

Mutual Authentication in Wimax Security using Diffie Hellman

Stephen Ochieng Oguta

Msc in Telecommunication And Information Engineering Student At Jomo Kenyatta University Of Agriculture
And Technology (P.O BOX 333, 40222 Oyugis Kenya)

Dr. S. Musyoki

Senior Lecturer, Department Of Telecommunication And Information Engineering At Jomo Kenyatta
University Of Agriculture And Technology (P.O.Box 62000, 00200, Nairobi, Kenya)

Dr. K. Langat

Senior Lecturer, Department Of Telecommunication And Information Engineering At Jomo Kenyatta University
Of Agriculture And Technology, (P.O.Box 62000, 00200, Nairobi, Kenya)

Abstract

Network security is becoming an area of concern with the expansion of wireless technology. Many businesses have lost a lot of money as a result of compromised network security. The Worldwide Interoperability for Microwave Access (WiMAX) is one example of 3G technology which is getting popular. Most business establishments use WiMAX to network their communication equipments. The popularity of WiMAX and its security vulnerability are the key motivation for this study. Presently, PKM versions of authentication are used to secure WiMAX networks. The PKM authentication methods expose the WiMAX network to third party risks like Man in the Middle attacks, eavesdropping and jamming attacks. WiMAX is thus vulnerable to network attacks that compromise the radio links between the communicating Subscriber Station (SS) and the serving Base Station (BS). The PKMv1 process involves a one sided authentication. The BS authenticates the SS but the SS has no capacity to authenticate a BS. As a result, a rogue BS can successfully enter the network of a SS without prevention. The rogue BS can then tap all the unencrypted management messages. This constitutes a major security flaw. 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 research, a modification of the Diffie-Hellman (DH) key exchange protocol is used to mitigate the man-in-the middle attack in WiMAX by modeling using the Dev C++ programming language. The DH protocol uses a unique algorithm whose solution must be obtained by both the SS and the BS for communication to be allowed. Both the BS and the SS are given an opportunity to authenticate one another before any communication can proceed.

Keywords: Diffie Hellman; Mutual Authentication; Security; WiMAX.

1 INTRODUCTION

With the deployment of wireless communication in recent years, security issues in wireless networks also become a growing concern [1] [2]. The Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineers Task Force (IETF) has proposed security mechanisms and protocols to countermeasure security breaches in a way that minimizes the damage which may be caused by the attacks [4]. 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]. Privacy or confidentiality is fundamental for secure communication, which provides resistance to interception and eavesdropping. Man-in-the-middle attack is another classic attack and is generally applicable in a communication protocol where mutual authentication is absent. Other familiar attacks include parallel session attack, reflection attack, interleaving attack, attack due to type flaw, attack due to name omission, and attack due to misuse of cryptographic services. PKM V1 and PKM V2 have been used in WiMAX for security purposes [3]. The above versions only secure the data being transferred. It also secures the BS. The MS/SS is however left vulnerable to rogue BS [4]. The rogue BS can tap the management messages before the actual passing of transmitted data. This paper addresses the weaknesses in WiMAX security system and consequently illustrates how DH can help improve the WiMAX network security. MITM takes advantage of the absence of mutual authentication to pose threats to the system [3].

1.1 Objective

The main objective of this paper is to highlight the application of DH algorithm in WiMAX mutual authentication

2 DIFFIE HELLMAN ALGORITHM

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. However, the exchange of vital management information is done before securing the network. In the PKMv2, the BS asks the SS for its certificates and manufacturing IDs. The BS also sends its management information details to SS in the public environment. Such vital information can be tapped by a rogue Station. 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.

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

Let

$$PkMS = GNb \text{ mod } P \quad 1$$

$$PkBS = GNa \text{ mod } P \quad 2$$

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 [6], [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 [8]. The AK in both SS and BS is calculated as follows:

$$AK = GNb \text{ mod } P = GNa \text{ mod } P \quad 3$$

The equation 3 illustrates the implementation of DH protocol.

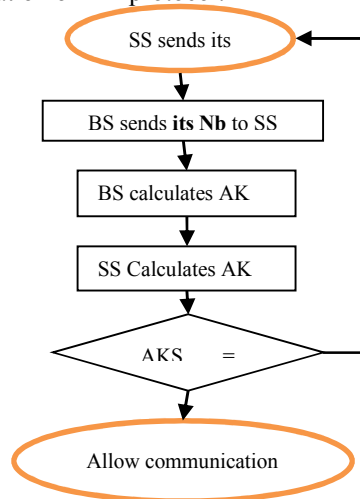


Figure 1: Implementation procedure for DH

Key

Na- Unique number from SS

Nb- Unique number from BS

AKB- BS authentication key

3 The Diffie Hellman mutual authentication code

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 [2] [5]. 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].

Figure 3.1 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 will be terminated if AKS and AKB are not the same. The mutual authentication code for DH protocol is programmed in Dev C ++ as shown in the code at the appendix section. The following code is written

in Dev C++. This program has the mutual authentication functions that illustrate DH algorithm.

4. RESULTS AND DISCUSSION

Dev C ++ allows for the demonstration of DH mutual authentication. The above code is written to help a BS and an SS to communicate one to another and in the process establish a shared authentication key that is later used to access the network [1]. The Responder commits to a protocol session with the Initiator if, and only if, it has correctly finished the session with the Initiator. The Responder will only commit to the Initiator if the latter is correctly authenticated by the Responder and the same applies to the Initiator, if it correctly validates the identity of the Responder as expressed in the challenge response process of the model. In the equations above, Nb is the nonce generated by the Responder, while Na is the nonce generated by Initiator.

Equation 3 explains that a shared authentication key must be obtained if two parties are to communicate. The results obtained in figure 2 below show the mutual authentication process. The SS selects its first number to be used in the DH algorithm. This number is used to obtain that calculation result. The result is then sent to BS in a public non secured environment [4]. The BS equally selects its number then sends the result of calculation. The two equipments only arrive at the same solution to the algorithm if they have the right formula. A wrong result is obtained if an equipment has a wrong algorithm. This translates to a MITM. Suspicious equipment can never get the right solution to the challenge because the algorithm is only known to legitimate BS and SS [8]. A legitimate station will always get the correct solution to the algorithm challenge. It is also necessary to have more than one trial on the algorithm challenge. This means that a legitimate station can sometimes miss the correct choice of number in the initial attempt. DH algorithm helps two stations which have no prior knowledge of one another to establish a common authentication key. System details can then be exchanged once the shared authentication key is obtained.

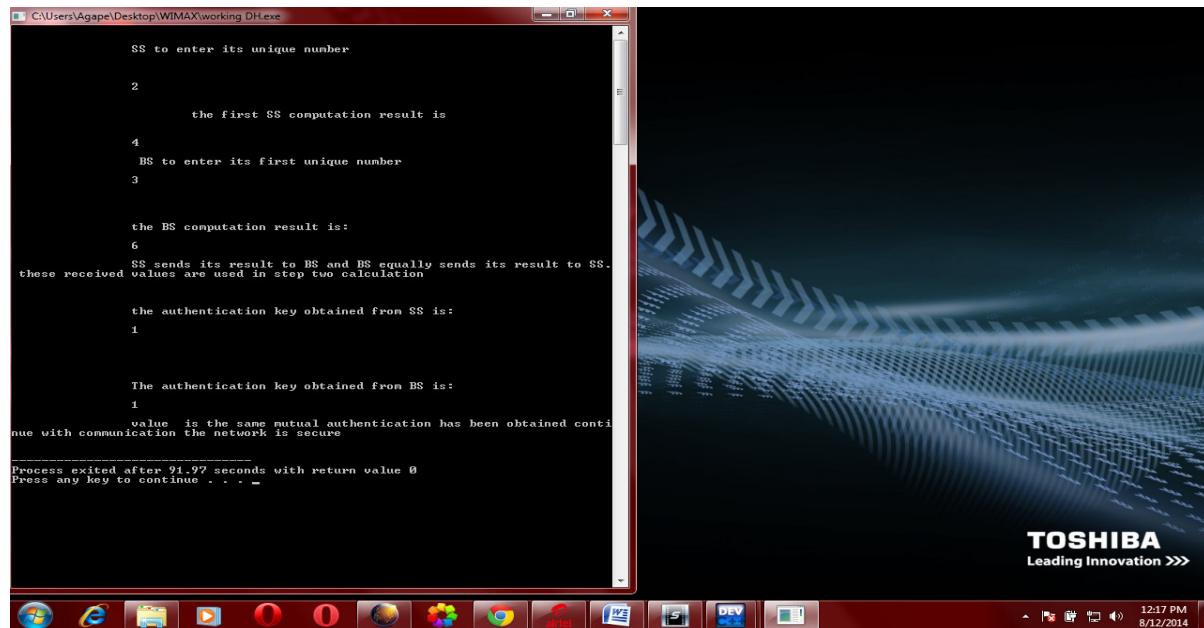
5. CONCLUSION

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. 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].

The results show that the DH protocol works to keep away any intruder in the network. The goal of DH is to carry out mutual authentication. The process of solving the algorithm is complex and only known by the legitimate communication gadgets. Any MITM is kept at bay since they do not have the knowledge of the protocol. 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. Further research is needed on the actual implementation of DH protocol in new mobile devices like smart phones and I pads.

V. 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.



```
C:\Users\Agape\Desktop\WiMAX\working\DH.exe

SS to enter its unique number
2
the first SS computation result is
4
BS to enter its first unique number
3

the BS computation result is:
6
SS sends its result to BS and BS equally sends its result to SS.
these received values are used in step two calculation

the authentication key obtained from SS is:
1

The authentication key obtained from BS is:
1
value is the same mutual authentication has been obtained conti
nue with communication the network is secure

Process exited after 91.97 seconds with return value 0
Press any key to continue . . .
```

Figure 2: Results of compilation

VI. ABOUT THE AUTHORS

Stephen Ochieng Oguta, Msc in Telecommunication and Information engineering student at Jomo Kenyatta University of Agriculture and Technology

Dr. S. Musyoki, Senior Lecturer, Department of Telecommunication and Information Engineering at Jomo Kenyatta University of Agriculture and Technology

Dr. K. Langat Senior Lecturer, Department of Telecommunication and Information Engineering at Jomo Kenyatta University of Agriculture and Technology

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," Colored Petri Nets and CPN Tools for Modeling and Validation of Concurrent Systems", Department of Computer Science, pp. 112-122, 2008.
- [9] D. Gollmann. *Computer Security Second Edition* West Sussex, England: John Wiley & Sons, Ltd, 2006. Pp. 45.

Appendix Implementation Code:

```
#include <iostream>
#include <math.h>
using namespace std;
int main ()
{
cout << "\n\n\t\t" ;
    int g, a, p, b, b2, A, X, B, Y, C, D, E, F, K1, K2 ;
    cout << "SS to enter its unique number\n\n";
    g = 5;
    p = 7; // the SS and BS agree to use same values of g and p. such an agreement is set at the point of
manufacture
cout << "\n\n\t\t" ;
    cin >> a ; // the SS selects its unique number for computation
    cout << "\n\n\t\t\t" ;
    A = pow (g, a);
    cout << "the first SS computation result is \n\n\n\t\t" ;
    B = A % p ;
    cout << B ; // this is the value obtained by the SS
    cout << "\n\n\t\t";
    // X is then sent by the SS across the network to the BS.
    cout << " BS to enter its first unique number \n\n\t\t" ;
    cin >> b ; // BS selects its unique number for computation
    cout << "\n\n" ;
    C = pow (g, b) ;
cout << "\n\n\t\t" ;
D = C % p;
    cout << "the BS computation result is: \n\n\t\t";
    cout << D ;
    cout << "\n\n\t\t" ;
    cout << "SS sends its result to BS and BS equally sends its result to SS. these received values are used in
step two calculation \n\n" ;
    E = pow (D, a) ;
    cout << "\n\n\t\t" ;
    K1 = E % p ;
    cout << "the authentication key obtained from SS is: \n\n\t\t" ;
    cout << K1 ;
    cout << "\n\n" ;
    F = pow (C, a);
    cout << "\n\n" ;
    K2 = F % p ;
    cout << "\n\n\t\t" ;
    cout << "The authentication key obtained from BS is: \n\n\t\t" ;
    cout << K2;
        cout << "\n\n\t\t" ;
        if ( K1 == K2)
        {
    cout << "value is the same mutual authentication has been obtained continue with communication the network is
secure\n\n\n\t\t" ;
        }
        else
        { cout << " mutual authentication not obtained. try again\n\n\t\t" ;
    cout << "SS to enter its unique number for second attempt \n\n\t\t";
        }
}
```