International Journal of Future Generation Communication and Networking
Vol. 9, No. 2 (2016), pp. 211-218
http://dx.doi.org/10.14257/ijfgcn.2016.9.2.22

ID- Based Authentication for WiMAX

Pushpi Rani1, Brijesh Kumar Chaurasia 2 and Geetam Singh Tomar3

1,2ITM University Gwalior, 3MIR Labs, (M.P.), India
2bkchaurasia@ gmail.com

Abstract

WiMAX is broadband wireless system being used for long range wireless networking, which makes this system vulnerable to security breaches. In this paperwe present authentication scheme using ID-based signature scheme for WiMAX, which offers a certificate-less public key verification. The proposed scheme has also increased message processing throughput as it has used elliptic curve cryptosystem, sigencryption and identity based cryptography.

Keywords: *WiMAX, ID based cryptography, ECC, Security and authentication*

1. Introduction

Worldwide interoperability for microwave access (WiMAX) is a fast growing broadband access technology that enables low-cost mobile internet and multimedia applications [1]. It has the capability to provide services in the area that are not easy to reach for wired infrastructure and the ability to surmount the physical restriction of traditional wired infrastructure. WiMAX is an emergent broadband wireless technology based on IEEE 802.16 standard [2]. The motive behind this technology is to ply fixed broadband wireless access to IP based user, as it is optimal for the distribution of IP centric service over a wide geographical area. The deployment of such rising broadband networks provides opportunities for services models and new applications [3]. It can be anticipated that there are a huge amount of services and new applications will be supplied on these commercial broadband network. WiMAX system provides broadband access avails to the residential and enterprise customer in an frugal way, so it's become very popular and growing vast day by day. Since the wireless medium is available to all, the assaulters can easily admittance to network and the network becomes more vulnerable for the user [4]. Therefore, the security support is highly desired for this system. To understand WiMAX security issues, it is needed to understand WiMAX architecture. The IEEE 802.16 protocol architecture is structured into two main layers: the medium access control (MAC) layer [5] and the physical (PHY) layer [5]. MAC layer is further sub divided into three parts, named as service specific convergence sub layer, MAC common part sub layer and security sub layer [6] depicted by this layered architecture in Figure 1.

ISSN: 2233-7857 IJFGCN

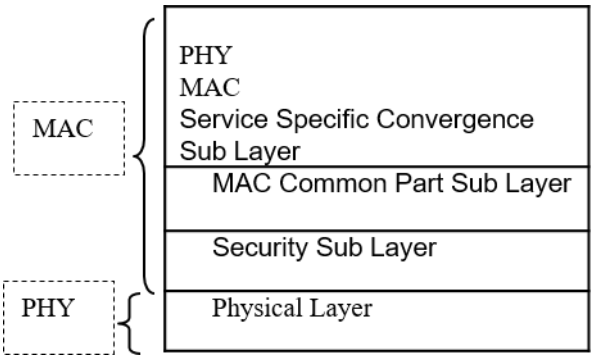

Figure 1. The WiMAX/IEEE 802.16 Protocol Structure

In WiMAX, most of the security issues are addressed and handled in the MAC security sub-layer [5]. The main security issues are authentication, privacy and message integrity. So, mutual authentication of entities such as nodes, service stations along with privacy preservation is needed in WiMAX. It is protected by the security features such as security association and public key infrastructure [5]. Further, WiMAX security level is defined in three parts these are as authentication, authorization and data encryption [7].

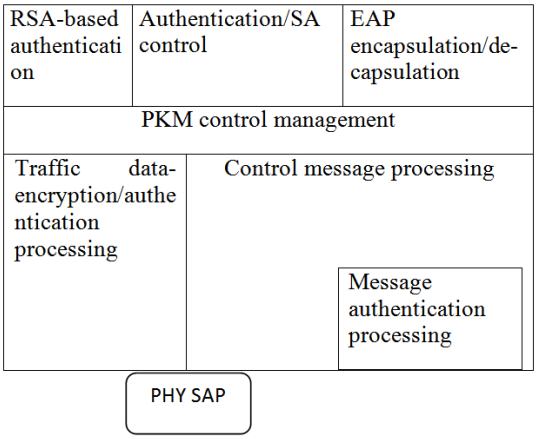

Figure 2 WiMAX/ IEEE 1.6 Protocol Security Structure

It supports three types of authentication which are handled in security sub-layer. The first is RSA based authentication which applies X.509 certificates together with RSA encryption. The second one is extensive authentication protocol (EAP) based authentication in which the service station (SS) is authenticated by an X.509 certificate. The third type of authentication that the security sub-layer supports is the RSA based authentication followed by EAP authentication. These all authentication scheme suffer from the vulnerabilities of secret because the distribution of public key. ID based authentication scheme proposed in this paper overcomes this limitation. This scheme eliminates the burden of the public key infrastructure inherent in certificate based authentication scheme.

The rest of the paper is organized as follows. Section 2 describes the related work. In section 3, proposed scheme is given. Section 4 is presented analytical evaluation and followed by conclusion in section 5.

2. Related Works

In the existing literature, clustering is the most suitable approach to extend network the problem of authentication is well known for ad hoc networks. PKM protocol uses RSA-1024 bit asymmetric key encryption along with one way and three way handshakes techniques to achieve authentication [5]. The extension of PKM and improved secure network authentication protocol (ISNAP) for IEEE 802.16 is presented in [8] and [9]. However, these approaches suffer from the distribution of public keys. The work in [6], addresses privacy preserving mutual authentication in WIMAX. The proposed mutual authentication scheme based on the infrastructure and incurs the low communication cost. Several group signature based authentication scheme is addressed in [10] and [11]. In these schemes, a group manager, who has the group master key, can reveal the identity of the group member and any member can sign the messages anonymously on behalf of the group to achieve anonymity and authentication. Such a signed message is publicly verifiable with the public key of the corresponding group. However, such schemes are setup based. An ID-based ring signature scheme is to achieve privacy protection with signer ambiguity feature presented in [12]. However, this scheme does not support conditional privacy. Further, ID-based batch verification scheme which is based on bilinear pairing is also discussed in existing literature. In this scheme, a pseudo-ID-based one-time signature scheme is used to minimize the transmission and verification cost of public key certificates [13]. Other security framework for VANET using identity-based cryptography (IBC) is presented in [14]. In this scheme, a pseudonym generation mechanism has been presented that exploits the implicit authentication provided by IBC to generate unforgeable, authenticated pseudonyms. This scheme works on identity-based sign encryption which combines signing and encryption operations and at the same time produces smaller cipher text as compared to sign and then encrypt. ID based conditional privacy preservation authentication scheme is presented in [15]. This scheme does not require the special one way hash function, called MaptoPoint function, in both the signature generation and verification processes. Shim's scheme requires heavy computational cost in the signature phase, where three multiplication point operations and three pairing operations are used, as the computational cost of one pairing operation is three or more times that of a one point multiplication operation.

3. Proposed Methodology

In this section, we propose an IBC based authentication mechanism for WiMAX to simplify the certificate distribution problem by using signers' identity information as their public keys.

The proposed identity based signature scheme consists of five algorithms: Setup, Registration, Sign, Verification and Secure Communication. The proposed scheme has these advantages the proposed scheme does not need to use any special one-way hash function, called MapToPoint; and there is no need for pairing operation, the computation cost of which is three or more times than that

of a point multiplication operation used in our scheme. By avoiding the use of pairing operations, our proposed scheme performs better than the other ID-based batch signature schemes. Details of each steps of algorithm are described as follows.

Setup: Let n be a large prime and F_n be the finite field over n, where n is the size of finite field. Let $(a, b) \in F_n$ be the parameters of elliptic curve ($y^2 = x^3 + ax + b \pmod n$, where $4a^3 + 27b^2 \neq 0$) over F_n. Let O denote infinity. Let P be the generator point of E and q be the prime order of P, where $P \neq O$. The private key generator (PKG) randomly chooses a number $s \in Zq$ as its master private key and then computes its corresponding public key $P_{pub} = \mathrm{sP}$. After that, PKG chooses two one-way hash function: H_1: $\{0,1\}^* \rightarrow Z_q$ and H_2: $\{0,1\}^* \rightarrow Z_q$. Next, PKG publishes $\{P, P_{pub}, q, H_1, H_2\}$ as its public parameters and keeps s [19].

Registration:

When a user registers on PKG, this user first sends their chosen identity ID_i to PKG via a secure channel. Upon receiving ID_i from the user, PKG computes

$$K_i = K_i P, \quad (1)$$

$$S_{IDi} = K_i + H_1 (ID_i, K_i) * s \; mod \; q, \quad (2)$$

Corresponding for this identityID_i, where K_i is a random number. After that PKG sends (K_i , S_{IDi}) back to the user via a secure channel.

Sign

Given a message M_i, a signer with an identity ID_i computes

$$R_i = r_i P, \quad (3)$$

$$X_i = H_2(K_i R_i ID_i M_i) * r_i + S_{IDi \; mod \; q}, \quad (4)$$

Where ri is a random number. (K_i, R_i, X_i) is the signature on message M_i for identity ID_i. Notice that R_i can be pre-computed before the signer signs a message M_i.

$$C = SignEncrypt_{K_{Session}}[K_i, R_i, X_i] \quad (5)$$

Where $K_{Session}$ is the secret key between receiver and sender.

Verification

Given a message M_i and its corresponding signature (K_i, R_i, X_i), a verifier can verify that the validity of a signature (K_i, R_i, X_i) with the following equation

$$V_i P = (K_i R_i ID_i M_i) R_i + K_i + H_1(ID_i K_i) P_{pub} \quad (6)$$

If the above equation (6) holds, it means that the signature (K_i, R_i, X_i) is a valid signature; otherwise, the verifier would reject the signature (K_i, R_i, X_i)

Secure Communication

This scheme provides the secret credential for secure communication. The credential includes the master private key, user's identity, message identity and session key between users. Each user, working in the network can easily hide their details and protect them using these credentials. Once the choice is made, they simply validate the identity-based signature on the message to verify the private key and communicate easily.

In the following discussion, we evaluate the computation cost of our identity-based signature scheme as follows. Since the $a_i \in R\{0,1\}^1$ $(i = 1, \ldots . n)$ are small random numbers, we omit the computational cost. In our scheme the signer with an identity ID_i. only needs one hash function operation, one multiplication point operation, and one multiplication operation to construct a signature (K_i, R_i, X_i).on the message M. in the verification process, the verifier only needs two hash function operations and three point multiplication operations to verify the validity of the signature (K_i, R_i, X_i).

5. Analytical Evaluation

To evaluate computation overhead of the proposed scheme, experiments were conducted to compare computation time among with proposed work and related works [17, 18]. Assume the notations,T_P, time for performing a pairing operation, T_M, time for scalar multiplication operation, T_{MP}, time for scalar multiplication point operation. Table I shows the required execution time for different cryptographic operations running on the given experimental platform: Core2duo 2.6 GHz machine with 2 GB RAM. We have evaluated our proposed mechanism by crypto library MIRACL [16]. Let T_H , time for performing MaptoPoint operation. The computation cost of scheme and existing scheme is given in Table II.

Table 1. Execution Time of Cryptographic Operation

	T_M	T_{MP}	T_P
Execution Time (*ms*)	0.03	1.50	8.12

On the basis of above observations, we can state the following facts:

Table 2. Computation Cost of Proposed Mechanism

	Signature generation	Signature Verification
Yoon et *al*. [17]	2 TMP + TH	TMP +TH+ 2TP
EIBS [18]	2TMP	TMP + 2TP +TH
Proposed Scheme	TM	TMP

Yoon scheme, EIBS scheme and proposed scheme can pre-compute the value$R_i = r_i P$ before constructing one signature on a message. Thus, in terms of signature generation, the proposed scheme has better performance than other

existing schemes. The proposed scheme does not require any pairing operation on signature verification and do not require ant MaptoPoint operation.

6. Conclusion

In this paper a ID based authentication mechanism is addressed for security management in WiMAX. The proposed scheme is based on identity-based batch signature scheme and does not use any MaptoPoint operation and pairing operation. Therefore, it is more efficient in terms of computational cost and time consumption. This scheme is supported secret authentication, message integrity, traceability, verification and non-repudiation. The performance analysis indicates that the proposed authentication scheme is faster than other existing scheme. Further, another advantage of this proposed scheme is that no special storage is required for certificates. However, batch verification for n numbers of users in WIMAX is a future scope of this work.

References

[1] K. Etemad, "Overview of Mobile WiMAX Technology and Evolution", In IEEE Communications Magazine, vol. 46, no. 10, **(2008)**, pp. 31-40.
[2] L. Valcarenghi, P. Monti, I. Cerutti, P Castoldi and L Wosinka, "Issues and solutions in Mobile WiMAX and wired Backhaul Network integration", IEEE ICTON-2009, **(2009)**, pp. 1-4.
[3] S.Y. Wang, C.C. Lin, P.H. Koo and Y.M. Huang, "NCTuns emulation Testbed for Evaluating real-life applications over WiMAX Networks", 21st IEEE International Symposium on Personal, Indoor and Mobile Radio Communication, **(2010)**, pp. 2030-2034.
[4] P. Rengaraju, C.H. Lung and Yi Qu, "Analysis on Mobile WiMAX Security", IEEE TIC-STH, **(2009)**, pp.439-444.
[5] S. Dubey and S. Kumar, "Security Issues in WiMAX: A Critical Review", International Journal of Information and Computation Technology, vol. 3, no. 3, **(2013)**, pp. 189-194.
[6] B.K. Chaurasia and S. Verma, "Privacy preserving mutual authentication in WiMAX", International Journal of Information Technology, Communications and Convergence, vol. 2, no. 4, **(2013)**, pp. 308-320.
[7] A. Bhatele, R. Parajuli and B.K. Chaurasia, "5th IEEE International Conference on Computational Intelligence and Communication Networks", **(2013)**, pp. 138-140.
[8] R.M. Hashmii, A.M. Siddiqui, M. Jabeen and K.S. Alimgeel, "Towards Secure WirelessMAN: Revisiting and Evaluating Authentication in WiMAX", In International Conference on Computer Networks and Information Technology (ICCNIT), **(2011)**, pp. 165-173.
[9] J. Huang and C.T. Huang, "Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations", In IEEE International Conference on Communications (ICC), **(2011)**, pp. 1-5.
[10] R. Lu, X. Zhu, P.H. Ho and X. Shen, "ECPP: Efficient Conditional privacy preservation protocol for secure vehicular communications", in Proceeding of IEEE Conference Computer Communication, **(2008)**, pp. 1229-1237.
[11] B.K. Chaurasia, S. Verma and S.M. Bhasker, "Message broadcast in VANETs using Group Signature**",** Fourth International Conference on Wireless Communication and Sensor Networks, **(2008)**, pp. 131-136.
[12] C. Gamage, B. Gras, B. Crispo and A.S. Tanabaum, "An Identity-based Ring Signature Scheme with Enhanced Privacy", Secure Communication and Workshops, **(2006)**, pp. 1-5.
[13] C. Zhang, R. Lu, X. Lin, P.H. Ho and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks", In proceeding of IEEE INFOCOM, **(2008)**, pp. 246-250.
[14] P. Kamat, A. Baliga and W. Trappe, "An Identity Based Security Framework for VANETs", **(2006)**, pp. 1-2.
[15] K.A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks", IEEE Transaction On vehicular technology, vol. 61, no. 4, **(2012)**, pp. 1874-1883.
[16] Shamus Software Ltd. MIRACL, "Multiprecision Integer and Rational Arithmetic C/C++ Library", Online Available at: http://indigo.ie/~mscott.
[17] H. Yoon, J.H. Cheon and Y.Kim, "Batch verification with ID-based signatures", International Conference on Information Security and Cryptology-ICISC 2004, (**2005),** pp. 233-248, 2005.
[18] K.A. Shim, "An ID-based aggregate signature scheme with constant pairing computations", Journal of System Software, vol. 83, no. 10, **(2010)**, pp. 1873-1880.
[19] B.K. Chaurasia and S. Verma, "Secure Pay While On Move Toll Collection through VANET", In International of Computer Standards & Interfaces, Elsevier, vol. 36, no. 2, **(2014)**, pp. 403-411.

Authors

Dr. Brijesh Kumar Chaurasia, He is received his Ph.D. from Indian Institute of Information Technology, Allahabad, India in Privacy Preservation in Vehicular Ad hoc Networks. He is received his M.Tech. Computer Science and Engg. From D.A.V.V., Indore, India. He is a Professor at ITM University Gwalior, India.

Dr. Geetam Singh Tomar, He is Prof. G S Tomar, he received his UG from Institute of Engineers Calcutta, PG from REC Allahabad, and Ph. D. from RGPV Bhopal in electronics engineering and PDF in Computer Engg from University of Kent, Canterbury, UK. He is the Director of Machine Intelligence Research Labs, Gwalior, India and also Director Shri Ram College of Engg and Management, Gwalior. Prior to this he served in Indian Air Force, MITS Gwalior, IIITM Gwalior and other institutes. He also served at Univ of Kent UK and University of West Indies Trinidad & Tobago. He received International Plato award for academic excellence in 2009 from IBC Cambridge UK. He was listed in 100 top educators of the world for 2009 and 2013 and was listed in who is who in the world for 2008 and 2009. He has organized more than 20 IEEE International conferences in India and other countries. He is member of IEEE/ISO working groups to finalise protocols. Delivered Keynote in many conferences abroad. He is chief editor of 5 International Journals and has 01 patent, published more than 155 research papers in international journals and IEEE conferences