensure the security of data within the third party WiMAX network. In this context, we propose to use Virtual Private Network (VPN) concentrators that provide end-to-end security not withstanding the underlying security mechanism.

VPN is a widely adopted technology that can transform a public network into a private network. Using encryption and authentication technologies to protect access, and tunnels for transmission, VPN enables secure site-to-site and remote access connections over IP [15]. The VPN concentrator encrypts all data coming into it and encodes it into a form that can only be decoded

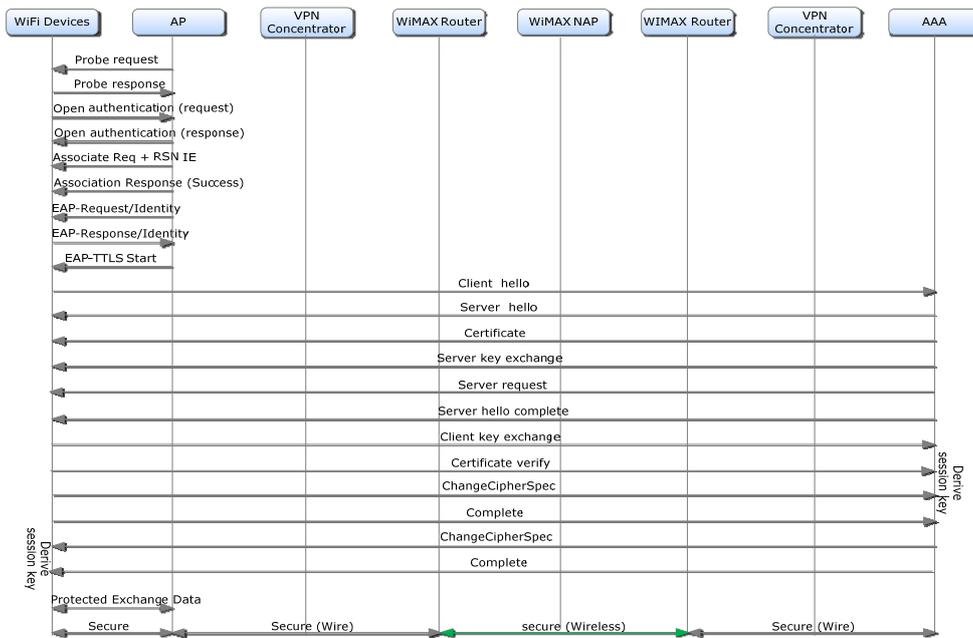


Figure 2. Authentication and Security Paradigm

this point the first negotiation stage is complete. The second stage of the negotiation is to exchange the session key. The wireless host will then verify the server certificate and send the derive session key message that contains the client key exchange, and the change cipher specification. The AAA server, in turn, will send the derive session key message that includes the change cipher specification. At the end of this second stage of EAP-TTLS authentication, the wireless host and the AAA server derive the Pairwise Master Key (PMK). The PMK is then transferred to the AP. The wireless host and the AP then perform a 4-way handshake to authenticate each other and derive the Pairwise Transient Key (PTK) for traffic encryption.

by the VPN concentrator at the other end. For example, as in symmetric-key encryption each VPN concentrator will share the same secret key. Therefore, in our proposed model, VPN concentrators are used to encrypt data before it is sent over the third party WiMAX network. Hence, the VPN concentrator in the backup site must use the same secret code to decode the data.

5. DISCUSSION

The major challenge in the proposed disaster recovery model is the authentication and authorization of the wireless hosts in the emergency network. Prior to disaster the wireless hosts will be authenticated by the AAA server located in the original site. In

our case we propose to use EAP-TTLS authentication mechanism to authenticate the wireless hosts with the AAA server. The AAA server is linked to the Active Directory Services (ADS) server to utilize the authentication database used to authenticate and authorize all users in the organization.

EAP-TTLS offers very good security facilitating a tunneled connection between the client and the server. The client can but not necessarily need to be authenticated via a CA-signed PKI certificate. This immensely simplifies the setup procedure as a certificate is not needed to be installed on every client. The server can securely be authenticated to the client via its CA certificate and both the client and the server can establish a secure connection ("tunnel"). The server can then use this established connection to authenticate the client. It can use an existing and widely deployed authentication protocol and infrastructure, incorporating legacy password mechanisms and authentication databases, while the secure tunnel provides protection from eavesdropping and man-in-the-middle attack.

The EAP-TTLS authentication mechanism uses the ADS to authenticate and authorize the wireless users via the AAA server. Therefore, in the event of a disaster, the wireless hosts in the swiftly established wireless networks should have access to an AAA server. Further, the AAA server must have access to an ADS server that contains the authentication database. Hence, it is necessary to equip the backup site with an AAA server linked to a replicate of the ADS server in the original site. With this setup in place, the wired and/or wireless users can be authenticated by either the AAA/ADS servers in the original site or that in the backup site. However, in case of the emergency network we will be accessing only the AAA/ADS servers at the backup site via the WiMAX network.

6. CONCLUSIONS

Natural and/or man-made disasters may strike anywhere and anytime. Damages caused by these kinds of disasters may be physical or psychological. They can also have significant impact on both small and large businesses. In today's competitive world, business success significantly depends on the availability of IT services, especially those with heavy dependency on such services. In this context we have proposed a disaster recovery model that can mitigate the effect on organizational networks facilitating quick resumption of lost IT services. The model includes adequate facilities to authenticate and authorize users and to secure the organizational data within and outside the emergency network.

7. REFERENCES

- [1] IEEE Std. 802.16-2004, IEEE Standard for Local and metropolitan area networks: Part 19: Air Interface for Fixed broadband wireless access systems.
- [2] Wenhua Jiao, Jianfeng Chen and Fang Liu. Provisioning end-to-end QoS Under IMS over WiMAX architecture. *Bell Labs Technical Journal*. Vol. 12, No. 1. pp. 115-121, 2007.
- [3] Weideman, I and Bacon, F. Hurricane Katrina's Effect on oil company stock prices. *Academy of Strategic Management Journal*. Special Issue 7, pp. 11-16, 2008.
- [4] Lacho, K. The Impact of Hurricane Katrina on Small Business in Ruston, Louisiana. *Academy of Strategic Management Journal*. Special Issue 7, pp. 77-84, 2008.
- [5] Anat Hovav, and John D'Arcy. The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security*, vol. 13, No.3. pp. 32-40, 2004.
- [6] Jack, N. The Effects of 9/11 and Terrorism on Human Resource Management: Recovery, Reconsideration, and Renewal. *Employee Responsibilities and Rights Journal*, Vol. 16, No.1. pp. 25-35, 2004.
- [7] Saleem, K. Luis, S. Deng, Y. Chen, S. Hristidis, V. Tao, L. Towards a Business Continuity Information Network for Rapid Disaster Recovery. *The proceedings of the 9th Annual International Digital Government Research Conference*. pp. 107-116, 2008.
- [8] Keeton, Santos, Beyer, Chase, and Wilkes 2004. Designing for Disasters. *Proceedings of the 3rd USENIX Conference on File and Storage Technologies*. 2004.
- [9] Mignanti, S. Castellano, M. Spada, M. Simoes, P. Tamea, G. Cimmino, A. Neves, P. Marchetti, I. Andreotti, F. Landi, G. and Pentikousis, K. WEIRD testbeds with fixed and mobile WiMAX technology for user applications, telemedicine and monitoring of impervious areas. *Proceedings of the 4th International Conference on Testbeds and Research infrastructures For the Development of Networks & Communities* 2008. 2008 (Brussels).
- [10] Donahoo, M.; Steckler, B., "Emergency mobile wireless networks," *Military Communications Conference, 2005*. Vol. 4, pp. 2413-2420, 2005.
- [11] Castrucci, M. Castellano, F. Bianco, F. Bestetti, E. Angori, F. Landi, G. Sing WiMAX Volcano Monitoring during an Emergency: WEIRD System. *Proceedings of the 4th International Conference on Testbeds and Research infrastructures For the Development of Networks & Communities* 2008. 2008 (Brussels).
- [12] Neves, P. Simoes, P. Gomes, A. Mario, L. Sargento, S. Fontes, F. Monteiro, E. Bohnert, T. WiMAX for Emergency Service: An Empirical Evaluation. *The 2007 International Conference on Next Generation Mobile Application, Service and Technologies*. 2007.
- [13] Rigney, C., Willens, S., Rubens, A., and Simpson, W. Remote Authentication Dial-In User Service (RADIUS). *RFC 2865*, June 2000.
- [14] Liu, D. Q. and Coslow, M. Extensible authentication protocols for IEEE standards 802.11 and 802.16. In *Proceedings of the international Conference on Mobile Technology, Applications, and Systems*. 2008 <http://doi.acm.org/10.1145/1506270.1506330>
- [15] Raghunath, S., Ramakrishnan, K. K., and Kalyanaraman, S. Measurement-based characterization of IP VPNs. *IEEE/ACM Trans. Netw.* 2007. <http://dx.doi.org/10.1109/TNET.2007.896539>