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 60-63
www.iosrjournals.org

Diffie Hellman Application in Wimax Security

Mr. S. Oguta, Proff. S. Musyoki and Dr. K. Langat.

(2014). Diffie Hellman Application in Wimax Security.
Corresponding Author: Mr. S. Oguta

Abstract- *The Worldwide Interoperability for Microwave Access (WiMAX) is a new technology which is presently being rolled out. WiMAX defines Privacy Key Management (PKM) protocol in the security sub-layer, which assures the security of connections access in WiMAX channel. PKM protocol has two goals, one is to provide the authorization process and the other is to secure distribution of keying data from the Base Station (BS) to Mobile Station (MS). PKM versions have a security loophole that endangers the network. The network management information is passed in a non-secure environment.*

The Man-In- The-Middle (MITM) attack exploits this weakness in the network by eavesdropping, interception and fabrication of the management messages, resulting in a breach in the reliability of the entire network. In this paper, a modification of the Diffie-Hellman (DH) key exchange protocol is proposed to mitigate the man-in-the middle attack in WiMAX by modeling the protocol in Network. The DH protocol uses a unique algorithm whose solution must be obtained by both the SS and the BS for communication to be allowed. DH provides an opportunity for a secure environment to be created before any communication is done. Exchange of network messages can then be allowed after mutual authentication. This paper will seek to highlight how DH can be implemented in the WiMAX network and consequently guarantee security in communication.

Keywords- *Diffie Hellman, WiMAX, Security, Mutual Authentication*

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).

DH protocol algorithm is a tool that ensures that mutual authentication takes place before the exchange of network management information [3]. When implemented in a WiMAX network, DH helps to save SS from a rogue BS.

II. PKM Versions

In PKMv1, SS uses the Authentication Information Message, to push its X.509 certificate which identifies its manufacturer to BS [1], [2]. 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 [7].

PKMv1 does not have a capacity for mutual authentication. IEEE 802.16e-2005 includes a new version (PKMv2) of the protocol that caters for this shortcoming of the first version. PKMv2 supports two different mechanisms for authentication: the SS and the BS may use RSA-based authentication or Extensible Authentication Protocol (EAP) -based authentication [2]. This is because the RSA based authentication applies X.509 digital certificates together with RSA encryption. Authentication is therefore made more secure. The flow

Stephen Ochieng Oguta, Msc in Telecommunication and Information engineering student at Jomo Kenyatta University of Agriculture and Technology
Proff. S. Musyoki, Senior Lecturer, Department of Telecommunication and Information Engineering at Technical University of Kenya
Dr. K. Langat Senior Lecturer, Department of Telecommunication and Information Engineering at Jomo Kenyatta University of Agriculture and Technology

of messages exchange in RSA-based authentication is shown as follows (figure1) [3]: The SS initiates the RSA-based mutual authentication process by sending two messages.

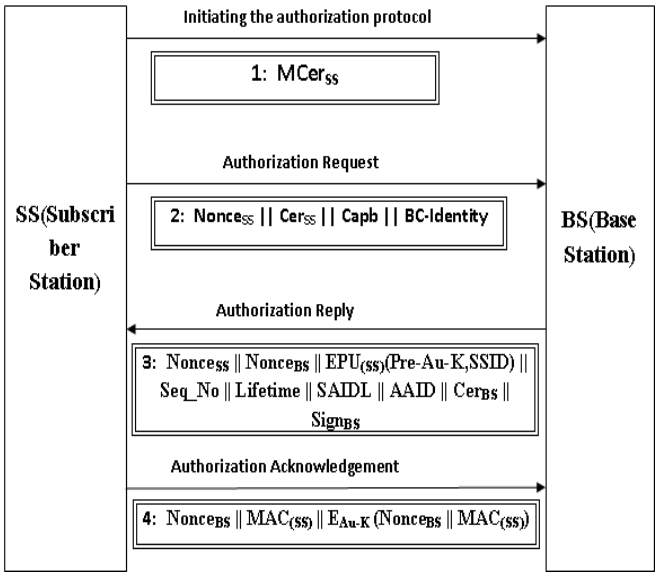

Figure 1: PKMv2 diagram [7]

Key for figure 1
$MCer_{ss}$ 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
$Seq\text{-}_{NO}$ Sequence number
Lifetime lifetime of the AK
SAID Security Association Identity
$MAC_{(ss)}$ MAC address of SS

III. DIFFIE-HELLMAN

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 [1], [3]. 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 [4].

A method to mutually authenticate the communicating parties to each other is generally needed to prevent this type of attack [8]. As shown in Figure 1, SS sends a request message to the BS that includes the certificate [6]. 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 [4] 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. 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 [3].

IV. Equations

The basic version of the Diffie-Hellman protocol is implemented as described below:
Let

$$PkMS = GN\mathbf{b} \bmod \mathrm{P} \quad 1$$

$$PkBS = GN\mathbf{a} \bmod \mathrm{P} \quad 2$$

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 and 2. In order to implement mutual authentication, AS sends Na to BS, BS calculates AKB [1], [7]. 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 [7]. The AK in both SS and BS is calculated as follows:

$$AK = GN\mathbf{b} \bmod \mathrm{P} = \mathrm{GNa} \bmod \mathrm{P} \quad 3$$

The equation 3 illustrates the implementation of DH protocol.

V. Application of the DH

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 [6]. 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 [8].

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 [5]. 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.

Figure 2 below 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.

VI. Conclusion

With the deployment of wireless communication in recent years, security issues in wireless networks also become a growing concern. 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.

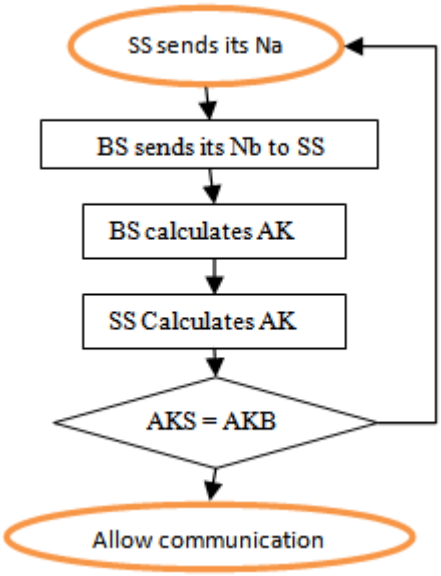

Figure 2: Implementation procedure for DH

Key
Na- Unique number from SS
Nb- Unique number from BS
AKB- BS authentication key

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.

Acknowledgement

S. Oguta would like to thank Dr. S. Musyoki and DR. K. Langat for your guidance and presence during the preparation of this paper. S. Oguta also appreciates his family for their understanding and encouragement.

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

IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) is UGC approved Journal with Sl. No. 4198, Journal no. 45125.

Mr. S. Oguta. " Diffie Hellman Application in Wimax Security." IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) 14.3 (2019): 60-63.