

Improving Security Authentication of IEEE 802.16 WiMax with New Public key algorithm

Prakash Kuppuswamy¹, Sikandhar Shah²

Lecturer, Department of Computer Engineering & Networks,
Jazan University, Jazan, KSA.^{1,2}

ABSTRACT

WiMAX technology is a new trend in wireless communication. The IEEE Standard 802.16 WiMAX protocol provides wireless broadband access to homes, businesses and core telecommunication networks worldwide. Many sophisticated authentication and encryption techniques have been embedded into WiMAX but it still exposes to various attacks in. This paper provides a mechanism for increasing the efficiency and hence improves the existing model of 802.16 protocols using new public key algorithm. We are attempting here new algorithm based on block cipher (Nlbc) for the replacement of RSA algorithm which is using in the IEEE Standard 802.16 WiMAX Technology.

Keywords: IEEE 802.16, WiMAX, network security, authentication, encryption, MAC module etc.,

1. INTRODUCTION

Worldwide Interoperability for Microwave Access was Established by IEEE Standards Board in 1999, the IEEE 802.16 is a working group on Broadband Wireless Access (BWA) developing standards for the global deployment of broadband Wireless Metropolitan Area Networks [Wiki_802.16]. In December 2001, the first 802.16 standard which was designed to specialize point-to-multipoint broadband wireless transmission in the 10-66 GHz spectrum with only a light-of-sight (LOS) capability. But with the lack of support for non-line-of-sight (NLOS) operation, this standard is not suitable for lower frequency applications. Therefore in 2003, the IEEE 802.16a standard was published to accommodate this requirement [1].

In last decade there has been great evolution in Wireless technology. WiMAX is an emerging technology used for deploying broadband wireless metropolitan area network. WiMAX works in same manners as Wi-Fi but the difference between them is high speed, larger distance, and large number of users. The radio link between WiMAX node support Non Line of sight(NLOS) and line of sight (LOS) signal propagation. For interconnection

between different WiMAX towers in LOS link microwave link can be used[2][5].

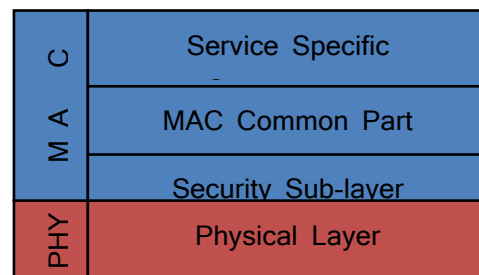


Figure 1. IEEE 802.16 Protocol structure

In the 802.16 standard, encrypting connections between the MS and the BS is made with a data encryption protocol applied for both ways. An encapsulation protocol is used for encrypting data packets across the BWA. An authentication protocol, the Privacy Key Management (PKM) protocol is used to provide the secure distribution of keying data from the BS to the MS [3]. Through this

secure key exchange, due to the key management protocol the MS and the BS synchronize keying data. The basic privacy mechanisms are strengthened by adding digital-certificate-based MS authentication to the key management protocol. In addition, the BS uses the PKM protocol to guarantee conditional access to network services [4]. The encryption algorithm used at MAC layer in the existing model is the RSA algorithm. In the proposed model, we use ECC (Elliptic Curve Cryptography) algorithm.

The task of securing 3G wireless networks and system is challenging one. Strong security mechanism is needed for core network, the application server, and to secure the end user. KEY management for 3G mobile wireless devices support network architecture as well as security issues of accessing the Internet from fixed location. It offers flexibility and mobility also [6].

In recent years there has been increasing interest shown in wireless technologies for subscriber access, as an alternative to traditional twisted-pair local loop. These approaches are generally referred to as wireless local loop (WLL), or fixed-wireless access. To provide a standardized approach to WLL, the IEEE 802 committee set up the 802.16 working group in 1999 to develop broadband wireless standards. IEEE 802.16 standardizes the air interface and related functions associated with WLL. Three working groups have been chartered to produce standards:

- IEEE 802.16.1 - Air interface for 10 to 66 GHz.
- IEEE 802.16.2 - Coexistence of broadband wireless access systems.
- IEEE 802.16.3 - Air interface for licensed frequencies, 2 to 11 GHz.

The work of 802.16.1 is the farthest along, and it's likely that it will generate the most interest in the industry, as it is targeted at available frequency bands. An 802.16 wireless service provides a communications path between a subscriber site and a core network. Examples of a core network are the public telephone network and the Internet. IEEE 802.16 standards are concerned with the air interface between a subscriber's transceiver station and a base transceiver station.

Protocols defined specifically for wireless transmission address issues related to the transmission of blocks of data over a network. The standards are organized into three-layer architecture. The lowest layer, the physical layer,

specifies the frequency band, the modulation scheme, error-correction techniques, synchronization between transmitter and receiver, data rate and the time-division multiplexing (TDM) structure.

For transmission from subscribers to a base station, the standard uses the Demand Assignment Multiple Access-Time Division Multiple Access technique. DAMA is a capacity assignment technique that adapts as needed to respond to demand changes among multiple stations. TDMA is the technique of dividing time on a channel into a sequence of frames, each consisting of a number of slots, and allocating one or more slots per frame to form a logical channel. With DAMA-TDMA, the assignment of slots to channels varies dynamically. For transmission from a base station to subscribers, the standard specifies two modes of operation, one targeted to support a continuous transmission stream (mode A), such as audio or video, and one targeted to support a burst transmission stream (mode B), such as IP-based traffic. Both are TDM schemes.

2. REVIEW OF LITERATURE

GuoSong Chu, Deng Wang, Shuliang Mei (2002) providing quality of service guarantees for heterogeneous classes of traffic with different QoS requirements in fixed broadband wireless access system is a very important and challenging problem. Although IEEE 802.16 MAC protocols have been proposed to support QoS guarantees for various kinds of applications, they do not suggest how to schedule traffic to fulfill QoS requirements. In order to provide different levels of QoS guarantees for various applications while still achieving high system utilization, QoS architecture should be integrated into the MAC protocol [7].

Yogesh Gedam, Dr.S.D.Chede (2011) The IEEE specified some powerful standards for WiMAX security based on security control including PKM-RSA. Many sophisticated authentication and encryption techniques have been added but secure technology does not constitute itself a secure end to end network, consequently WiMAX network unable to protect against criminal and malicious exploitation of network infrastructure. This paper presents a multiple key concept in privacy and key management protocol to enhance the security in Wireless communication [2].

Pranita K. Gandhewar, Kapil N. Hande (2011) The IEEE Standard 802.16 promises to provide wireless broadband access to homes, businesses and core

telecommunication networks worldwide. However, security is a key concern to the success of IEEE Standard 802.16. Wireless networking is not as secure as other networking technologies. This paper provides a mechanism for increasing the efficiency & hence improves the existing model[8].

Monika rani,, Anil Rose and MridulChawla(2011)New technologies are evolving each day to facilitate human beings. From analog communication to 2G, 2G TO 3G and now we are heading towards WiMAX, atelecommunications protocol that provides fixed and fully mobile internet access. In this paper, we point out several potential security threats and vulnerabilities. We propose some possible security improvements and solutions to eliminate the vulnerabilities using public key cryptography[9].

PrakashKuppuswamy, C.Chandrasekar (2011) this paper deals with a new algorithm, which is based on linear block cipher. Encryption as cipher text use invertible square matrix, blocking the message according to the selected square matrix ie., if the square matrix is 3 x 3 make the message or plain text 3 blocks, and select 'e' as any natural number and multiply with selected matrix and message, use modulation 37, then the remainder is our cipher text or encrypted message[10].

3. PROPOSED STRUCTURE

3.1 RSA Based Authentication Security Layer

WiMAX has a very flexible MAC layer that can accommodate a variety of traffic types, including voice, video, and multimedia, and provide strong QoS. The authentication security using RSA algorithm in IEEE 802.16 MAC layer. The MS acts as the client; the BS, as the server. PKM uses X.509 digital certificates and RSA (Rivest-Shamir-Adleman) public-key encryption algorithms to securely perform key exchanges between the BS and the MS. The MAC layer takes packets from the upper layer, these packets are called MAC service data units (MSDUs) and organizes them into MAC protocol data units (MPDUs) for transmission over the air. For received transmissions, the MAC layer does the reverse. In following figure 2 mentioned the relationship of MAC layer and RSA authentication encryption.

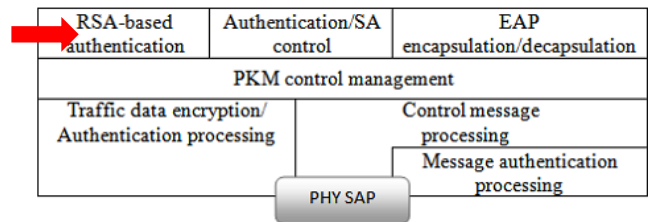


Fig2. RSA based MAC layer in IEEE 802.16

3.2 Nlbc proposed Authentication Security Layer

The proposed new protocol system is fully secure for Message authentication and Private key management. Specifically, the block cipher has been demonstrated that several security requirements are contradicting each other, thus requiring special treatment, while there are requirements that can either not be fulfilled, given the currently available technology, or they can be handled provided that a substantial increase in cost and complexity is accepted. We are proposing here to replace the RSA algorithm with the Nlbc algorithm. The protocol structures of the Nlbc algorithm were as follows:-

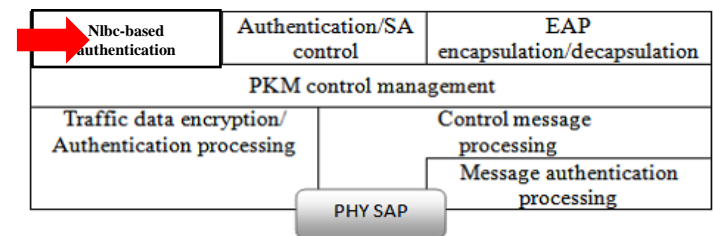


Fig3. Proposed Block cipher MAC layer in IEEE 802.16

Proposed model of handshake identification using Nlbc encryption techniques

- i) Nlbc-Request (SS → BS): MS_Random, MS_Certificate, SAID, SigSS.
- ii) Nlbc-Reply (SS → BS): MS_Random, BS_Random, Encrypted pre-PAK, Key Lifetime, Key Sequence Number, Bs_Certificate, SigBS.
- iii) Nlbc-Acknowledgement (SS → BS): BS_Random, Auth Result Code, Error-Code, Display-String, SigSS

4. IMPLEMENTATION STRUCTURE

In order to securely exchange keys between BS and SS, the PKM protocol uses the symmetric cryptography and X.509 certificates. The protocol is based on three phases. The BS plays the role of the server and it manages identification keys to the SS, who plays the role of client.

The BS authenticates a SS client using PKM protocol in the initial authorization exchange. SS uses a digital certificate for authentication at the BS. Also, the BS uses a shared secret encrypted key, which can be periodically changed by the SS, to communicate with the SS, key provided by PKM protocol.

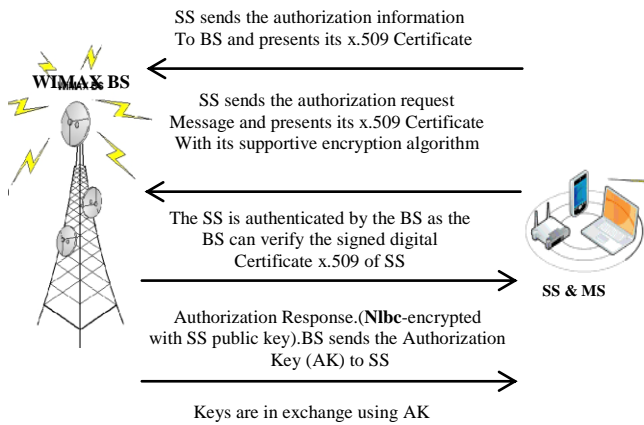


Figure 3. WiMax Security Framework

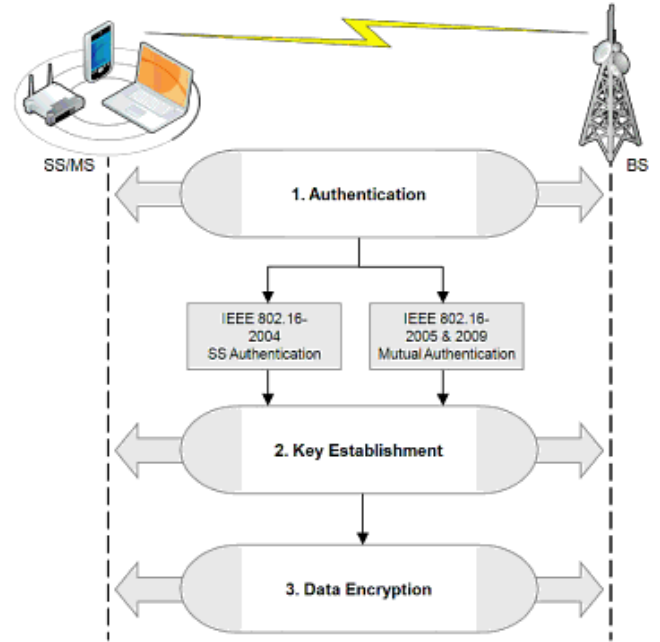


Figure 3. WiMax Security Framework

An essential improvement on WiMAX security mechanism is to add the certificate Chain Request and Certificate Chain Reply messages for enabling a node which will verify the Authorizations-Node-Certificate where the messages complete the Nlbc authentication within the PKM-MSH.

The IEEE 802.16 standard has improved mutual authentication between BS and SS where random numbers are included to stop replay attacks. In order for the handshake identification to be successfully followed the Nlbc based authentication has incorporated its own certificate.

4.1 Key Establishment

4.1.1. RSA

- 1) Firstly find two large primes p and q and compute their product $n = p \times q$.
- 2) Secondly find an integer d that is co-prime to $\phi(n) = (p-1)(q-1)$.
- 3) Compute e from $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$.
- 4) Then broadcast the public key, which is the pair of numbers (e, n) .

4.1.2 Nlbc

- Step 1: Assign the value of $n = 37$
- Step 2: Select invertible matrix i.e “ k ”
- Step 3: “ k ” should be giving the result of $k \cdot k^{-1} \pmod{37} = 1$
- Step 4: Select any integer value and multiply with “ k ” i.e., called “ d ” private key

Step 5: Find inverse of the integer value using mod 37, known as “e” another public key
 Now announce “n” and “e” as public key and k^{-1} , “d” as a private key

4.2 Data Encryption/Decryption

4.2.1 RSA

Now encrypt each message, m, using the public key by applying the rule $C = m^e \pmod{n}$.
 The receiver will decrypts the message using the rule $m = C^d \pmod{n}$.

4.2.2 Nlbc

Multiply message ‘m’ using $k \times k$ square matrix and e value. The equation is $C = (k * m * e) \pmod{37}$
 The receiver will decrypts the message using the rule $m = (k^{-1} * c * d) \pmod{37}$.

5. BENEFITS OF PROPOSED ALGORITHM STRUCTURE

The proposed system is most suitable for data encryption using new cryptographic block cipher schemes of proven robustness to provide privacy. Wi-Fi, WiMAX systems were designed at the outset with robust security in mind. The standard includes state-of-the-art methods for ensuring user data privacy and preventing unauthorized access, with additional protocol optimization for mobility. Security is handled by a privacy sublayer within the WiMAX MAC. The key aspects of WiMAX security are as follow.

- ❖ Support for privacy
- ❖ Device/user authentication.
- ❖ Flexible key-management protocol
- ❖ Protection of control messages
- ❖ Support for fast handover

6. CONCLUSION

Satisfying security requirements is one of the most important goals for all the communication system security designers. Also it will ensure the confidentiality, integrity and authentication. The existing security model uses RSA algorithm for encryption, while the proposed security model of IEEE 802.16 uses New linear block cipher cryptography (Nlbc) encryption algorithm. Proposed algorithm uses smaller key size as compared to RSA. The reason for selecting linear block cipher for our New algorithm; The linear algebra will not produce same kind of result for the repeated text variable. Also, we can construct 2 blocks, 3 block square matrix variable each


and every time, which will secure our algorithm more. We know that the devices in the wireless network are battery driven. Using smaller key, we require low computational time, low computational power and small memory so on.

REFERENCES

- 1) Trung Nguyen, Raj Jain, “A survey of WiMAX security threats”, www.cse.wustl.edu/~jain/cse571-09/ftp/wimax2/index.html, April 2009.
- 2) Yogesh Gedam, Dr. S. D. Chede, “Design and Improvement in WiMAX 3G security using Multiple Keys”, ISSN : 0975-5462 Vol. 3 No. 7 July 2011.
- 3) Mitko Bogdanoski, Pero Latkoski, Aleksandar Risteski, Borislav Popovski, “IEEE 802.16 Security Issues: A Survey”, 16th Telecommunications Forum TELFOR 2008, November 25-27 2008.
- 4) Ayesha Altaf, M. Younus Javed & Attiq Ahmed, “Security Enhancements for Privacy and Key Management Protocol in IEEE 802.16e-2005”, Ninth ACIS International Conference on Software Engineering, 2008.
- 5) T. L. Singal “Wireless communication,” chapter 14 Emerging wireless network technology, Tata McGraw Hill Publication, 2010.
- 6) F. Chee-Da Tsai, J. Cheny, C. W. Chang, W. J. Lien, C. H. Hung, and J. H., “Design and implementation of wimax Module for ns-2 Simulator”, 2006.
- 7) Guo Song Chu, Deng Wang, Shunliang Mei, Communications, Circuits and Systems and West Sino Expositions, IEEE 2002 International Conference on 29 June-1 July 2002.
- 8) Pranita K. Gandhewar, Kapil N. Hande, Performance Improvement of IEEE 802.16 / Wimax Using Elliptic Curve Cryptography, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (3), 2011.
- 9) Monika rani, Anil Rose and Mridul Chawla, Review of Public key cryptography on WiMax using RSA Algorithm, Journal of Engineering Research and Studies, JERS/Vol. II/ Issue IV/October-December, 2011.
- 10) Prakash Kuppaswamy, C. Chandrasekar, “Enrichment of Security through Cryptographic Public key algorithm based on Block cipher”, Indian Journal of Computer Science and Engineering (IJCSE), ISSN : 0976-5166 Vol. 2 No. 3 Jun-Jul 2011.
- 11) Md. Rezaul Karim, Siddiqui and Sayed Mohammad Atiqur Rahman, “Security analysis of the WiMAX

Technology in Wireless Mesh networks”, Master thesis, Blekinge Institute of Technology, Karlskrona, Sweden, 2009.

- 12) Zhang, Y. & Chen, H, “Mobile WiMAX Toward Broadband Wireless Metropolitan Area Networks”, State: Auerbach Publications, 2008.

	<p>Prakash Kuppuswamy, Lecturer, Computer Engineering & Networks Department in Jazan University, KSA. He is research Scholar-Doctorate Degree yet to be awarded by ‘Dravidian University’. He has published 20 International Research journals/Technical papers and participated in many international conferences in Rep. of Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and Network algorithms.</p>
	<p>Sikandhar Shah, Lecturer, Computer Engineering and Networks Department in Jazan University, KSA. He completed MSc Computing and Performance Engineering, from University of Bradford, UK in 2007. Specialization: Network Performance Engineering Areas of Interest: Mobile Adhoc & Wireless sensor networks, Performance Modelling, congestion control, Network Professional: Cisco Certified Network Professional</p>