IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 14, Issue 3 Ser. II (May. – June. 2019), PP 53-59
www.iosrjournals.org

Security Analysis of Wimax Technology

Stephen Oguta

Abstract: *Wimax technology (IEEE 802.16) carries with it promising security capabilities compared to its predecessors. The IEEE 802.16 standard has high data rates and bandwidths. WiMAX architecture can transmit up to 40mbps of data over a wireless medium. The wireless transmission carries with it a lot of security threats. In order to protect data exchange between the MAC layer and PHY layer WiMAX specifies a security sub-layer at the bottom of the MAC layer. The security sub-layer provides privacy with SS and BS from service hijacking. For providing authentication, data traffic privacy services and key management a PKM protocol defined by the WiMAX MAC as a sub-layer where the PKM protocol is the main protocol work in the security sub-layer. Security improvements have taken place to cub weaknesses in the PKM versions. PKMv1 works by identifying the SS and the BS. PKMv2 comes in handy to carry out mutual authentication between the SS and the BS. This mutual authentication however takes place after the exchange of essential security details of the communicating parties.*

The objective of this conference paper is to highlight security orientation that exists in the WiMAX architecture. Some of the security aspects that shall be dwelt on include authentication keys like AK, KEK, DH and HMAC. These keys are used for authentication, authorization and management information transmission. This paper shall also highlight security vulnerabilities, threats and risks. Even with WiMAX-802.16 enhanced security measures, Mobile WiMAX is still considered vulnerable to network attacks. One such threat is the MITM attack that targets the unencrypted management messages at the Initial Network Entry point be it in Fixed WiMAX (802.16d-2004) or Mobile WiMAX. Possible solutions to security flaws shall also be suggested in this paper. Some solutions to security flaws include mutual authentication, spreading technique for jamming, authentication node spoofing among others. Diffie Hellman algorithm is also highlighted in this paper as a possible method for implementing mutual authentication in WiMAX system.

Key words: *IEEE 802.16, WiMAX, Vulnerabilities, Security threats, Diffie Hellman.*

Date of Submission: 22-05-2019 Date of acceptance: 08-06-2019

I. Introduction

WiMAX-802.16 is an emerging standard that offers broadband wireless access with high bandwidths and transmission rates [1]. However, like all other wireless networks, WiMAX is vulnerable to network attacks that compromise the radio links between the communicating Subscriber Station (SS) and the serving Base Station (BS) [2] [3]. With the integration of mobility in the 802.16e-2005 Mobile WiMAX standard [4], complexities in ensuring secure access to this network are introduced. Mobile WiMAX employs the Privacy and Key Management protocol version 2 (PKMv2) that supports robust mutual authentication mechanisms, the Advanced Encryption Standard (AES) [5] [6] and message confidentiality by of use Hashbased Message Authentication Code (HMAC) or Cipherbased MAC (CMAC).

Unfortunately, even with WiMAX-802.16 enhanced security measures, Mobile WiMAX is still considered vulnerable to network attacks [7]. One such threat is the MITM attack that targets the unencrypted management messages at the Initial Network Entry point be it in Fixed WiMAX (802.16d-2004) or Mobile WiMAX [8] [9] [10]. Communication, in this case, the Initial Network Entry (INE) procedure, creates detailed profiles of the victim Subscriber Station (SS) inclusive of its security settings and associations with the serving Base station (BS), imitates the legitimate station and then modifies the management messages exposing the network to other destructive attacks like replay attacks, masquerade attacks and denial-of-service (DoS) attacks [11].

The MITM attack fools legitimate stations participating in a communication process into operating as if they are still communicating with each other while disrupting the efficient functioning of the network [9]. Protection keys, like Authorization Key (AK), Traffic Encryption Key (TEK), Key Encryption Key (KEK) or HMAC (Message Authentication Key), which are used in security sub layer [12], provide a better security for WiMAX technology. But security risks, threats or vulnerabilities are still available for WiMAX technology. DH protocol algorithm is a tool that ensures that mutual authentication takes place before the exchange of network management information [13]. When implemented in a WiMAX network, DH helps to save SS from a rogue BS.

II. Literature Review

In order to avoid the limitations of traditional wired networks, there have been many efforts to develop wireless technologies. Wireless technology has been developed from 19th century and lots of development done on this respect. Wireless networks are based on the IEEE 802.11 standard [13] [17]. IEEE 802.11 standard was first created in the 2.4 GHz band using protocols defined by the IEEE 802.11b standard [18]. The figure 1.1 below illustrates a WiMAX network. The SS communicate with the BS via wireless connection. The BS is then connected to the core network through long distance communication links like WiMAX, fiber optics or satellite.

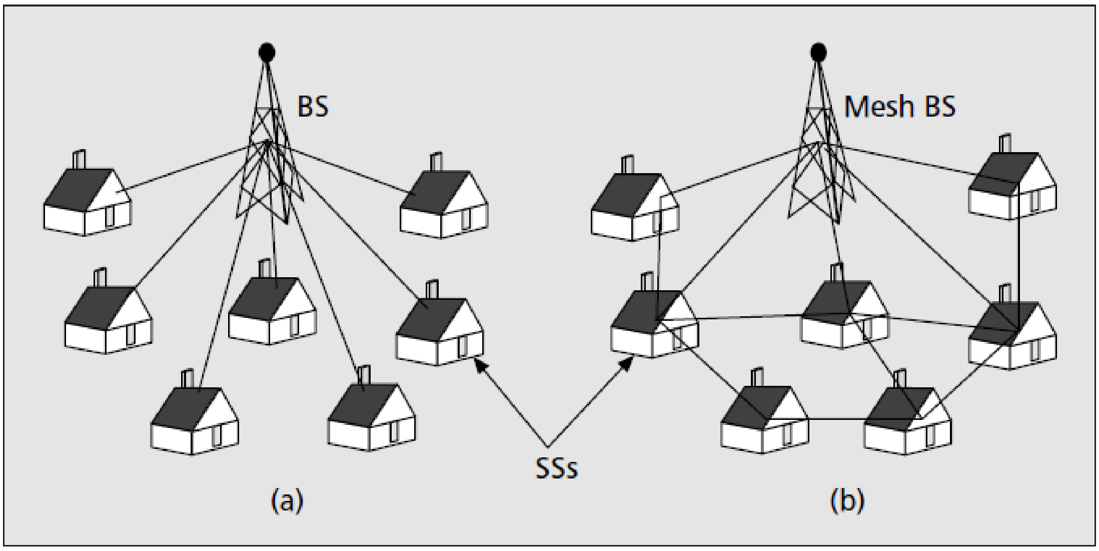

Figure 1.1: WIMAX Network [18]

Two other well-known standards in IEEE 802.11 standard family are IEEE 802.11a and IEEE 802.11g [2] [16]. Though they provide high speed WLAN standard, the coverage area is limited. The IEEE 802.11 standard, commercially known as WiFi, requires a large number of WiFi access points and to connect to a wired node [3] [13] [14]. Due to this reason Institute of Electrical and Electronics Engineers (IEEE) is developing a new standard to provide a large wireless networks [7].

IEEE 802.16 is a standard providing broadband access as an alternative to cable connection [7] [23]. WiMAX is the trade name IEEE 802.16 standard. With the support for Mesh networking, WiMAX systems can be easily configured as a Wireless Metropolitan Area Networks (WMAN) [4] [9] [14]. It has further enhanced the ability of WMANs with mobility support.

Researchers have started to revisit the protocol design for existing wireless network likely IEEE802.11, adhoc and IEEE 802.16 [2] [19]. They are all actively working on new applications for WMANs. EEE 802.16 (2004) provides extended support for NLoS in 2 – 11 GHz spectrum with Mesh network connections. The Figure 1.2 illustrates the WiMAX architecture diagram. The WiMAX protocol architecture is structured into two major layers (see Fig. 2.2): - the MAC layer and the PHY layer.

MAC layer contains 3 sub layers. Starting from the base, the first sub layer is SS which encrypts and decrypts the data which are entering and leaving in and from PHY layer. This sub layer uses for data traffic 56bit DES (Data Encryption Standard) encryption and for Key Exchanges uses 3DES encryption [1]. The second MAC sub layer is the Service Specific Convergence Sub layer (SSCS). This sub layer maps higher level data services to MAC layer service flow and connections [2] [3] [4].

The third sub layer is the Common Part Sub layer (CPS). In this sub layer are constructed the MPDUs (MAC Protocol Data Units). The CPS sub layer defines rules and mechanisms for ARQ (Automatic Repeat Request 10), for connection control and for system access bandwidth allocation. It also provides centralization, channel access and duplexing. CS and CAP are communicated by MAC SAP (Service Access Point) [1]. The PHY layer it's a connection between MPDU and the PHY layer frames with the encoding of the radio frequency signals when sent and received through modulation. WiMAX technology architecture (figure 1.2) was created so as to allow its connection with IP networks which provide Internet services.

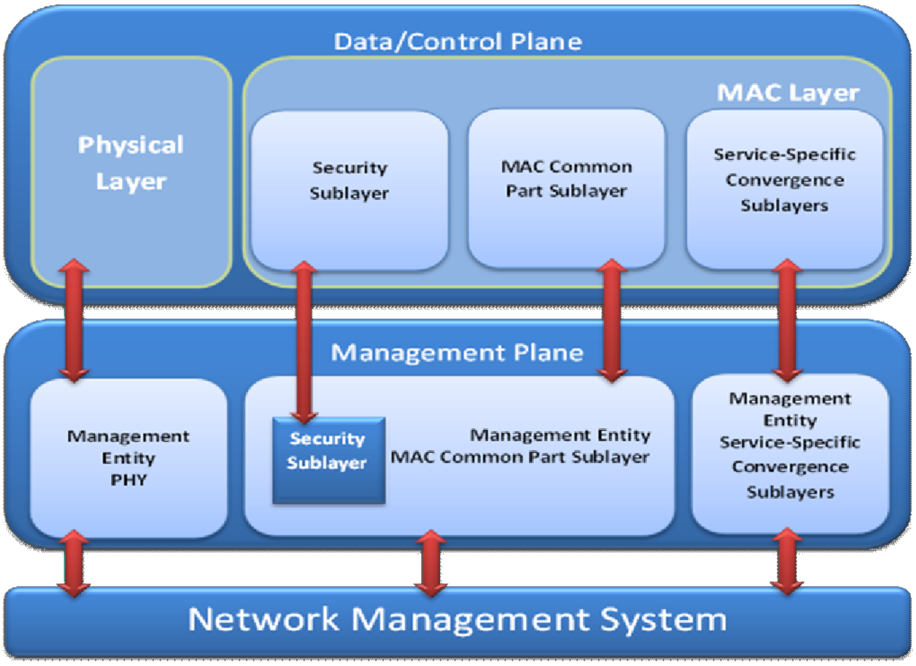
Data/Control Plane
Physical Layer
MAC Layer
Security Sublayer
MAC Common Part Sublayer
Service-Specific Convergence Sublayers
Management Plane
Management Entity PHY
Security Sublayer
Management Entity MAC Common Part Sublayer
Management Entity Service-Specific Convergence Sublayers
Network Management System

Figure 1.2: WiMAX Architecture [1]

III. Theoretical analysis

Pkmv1 Authentication Protocol

SS uses the Authentication Information Message, to push its X.509 certificate which identifies its manufacturer to BS [1] [20]. BS uses this certificate to decide whether SS is a trusted device. BS may use this message in order to allow access only to devices from recognized manufacturers, according to its security policy [21]. SS sends Message 2, named as the Authorization Request immediately after Message 1(figure 1.3) [3]. Message 2 consists of SS's X.509 certificate with the SS public key, its security capabilities which are actually the authentication and encryption algorithms that SS support, and the security association identity (SAID) which is the ID of the secure link between SS and BS [4].

Using the certificate, BS determines whether to authorize SS; and the public key of SS which is also in the certificate lets BS construct Message 3 [1]. If successful, namely SS is authorized after BS verifies its certificate, BS responds with Message 3, the Authorization Reply. This message includes the AK, encrypted using the Rivest, Shamir, and Adelman

(RSA) public-key encryption protocol using the public-key of SS which was obtained in the previous message, the lifetime of the AK as unsigned number in unit of seconds, the sequence number for AK as a 4-bit value and the list of SA descriptors each including an SAID and the SA cipher suit [9].

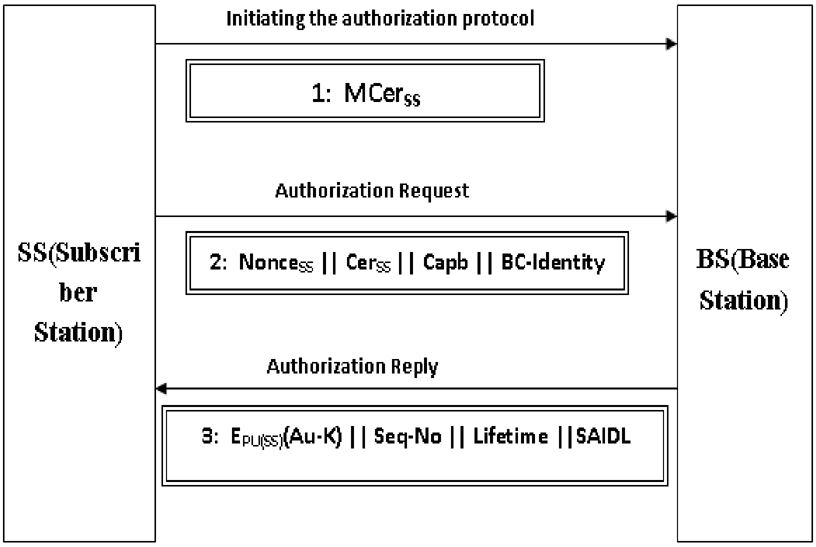
SS(Subscriber Station)
BS(Base Station)
Initiating the authorization protocol
1: MCer_SS
Authorization Request
2: Nonce_SS || Cer_SS || Capb || BC-Identity
Authorization Reply
3: E_PU(SS)(Au-K) || Seq-No || Lifetime ||SAIDL

Figure 1.3: PKMV 1 diagram [3]

Key for figure 2.3

MCer_{ss}	Manufacturer’s certificate of SS
Nonce_{ss}	A number chosen by SS for identification purposes
Cer_{ss}	Certificate belonging to SS
Capb	Security capabilities of SS
BC-Identity	Security capabilities of SS
$\text{E}_{pu(ss)}$(Au-K)	Authentication key features
Seq-$_{\text{NO}}$	Sequence number
Lifetime	lifetime of the AK
SAIDL	Security Association Identity

Pkmv2 Authentication Protocol

The latest standard, IEEE 802.16e-2005, includes a new version (PKMv2) of the protocol that caters for the shortcomings of the first version. PKMv1 does not have a capacity for mutual authentication. Furthermore PKMv2 supports two different mechanisms for authentication: the SS and the BS may use RSA-based authentication or Extensible Authentication Protocol (EAP) -based authentication [21]. This is because the RSA based authentication applies X.509 digital certificates together with RSA encryption. Authentication is therefore made more secure. The flow of messages exchange in RSA-based authentication is shown as follows (figure.1.3) [3]: The SS initiates the RSA-based mutual authentication process by sending two messages. The first message contains the manufacturer X.509 certificate.

The second, authorization request message, contains the SS’sX.509 certificate, a 64-bit SS random number Ns, list of security capabilities that the SS supports, the SAID and the SS signature [22]. If the SS is authenticated and authorized to join the network, the BS sends an authorization reply message. In the response message, the BS includes the 64 bit SS random number Ns received, its own 64-bitrandomnumber Nb, a 256-bit key pre-primary authorization key (pre-PAK) [3] encrypted with the SS’s public key, the prePAK key lifetime and its sequence number, a list of SAIDs (one or more), the BS’sX.509 certificate and BS’s signature in the authorization reply [5].

The SS verifies likeness by comparing the Ns it sent with the received Ns in the authorization response message. It then extracts the PAK, because only the authorized SS can extract the PAK [8].

This can be used as a proof of authorization. Finally, the last message of this authentication is send by the SS to confirm the authentication of the BS [8]. The SS includes the BS random number Nb received in the authorization response message, used to proof likeness, the SS’s MAC address and a cryptographic checksum of the message [12] [17].

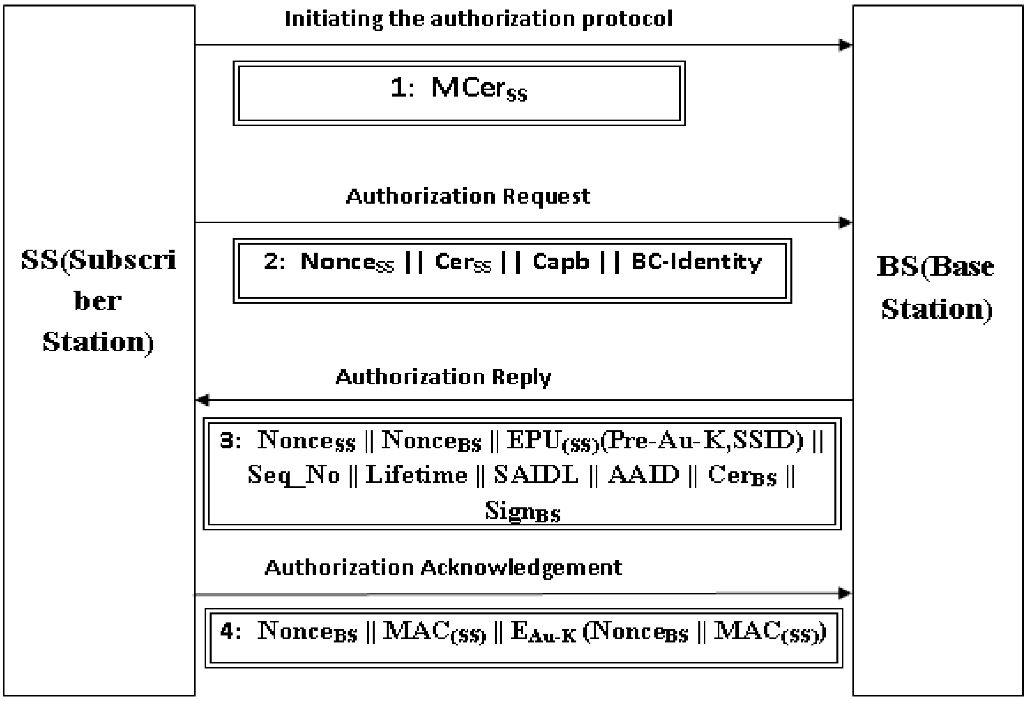
SS(Subscri ber Station)
BS(Base Station)
Initiating the authorization protocol
1: MCer$_{SS}$
Authorization Request
2: Nonce$_{SS}$ || Cer$_{SS}$ || Capb || BC-Identity
Authorization Reply
3: Nonce$_{SS}$ || Nonce$_{BS}$ || EPU$_{(SS)}$(Pre-Au-K,SSID) || Seq_No || Lifetime || SAIDL || AAID || Cer$_{BS}$ || Sign$_{BS}$
Authorization Acknowledgement
4: Nonce$_{BS}$ || MAC$_{(SS)}$ || E$_{Au-K}$ (Nonce$_{BS}$ || MAC$_{(SS)}$)

Figure 1.4: PKMV 2 diagram [17]

MCer$_{ss}$	Manufacturer's certificate of SS
Nonce$_{ss}$	A number chosen by SS for identification purposes
Nonce$_{BS}$	A number chosen by BS for identification purposes
Cer$_{ss}$	Certificate belonging to SS
Cer$_{BS}$	Certificate belonging to BS
Capb	Security capabilities of SS
BC-Identity	Security capabilities of SS
E$_{pu(ss)}$(Au-K)	Authentication key features
Seq-$_{NO}$	Sequence number
Lifetime	lifetime of the AK
SAID	Security Association Identity
MAC $_{(ss)}$	MAC address of SS

Application

PKMv1 AND PKMv2 have security flaw. Mutual authentication takes place in PKMv2 only after the transfer of management information. This is where DH algorithm comes in handy. DH carries out authentication first before the exchange of management information gets transferred. Diffie-Hellman key exchange (DH) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to establish together a shared secret key over an insecure communications channel [21] [23]. Then they use this key to encrypt subsequent communications using a symmetric-key cipher. The scheme was first published publicly by Whitfield Diffie and Martin [24].

The Diffie- Hellman exchange by itself does not provide authentication of the communicating parties and is thus susceptible to a man-in-the-middle attack [20]. A method to mutually authenticate the communicating parties to each other is generally needed to prevent this type of attack [2]. As shown in Figure 1.4, SS sends a request message to the BS that includes the certificate [17]. BS then responds to the challenge. Communication is only allowed when a common answer is obtained between the SS and BS. A nonce is a cryptographic number that is used only once for the purposes of authentication. Being a RSA encryption, P can encrypt nonce and User A can decrypt to receive nonce.

The Diffie-Hellman key exchange protocol [14] [15] [16] originally supports unauthenticated key agreements between stations wishing to communicate. The stations need not know each other's identities to establish a shared secret key through exchanging their public key messages in an open channel. This poses a threat since a malicious station can exchange its own public key with a legitimate base station (BS) or can exchange it with a legitimate mobile station (MS) so as to generate the shared key used for encryption purposes [25]. This compromises the security of the entire WiMAX network and thus entity authentication before implementation of the Diffie-Hellman key exchange protocol is vital as proposed by the authors of [13]. The basic version of the Diffie-Hellman protocol is implemented as described below:

Let

$$PkMS = GN\mathrm{b} \bmod \mathrm{P} \qquad 1.1$$

$$PkBS = GN\mathrm{a} \bmod \mathrm{P} \qquad 1.2$$

Where:

- PkMS is the mobile Station's public key
- PkBS is the base Station's public key
- G and P are global variables called primes numbers
- G is a primitive root of P.
- 'Na' and 'Nb' are the private keys of the MS and the BS respectively.

In the basic version of DH, after the respective exchange of the public keys, the MS and the BS calculate the shared encryption key as shown in the equations 1.1 and 1.2. In order to implement mutual authentication, AS sends Na to BS, BS calculates AKB [11] [18]. BS then sends another unique number Nb to SS. Similarly, SS calculates AKS. If AKS is equal to AKB, AS believes this message sent by BS [8]. The AK in both SS and BS is calculated as follows:

$$AK = GN\mathrm{b} \bmod \mathrm{P} = \mathrm{GNa} \bmod \mathrm{P} \qquad 1.3$$

The above equation 1.3 illustrates the implementation of DH protocol. The first phase of the implementation of the modified Diffie-Hellman protocol towards curbing the MITM attack involves entity authentication of the principals wishing to communicate over the WiMAX network [6]. A mobile station (MS) claiming to be legitimate receives a challenge (Nb) from the serving base station (BS). It calculates the solution to the challenge using its cryptographic function and then sends the result and its identity to the BS [16]. The BS confirms the MS's solution and sends an acceptance token as proof of authentication. Upon receipt, the MS sends a challenge (Na) to the BS which calculates the corresponding solution based on the MS's cryptographic function and sends it to the MS [17].

The MS in turn verifies the solution and sends back an acceptance token to the BS as proof of successful authentication. Finally, successful mutual entity authentication is achieved. In this model, it is assumed that it is only the legitimate BS and the legitimate MS that have knowledge of the cryptographic function used to calculate the challenge sent in the protocol run [19]. Therefore, a perpetrator in the network is not able to bring forth the correct value to the given challenge and is thus isolated as an intruder to the network [14].

Methodology

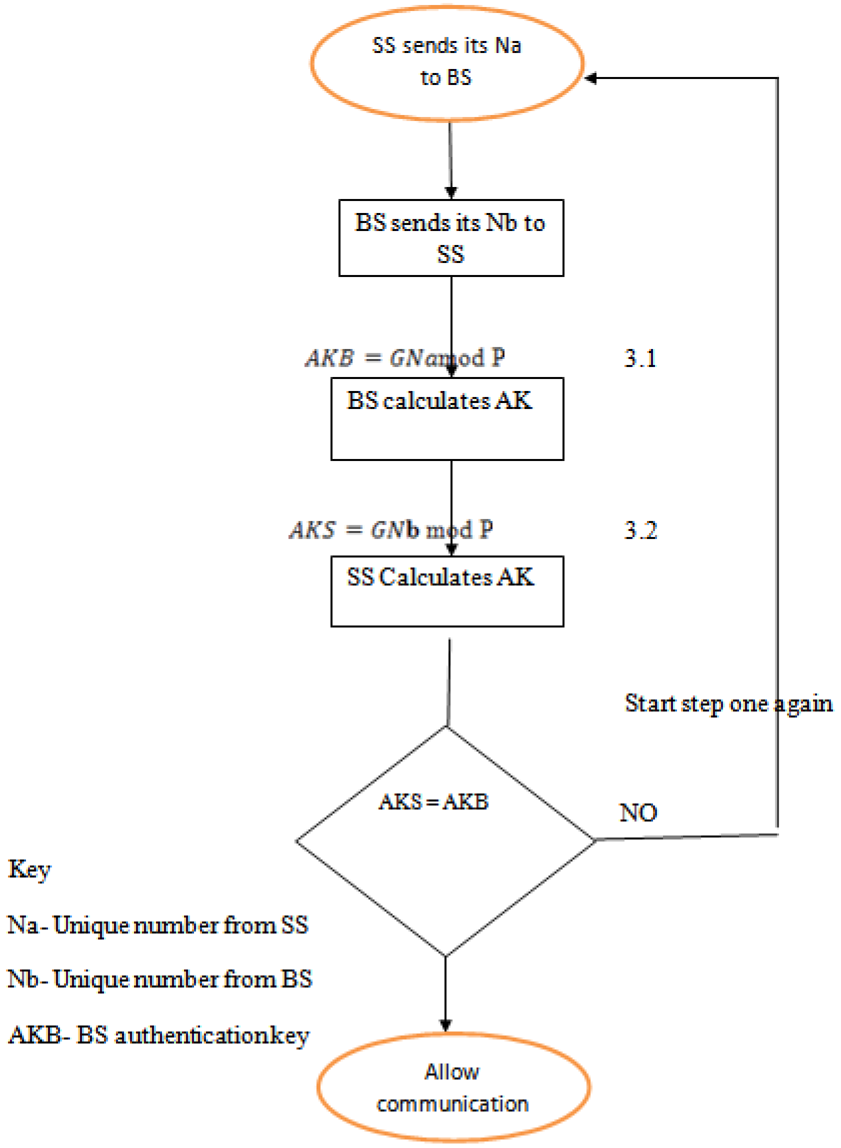

Figure 1.5 above illustrates the implementation procedure of the proposed protocol. The SS sends a number Na to the BS. The BS then sends another unique number Nb to SS. BS calculates a unique authentication key using the number received from the SS. The SS also calculates a unique authentication key using the number received from the BS. The two results obtained from the calculations must be the same for authentication is to succeed. Communication is only allowed if the authentication keys are the same. Otherwise, communication will be terminated if AKS and AKB are not the same.

IV. Conclusion

With the deployment of wireless communication in recent years, security issues in wireless networks also become a growing concern [14] [15]. Privacy or confidentiality is fundamental for secure communication, which provides resistance to interception and eavesdropping. Message authentication provides integrity of the message and sender authentication, corresponding to the security attacks of message modification and impersonation. Message replay attack is one of the most common attacks on authentication and authenticated key establishment protocols [16]. If the messages exchanged in an authentication protocol do not carry appropriate freshness identifiers, then an adversary can easily get himself authenticated by replaying messages copied from a legitimate authentication session.

Even if WiMAX technology has complex authentication and authorization methods and a very strong encryption technique, it is still vulnerable to different attacks or threats like jamming, scrambling, MITM or water torture attacks [8]. Diffie Hellmann protocol algorithm introduces mutual authentication between the BS and SS prior to the exchange of any management information. WiMAX is selected for this research because it is a recent technology and is presently being rolled out in many parts of the world because of its broadband capacities. This technology provides an environment for many gadgets to communicate. A rogue BS can pose as a genuine BS to fool the SS equipments. DH protocol is consequently relevant in WiMAX since it allows for mutual authentication prior to the exchange of sensitive network information. Disruption of communication by an attacker often results into great loses in businesses. Network security is therefore very important.

References

[1]. Z.You, X.Xie, W.Zheng," Verification and Research of a WiMAX authentication protocol Based on SSM", ICETC, pp. 34-43, 2010.

[2]. E.Yuksel," Analysis of the PKMv2 Protocol in IEEE 802.16e-2005 Using Static Analysis", Technical Paper at University of Denmark, pp. 45-54, Feb 2007.

[3]. Z.You, X.Xie, W.Zheng," Verification and Research of a WiMAX authentication protocol Based on SSM", ICETC, pp. 22-32, 2010.

[4]. H.Tseng, R.Hong, W.Yang,"A chaotic maps-base key agreement protocol that preserves user anonymity", IEEE ICC, vol. 3, pp. 67-70, 2009.

[5]. S.Sidharth, M.P.Sebastian," A Revised Secure Authentication Protocol for IEEE 802.16 (e)", International Conference on Advances in Computer Engineering, pp. 34-42, 2010.

[6]. K.C.Chen, J.Boberto and B. De Marca, *Mobile WiMAX*. John Wiley & Sons Ltd, p. 56, 2008.

[7]. K. Jensen, L.Kristensen, L. Wells," Coloured Petri Nets and CPN Tools for Modeling and Validation of Concurrent Systems", Department of Computer Science, pp. 112-122, 2008.

[8]. M.Barbeau, "WiMAX/802.16 Threat Analysis," in *Proceedings of ACM Q2SWinet'05*, Montreal, Quebec, Canada, 2005, pp. 8-15.

[9]. H.Tseng, R.Hong, W.Yang,"A chaotic maps-base key agreement protocol that preserves user anonymity", IEEE ICC, pp.44, 2009.

[10]. J.Huang, C.Tser," Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations", IEEE journal, Vol. 34, issue. 6, pp.45, 2011.

[11]. M.Bogdanoski, P.Latkoski, A.Risteski, and B.Popovski, "IEEE 802.16 Security Issues: A Survey," in *16th Telecommunications forum TELFOR 2008*, Belgrade, Serbia, pp. 123, 2008.

[12]. M.Holbal, T, Welzer," An Improved Authentication Protocol Based on One-Way Hash Functions and Diffie-Hellman Key Exchange", International Conference on Availability, Reliability and Security, 2009, pp. 87.

[13]. R.K.Guha, Z.Furqan, and S.Muhammad, "Discovering Man-In-The-Middle attacks in authentication protocols," in *MILCOM 2007*, Orlando, FL, October 29-31, 2007, pp. 56.

[14]. A.M.Taha, A.T. Abdel, and S.Tahar, "Formal Verification of IEEE 802.16 Security Sublayer Using Scyther Tool," in *IEEE International Conference on Network and Service, N2S '09*, 2009, pp. 1-5.

[15]. P.Narayana et al., "Automatic Vulnerability Checking of IEEE 802.16 WiMAX Protocols through TLA+," in *Proceedings of the 2nd IEEE Workshop on Secure Network Protocols*, November, 2006, pp. 44-49.

[16]. T.Han, N.Zhang, K.Liu, B.Tang, and Y.Liu, "Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions," in *IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 2008, pp. 828-833.

[17]. M. Bogdanoski, P.Latkoski, A.Risteski, B.Popovski," IEEE 802.16 Security Issues: A Survey", Telecommunication forum, 2008.

[18]. F.Leu, Y. Huang, C.H.Chiu," Improving security levels of IEEE802.16e authentication by Involving Diffie Hellman PKDS", International Conference on Complex, Intelligent and Software Intensive Systems, pp. 67-74, 2010.

[19]. K.C.Chen, J.Boberto and B. De Marca, *Mobile WiMAX*. NY: John Wiley & Sons Ltd, pp. 134, 2008.

[20]. E.M. Clarke, O.Grumberg, and D.A. Peled, *Model Checking*. California: The MIT press, 1999, PP. 121.

[21]. E.Liu, K.Huang and L.Jin,"the design of trusted access scheme base on identity for WiMAX network" IEEE computer society (International Workshop on Education Technology and Computer Science), 2009, PP. 66.

[22]. E.Liu, K.Huang and L.Jin,"the design of trusted access scheme base on identity for WiMAX network" IEEE computer society (International Workshop on Education Technology and Computer Science), 2009, PP. 28.

[23]. J.Huang, C.Tser," Secure Mutual Authentication Protocols for Mobile Multi-hop Relay WiMAX Networks against Rogue Base/Relay Stations" IEEE, 2011, PP. 89.

[24]. S.Sidharth, M.P.Sebastian," A Revised Secure Authentication Protocol for IEEE 802.16 (e)", International Conference on Advances in Computer Engineering, pp. 34-42, 2010.

[25]. B. Diffie and M.Hellman, *An overview of Public Key Cryptography*, in IEEE communication magazine, November 1978, vol 16, no. 6.

Stephen Oguta. " Security Analysis of Wimax Technology." IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) 14.3 (2019): 53-59.