



WiMAX User Access Control using Fingerprint Biometric System

B. DAS, M. M. SHAIKH, M. R. ANJUM*, A. A. JAMALI⁺⁺, M. F. L. ABDULLAH^{**}, Y. AL-ASHQA^{**}

Department of Electronic Engineering, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshh, Sindh, Pakistan.

Received 14th September 2017 and Revised 26th March 2018

Abstract: WiMAX offers the wireless connectivity for mobile internet and its security support is compulsory for networks to protect the both user and network because wireless medium is available to all and the attackers can easily access the network. This makes the network less secure for the users and service providers. Currently, WiMAX system is dealing with many security challenges. WiMAX has air interface channel for transmission medium and due to this both the PHY and MAC layers are readily exposed to security threats. There are many solutions are available to protect the WiMAX system such as; powerful WiMAX transmitter, a high gain WiMAX transmission or receiving antenna, and protocol design. However, each solution has its own advantages and disadvantages in particular scenario. In the existing research, there is lack of integrated presentation of solutions to all the security issues of mobile WiMAX network. In this paper, a system is proposed to provide more security for admittance control system for WiMAX system to prevent from network usage from the unauthorized persons. In the proposed system a fingerprint based system is designed to secure WiMAX system from the network usage of unauthorized persons. The system is developed using MATLAB Simulink model and design is successfully verified for real-time fingerprint. The designed system offers the robustness and reliability of managing the users of WiMAX system.

Keywords: Additive white Gaussian noise (AWGN), Biometric System, Fingerprint Recognition System, WiMAX (Worldwide Interoperability for Microwave Access).

1. INTRODUCTION

Broadband Wireless Technology offers the high speed internet facilitates for the residential and small and Medium Enterprises (SMEs) (Kaushal *et al.*, 2017). Wireless broadband access is standardized using IEEE standard of IEEE 802.16. This Standard is also well recognized with Worldwide Interoperability for Microwave Access (WiMAX) technology. WiMAX offers the high-speed connectivity for many users, cable broadband is not practicable. It has been reported that WiMAX technology is encountered with issues such as; data and network security (Shon, *et al.*, 2010), management of operation in terms of unauthorized users (Nguyen, 2009). From the existing WiMAX security system (Khan, and Yousef, 2017), (Sain, *et al.*, 2017), it is determined that an admission control system can be developed to reserve radio resources for precise connections and avert the unauthorized network consumers. It has been also demonstrated that to secure and shield the WiMAX technology in terms of data and network security and management of operation from unauthorized persons from using it there are different solutions are proposed (Gilanian-Sadeghi, *et al.*, 2017), (Strohmeier, Schäfer, *et al.*, (2017). However, each secure WiMAX technology has its own advantages and disadvantages for the particular situation of WiMAX system. In this paper, a new system is proposed to provide more security for admittance control system for

WiMAX system to prevent from network usage from the unauthorized persons via biometric system.

2. BACKGROUND

WiMAX is the abbreviation of Worldwide Interoperability for Microwave Access that provides the wireless connectivity for broadband solution. WiMAX is categorized based on IEEE 802.16 Standard that is for wireless broadband. WiMAX system security support is compulsory for networks to protect the users as well as the network. Wireless medium is available to all, the attackers can easily access the network and the network becomes more vulnerable for the user and the network service provider. WiMAX system has many security challenges because WiMAX is exposed more to security intimidations than other wireless networks. These threats include attacks against IEEE 802.16-2001 that require an adversary to physically place the attacking equipment between base stations. There are many WiMAX security solutions are available, such as; Protocol Key Management (PKM), Security Association (SA), WiMAX security certification and etc. for secure services. However, all these protocol based security solution can be cracked using software bugs. Therefore, the need of authentication system for WiMAX is in high demand (Ahson and Ilyas, 2007). In the existing research, there is lack of integrated presentation of solutions to all the security issues of mobile WiMAX

⁺⁺Corresponding Author Email: jamali.abdulaleem@quest.edu.pk ; Tel : +92-332-285762

^{*}Department of Electronic Engineering, Islamia University Bahawalpur, Pakistan

^{**}Faculty of Electrical and Electronic Engineering, Universiti Tun Hussain Onn Malaysia, Johor, Malaysia.

network, which is important for researchers and practitioners (Rengaraju, Lung, *et al.*, 2009). For this reason, the biometric based system integration with WiMAX is required to secure network. Biometrics system refers to a system that provides an identification of life based on physiological or behavioral characteristics. The existing WiMAX user secure system are discussed as follow; (Tsagkaris and Demestichas 2009) discussed the security precaution are required for the network authentication and access system. (Ranjan, 2016) discussed the authentication techniques are discussed for Internet of Things (IoT) and access control is for managing interaction and communication between users and systems. IoT including RFID and sensor networks to traditional server-based computing. In this work, a solution to issues with WiMAX's user security system is proposed via biometric (Fingerprint) system to provide a safeguard to WiMAX system. In this research, for WiMAX authentication system, the biometric system based i.e fingerprint identification system is developed. Fingerprint-based identification provides the credentials via human fingerprints for personal identification. The fingerprints are believed to be unique across individuals and across fingers of same individual.

3. METHODOLOGY

In this paper, the biometric systems via Fingerprint system is designed to secure WiMAX protocol that provides the efficient method to manage users' authentication for WiMAX network. The designed methodology for the proposed system is demonstrated in (Fig. 1). It can be observed from Fig 1 that user can't access the WiMAX network until their successful biometric verification is not achieved using system. The users that are registered in the biometric database after successful verification will be allowed to access the WiMAX network. The system is designed using MATLAB that provides the system design and verification for the designed multiple biometric system. It is also demonstrated in (Fig. 1) that the user to access the WiMAX network gives his fingerprints on fingerprint device. The given fingerprint will be compared with the database. If the exact fingerprints are matched with database for the user, the WiMAX network allocate a lot for that user. The system is designed in mainly two ways. In the first, WiMAX system is demosntarted. Secondly, fingerprint system integrated with WiMAX to control the user interaction.

4. WIMAX SYSTEM DESIGN

The WiMAX system is designed using transmitter, channel and receiver. The WiMAX transmitter is further categorized in different components such as; MAC data Randomizer, Block Encoder, convolution Encoder,

Interleaver, IO Mapper, and Modulation Scheme as shown in (Fig. 2).

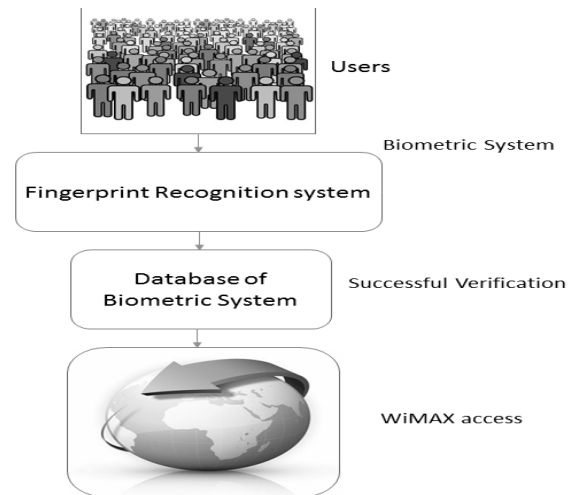


Fig. 1: Design methodology for multiple Biometric WiMAX access system

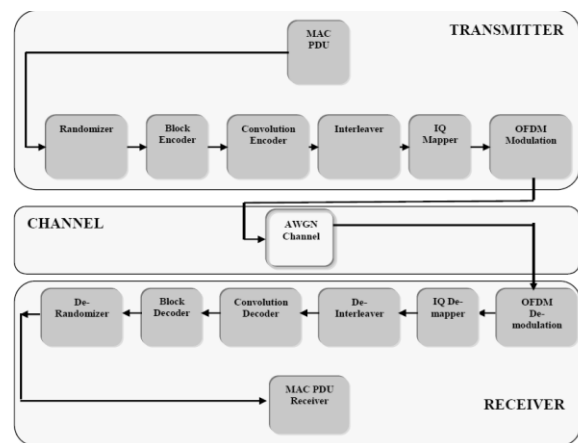


Fig. 2: WiMAX system block diagram

The WiMAX transmitter transmit the data over AWGN channel. The AWGN channel is characterized using different parameters. Finally, the receiver block, which consist of De-randomizer, Block Decoder, Convolution Decoder, De-Interleaver, IQ Demapper, OFDM modulation, and MAC receiver. The complete WiMAX system block diagram is shown in Fig. 2. WiMAX transmitter composed of signal generator, that include data randomization, data coding, data interleaving, data mapping, and data modulation as demonstrated in (Fig. 2). In the WiMAX receiver, the OFDM modulation is performed using elimination of CP, Fourier Transform, and disassembling the data frame. It is contrary operation of OFDM modulation. In the next, the designed Fingerprint biometric system is discussed.

5. SYSTEM DESIGN FOR FINGERPRINT BIOMETRIC SYSTEM

The fingerprint biometric system is used to collect the fingerprints from the user for WiMAX network access. The fingerprint system design is demonstrated as shown in (Fig. 3). The designed system offers the feature extraction of fingerprint for the user. It is defined that the designed fingerprint system is developed in MATLAB. The fingerprint system determines a reference point and region of interest for the fingerprint image. It tessellate the region of interest around the reference point. The fingerprint system has the filtertaion a Gabor filters. Finally, FingerCode (feature vector) are computed using the average absolute deviation of gray values in individual sectors in filtered images.

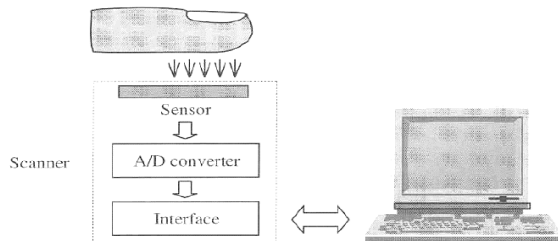


Fig. 3: Fingerprint System Design.

The fingerprint system is designed using centralization, Cropping, Sectorizing, Normalizing, Gabor, Convolute normalized image with Gabor filters, and Check. In the centralizing, input image is divided into non-overlap chunks. The gradients and local ridge orientation of each chunk centered at pixel is computus. Finally, the binarization is performed. Bsinarize implements intensity thresholding and other binary segmentation methods for images and can operate either automatically or given explicit cutoff values.

6. INTEGRATION OF FINGERPRINT BIOMETRIC SYSTEM WITH DESIGNED WIMAX SYSTEM

The designed WiMAX system and Fingerprint biometric system is combined together as illustrate in (Fig. 4) It can observed from Figure 4 that the system processing is initiate with input image after that a reference point and region of interest is extracted from the fingerprint image. This region of interest fingerprint image is proceed for the centralization, where the gradient for each is computed. After centralization, this fingerprint image process for cropping so that center point of 175 X 175 pixel area can be extracted. Later, the fingerprint image is sectorizing for detail extraction of fingerprint image for five concentric band of width 15 pixels with total 80 sectors. This noise from the

sectorizing image is eliminated due to finger pressure difference. This normalized image is filtered to produce clearer image for classification.

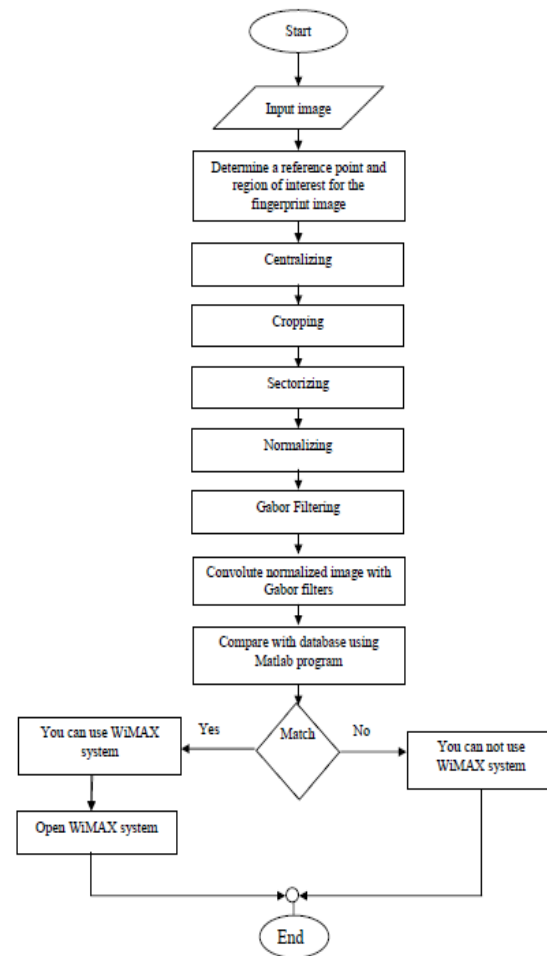


Fig. 4: Integration of WiMAX and Fingerprint biometric system.

The filtered fingerprint image is compare with database using MATLAB program. If the fingerprint image is matched with database, the WiMAX access will open for the user. In case, the fingerprint image is not matched with database, the WiMAX access is not open for the user. The user may be eligible for the WiMAX system access only his/her particular fingerprint images are registered in database. Otherwise, WiMAX network access is not possible for the match denied fingerprint image of the person. In the next, the results of the designed system is dicussed.

7. RESULTS AND DISCUSSION

In this work, WiMAX user control system is designed using MATLAB using biometric system. The designed system is initiated by designing the simulator for combining the WiMAX and biometric system. The

main Graphical User Interface for the designed WiMAX user control system using biometric system in MATLAB is demonstrated using (Fig.5).



Fig. 5: Graphical User Interface for the designed WiMAX access system using biometric system

It can be observed from (Fig. 5) that the Graphical User Interface for the designed WiMAX user control system using biometric system after the successful verification of both system the user will be allow to access the WiMAX system.

The WiMAX simulation system is designed using IEEE 802.16e WiMAX standard along with ETSI HiperMAN and PHY layer Model. The designed WiMAX simulation system is developed in MATLAB using the different blocks. The designed model for WiMAX simulation system is developed in MATLAB. The Simulink model for the designed WiMAX simulation system is shown in Fig. 6. It is illustrated in (Fig. 6) that the designed WiMAX simulation system has three part; WiMAX transmitter, AWGN Channel and WiMAX receiver.

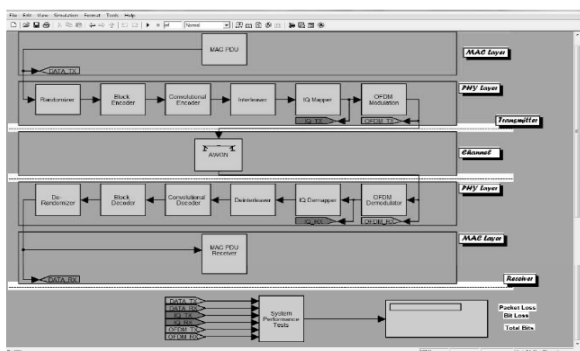


Fig. 6: MATLAB Simulink model for the designed WiMAX simulation system

It can be observed that Simulink model for the designed WiMAX simulation system in (Fig. 6) is designed using different Simulink blocks. The designed WiMAX simulation system consist of MAC layer, PHY layer, WiMAX transmitter, AWGN Channel, and

receiver that are developed in MATLAB Simulink. The model also demonstrates the packet loss, bit loss and total loss for WiMAX system.

It is defined that execution of RS encoding is verified by arriving the aforementioned test vectorx Hex data as an input. Similiray, RS encoder verified for the output vector. Likewise, the complete model is tested using vector block for ensuring correct working of each block. The performance of the designed WiMAX simulation is demonstrated using modulation and code rate equal $\frac{3}{4}$. The performance of the designed WiMAX simulation is demonstrated using (Fig. 7) and in (Fig. 8).

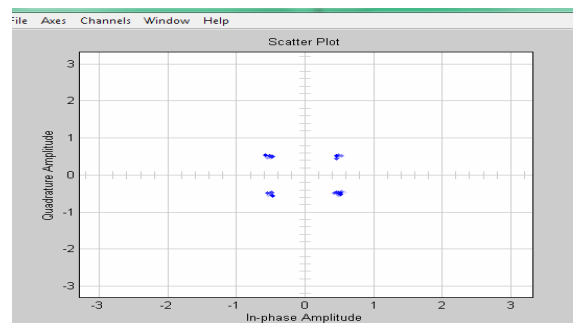


Fig. 7: Constellation diagram

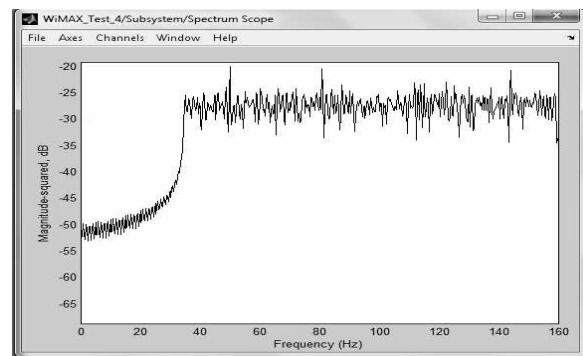


Fig. 8: Spectrum of WiMAX

After the successful performance analysis of designed WiMAX simulation system, the performance of Fingerprint system is demosntared. The fingerprint Biometric System is configured in MATLAB. It is defined that fingerprint biometric System is designed using MATLAB coding that has different function. It is defined that after the successful execution of aforementioned fingerprint biometric System MATLAB program, in result, a window will papered for further action to use the fingerprint biometric System. This fingerprint biometric System has different feature image to be add in database, image to be taken for fingerprint recognition, and also the fingerprint can be deleted from the database to manage and control the WiMAX access as shown in (Fig. 9).



Fig. 9: Main window for fingerprint recognition system after code execution

After that user will press the button (Pick out image and add to database) and then the window in (Fig. 10) will be display;

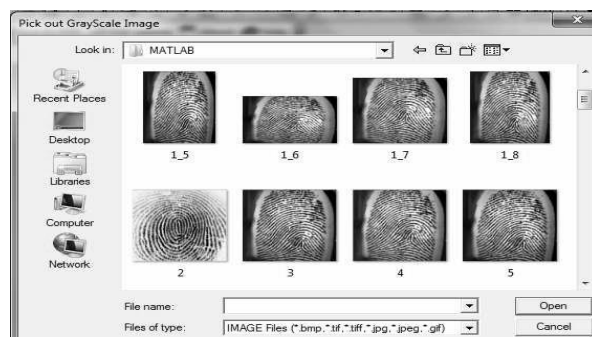


Fig. 10: Window for pick out Grayscale image.

The selection of these image are used option "Pick out image for fingerprint recognition". In case user's selected image and its not associated with images in database, the singing message of "Sorry, you are not allowed to use WiMAX system" is appeared and the access to WiMAX access is restricted. Otherwise the singing message of "Welcome, you can use WiMAX system" is appeared and the access to WiMAX is allowed for user.

8. CONCLUSION

In this work, the integration of WiMAX system is performed in association with biometrics system is demonstrated to manage, control and authenticate the user access system for WiMAX system. The system is developed using MATLAB Simulink. Biometric system offer the comparison of fingerprint recognition of the user available in database with the users' that want to access the WiMAX network. If the matching between both image and voice is successful, the WiMAX network is allowed for the users'. In case, the matching is failed, the WiMAX network is restricted. The designed system benefits directly or indirectly to cost savings, network security issues, and delivery of enhance services of WiMAX.

ACKNOWLEDGMENTS:

This work is supported by Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Sindh, Pakistan and Universiti Tun Hussein Onn Malaysia. The authors would like to thank both the organization for their support and encouragement to carry out this research work.

REFERENCES:

- Ahson, S. A., and M. Ilyas. (Eds.). (2007). WiMAX: standards and security. CRC press.
- Gilanian-Sadeghi. M. M., B. M. Ali. and M. Ma. (2017). A Novel Energy Efficient Key Distribution Scheme for Mobile WiMAX Network. *Wireless Personal Communications*, 92(2), 727-748.
- Kaushal. H., V. K. Jain. and S. Kar. (2017). Overview of Wireless Optical Communication Systems. *Free Space Optical Communication*, 1-39.
- Khan. I., and S. Yousef. (2017). Using Dual Trigger Handover Algorithm to Improve WiMAX Handover Delay. In *International Conference on Global Security, Safety, and Sustainability*, pp. 281-289, Springer, Cham.
- Nguyen. T., (2009). A survey of WiMAX security threats. *Computer Science Department, Washington University*, 1-15.
- Ranjan. A. K., and G. Somani. (2016). Access Control and Authentication in the Internet of Things Environment. In *Connectivity Frameworks for Smart Devices*, 283-305. Springer International Publishing.
- Rengaraju. P., Y. Qu. and A. Srinivasan. (2009, September). Analysis on mobile WiMAX security. In *Science and Technology for Humanity (TIC-STH), IEEE Toronto International Conference*, 439-444.
- Sain. M., Y. J. Kang. and H. J. Lee. (2017). Survey on security in Internet of Things: State of the art and challenges. In *IEEE 19th International Conference Advanced Communication Technology*, pp. 699-704.
- Shon. T., B. Koo. J. Park. And H. Chang. (2010). Novel approaches to enhance mobile WiMAX security. *EURASIP Journal on Wireless Communications and Networking*, 1, 926275.
- Strohmeier. M., M. Schäfer. R. Pinheiro. V. Lenders. and I. Martinovic. (2017). On Perception and Reality in Wireless Air Traffic Communication Security. *IEEE Transactions on Intelligent Transportation Systems*, 18(6), 1338-1357.
- Tsakkaris. K., and P. Demestichas. (2009). Wimax network. *IEEE Vehicular Technology* 4(2). 7667-7672.