A DH-DSS Based Approach to Improve Mobile WiMAX Security against DoS Attack

Zeinab Kalantari
Department of Computer Engineering
Islamic Azad University - Rafsanjan Branch
Rafsanjan, Iran
zeinab.kalantari@gmail.com

Maryam Shojaei
Department of Computer Engineering,
University of Isfahan
Isfahan, Iran
shojaei.maryam@gmail.com

Abstract—The convenience of IEEE 802.16-based wireless access networks has led to widespread deployment of this technology. Although IEEE 802.16 has added a security layer, there are some security flaws which lead to some serious threats. Unsecure initial network entry, handover process and sleep mode in IEEE 802.16e based networks can result to DoS attack, which is a great security threat to wireless networks. In this paper we propose a DH-DSS (Diffie Hellman-Digital Signature Scheme) method to provide more security in the initial network entry process. The proposed solution is more efficient in terms of bandwidth and computational costs. We first give an overview of security of mobile WiMAX networks. Then we investigate DoS vulnerabilities toward IEEE 802.16 based network and propose a method for a secure initial network entry.

Keywords-Initial network entry, Hand over, DoS attack, DH-DSS, WiMAX Security

I. INTRODUCTION (HEADING 1)

This Mobile WiMAX technology is considered as one of the promising wireless technologies because it can support high-speed, broadband data transmission, fully-supported mobility, wide coverage and high capacity. Of these, Mobile WiMAX has many advantages and unique characteristics such as superior performance (multiple handoff mechanisms, power-saving mechanisms, advanced Quality of Service and low latency, advanced Authentication, Authorization, Accounting functionality), flexibility (global roaming, deployment from the edge infrastructure to overlay/complement networks, various spectrum usage), advanced IP-based architecture (fully support Internet Multimedia Subsystem, 3GPP2, and Multichannel Multipoint Distribution), attractive economics (open standards, mass adoption of subscriber units, attractive Intellectual property rights structure) [1-4].

Broadband wireless access security becomes more complicated when wireless devices are added to the network. Threats are ranked according to the level of risk they present. In wireless network environment DoS attacks have been identified as a principal threat [5]. In WiMAX networks initial network procedure, hand over process and sleep mode are not effectively secured that makes Dos attacks possible [6]. In this paper we first briefly review DoS vulnerabilities in IEEE 802.16e. Then we explain three deficiencies which may result to DoS attack, the initial network entry process, hand over process and sleep mode. In section 3 we discuss the related works. Then we propose a DH-DSS method for a secure initial network entry. Finally we draw conclusion in section 5.

II. DOS VULNERABILITIES IN IEEE 802.16

Denial of Service (DoS) attack has been identified as a major threat to network services. Denial of Service (DoS) attack is an event in which a subscriber is deprived of the service of a resource they would normally expect to have. This attack exploits the transient behavior of a system and gradually reduces the system capacity or service quality. Almost all the DoS vulnerabilities in Mobile WiMAX networks are due to unauthenticated or unencrypted management messages. We discuss these vulnerabilities in three processes: the initial network process, resource saving process and handover process.

A. Handover Process

Mobile WiMAX supports mobility and handover. The handover process is shown in Figure 1. In handover process an MS migrates from the air-interface provided by one BS to the air-interface provided by another BS.

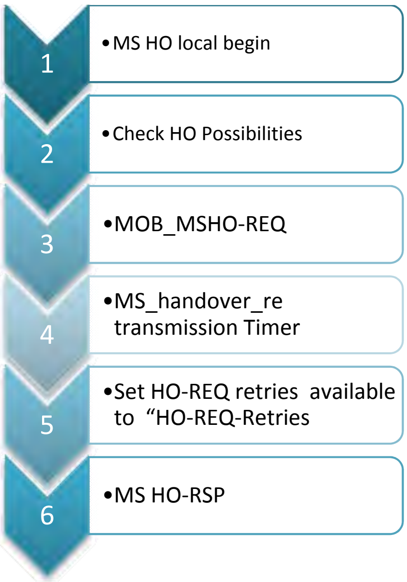
1
•MS HO local begin
2
•Check HO Possibilities
3
•MOB_MSHO-REQ
4
•MS_handover_re transmission Timer
5
•Set HO-REQ retries available to "HO-REQ-Retries
6
•MS HO-RSP

Figure 1: MS initiating HO with the BS

Thus, a BS can send advertisement management messages to its neighbors periodically to identify the network and define the characteristics of neighbor BS to potential SS that is seeking handover possibilities. Since this message is also unauthenticated a DoS attack may occur [6].

B. *Initial Network Entry Process*

In the initial network entry process, the SS sends a Ranging Request (RNG-REQ) message to BS, seeking to join the network. The message contains some information needed to connect to network. The BS responds to the SS request using a Ranging Response (RNG-RSP) message [1]. This message also consists of important information. However, the RNG-RSP message is neither encrypted nor authenticated, and it is stateless [6]. Attacker would take advantages of this leak to implement a DoS attack. The network entry procedure is shown in figure 2.

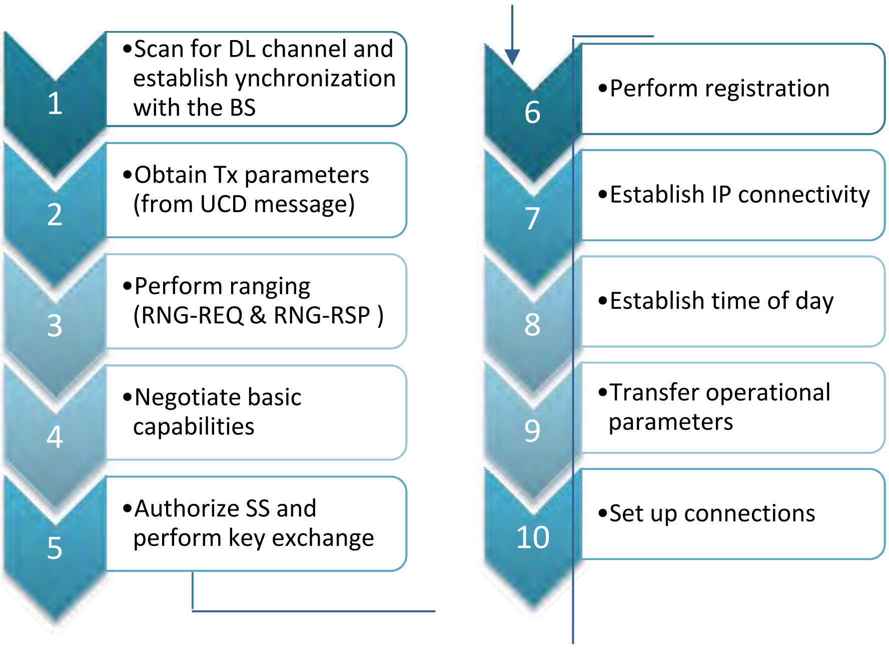
1
•Scan for DL channel and establish ynchronization with the BS
2
•Obtain Tx parameters (from UCD message)
3
•Perform ranging (RNG-REQ & RNG-RSP)
4
•Negotiate basic capabilities
5
•Authorize SS and perform key exchange
6
•Perform registration
7
•Establish IP connectivity
8
•Establish time of day
9
•Transfer operational parameters
10
•Set up connections

Figure 2: Initial Network Entry Process

Implementation of phase 5 is optional. This phase shall be performed if both SS and BS support Authorization Policy. Implementation of phases 7, 8, and 9 at the SS is optional [1]. These phases shall only be performed if the SS has indicated in the REG-REQ message that it is a managed SS.

C. *Resource Saving Process*

Mobile WiMAX minimizes the SS's power consumption and decreases usage of BS air interface resources by presenting the sleep mode. In Sleep mode an SS administers pre-negotiated periods of non-attendence from the

BS air interface. The messages transmitted in this process are not authenticated, So two potential DoS attacks may occur and threaten the network. The first, in sleep mode the SS may be set in bandwidth request and uplink sleep control messages and an attacker may send the bandwidth request and uplink sleep control message with the ID of the victim SS. As a result, the BS will stop transmitting messages to that SS, so DoS attack. Occur. The second, the BS may also send Traffic Indication Message to an SS indicating a sleeping SS that the traffic is sending to it. Therefore, the SS is waked up from sleep mode. An adversary could generate this message to frequently wake up MSs and exhaust victim SS's battery. Then the victim cannot communicate with others until it refreshes its battery, thus performing a DoS attack [6].

III. RELATED WORKS AND BACKGROUND

DoS attacks are one the crucial vulnerabilities towards the networks and Internet that the adversaries can exploit and attack the network. Therefore, over the years, a plethora of research has been reported in the area of DoS attack and defense mechanisms in this field. In mobile WiMAX networks many researchers also have studied the DoS vulnerabilities of this protocol and proposed solutions. Tao et al. analyzed DoS attack in mobile WiMAX networks and proposed the Diffie – Hellman key exchange algorithm [6]. Pranita and Gandhewar studied the initial network entry process and proposed using the Diffie-Helman Elliptic Curve key exchange algorithm, because this protocol is much faster than the Diffie-Hellman key exchange protocol [11]. Reena et al. in [12] analyzed and studied IEEE 802.16e security vulnerabilities. Among them they also studied security deficiencies resulted to DoS attack both at physical layer and MAC layer, but they didn’t provide any solution. In [8] Bart proposed using Timestamp approach along with Signature of BS and SS for Authentication, but Addition of Timestamp and Signature requires modification in Standard. In [9] Georgios et al. also studied deficiencies of PKMv2 that leads to DoS attack. In this work we are going to study three vulnerabilities leading to DoS attack that we can use the same solution for all of them.

IV. PROPOSED SOLUTION

In mobile WiMAX networks in order to prevent DoS attack or at least reduce its vulnerabilities, it is highly recommended that messages communicated between BS and SS in the initial network entry and handover process be authenticated. Therefore by securing the initial network entry and handover procedure, DoS attacks would be largely prevented and the security level of the network will enhance. We developed an Elliptic Curve-Diffie Hellman (DH) key exchange that can be securely integrated into a digital signature scheme (DSS) to enable an authenticated key agreement between the SS and the BS in the initial network entry, handover and sleep mode. In this kind of DH-DSS protocols ephemeral public keys are first signed using a DSS for authentication purposes and then used in a DH key agreement to derive a fresh session key.

As a step towards an efficient protocol design, we show how a DH key exchange can be securely integrated into a DSS. The idea of integrating a DH key exchange into a DSS was first proposed by Arazi [7]. The integration, as first proposed by Arazi, saves one costly computation step and significantly reduces the bandwidth [7]. The proposed solution is more efficient in terms of bandwidth and computational costs than Elliptic Curve-Diffie Hellman protocols by providing a theoretical analysis. The Diffie-Hellman algorithm is illustrated in figure 3. In figure 4 it is explained how the digital signature will sign the key.

Diffie-Hellman & Digital Signature Algorithms Parameters

Global parameters:

***p*:** a prime number, $|p| = 512 \sim 1024$ (bits), multiple of 64
***q*:** a 160-bit prime factor of (p-1)
***h*:** $1< h < p\text{-}1$
$\boldsymbol{g} = (h(p\text{-}1)/q) \bmod p$
H( ): a hash function,

SS’s Private Parameter:
x, random integer with $0 < x < q$

SS’s Public Parameter:
$\boldsymbol{y} = g^{x} \bmod p$
***m*:** message

Per-Message Secret Parameter:
***k*:** random integer with $0 < k < q$

Figure 3: Diffie-Hellman Algorithm Parameters

Signing & Verifying

Signing (SS)
r **=** $(g^k \bmod p) \bmod q$
s **=** $[k^{-1}(H(m) + xr)] \bmod q$; ps: $[(k^{-1})k] \bmod q = 1$
=>
signature = *(r,s)*

Verifying (BS)

w = $(s)^{-1} \bmod q$
u1 = $[H(m)w] \bmod q$
u2 = $(r)w \bmod q$
v = $[(g^{u1}y^{u2}) \bmod p] \bmod q$
Test v ?= r

Figure 4: Digital Signature Algorithm Parameters

According to [10] Diffie-Hellman is exposed to key attack. So we use a key exchange protocol which is more secure than DH key exchange protocol. In figure 5 it is shown how a secured key exchange protocol is used to enhance the security of the mentioned procedure mobile WiMAX network security.

Integrated Diffie Hellman – Digital Signature Scheme Protocol

SS
Select random Integers v1, v2
$\mathbf{m_A}$ = g^{v1} mod p
$\mathbf{n_A}$ = $(\mathbf{y_A})^{v2}$ mod p
$\xrightarrow{(\mathbf{m_A}, \mathbf{n_A})}$ **BS**

Select Random Integers w1, w2
$\mathbf{K_{AB}}$ =$(m_A)^{X_B.W1}$ mod p = $g^{X_B.v1.w1}$ mod p
$\mathbf{K_{BA}}$ = $(n_A)^{w2}$ mod p = $g^{X_A.v2.w2}$ mod p)
$\mathbf{m_B}$ = $(y_B)^{w1}$ mod p
$\mathbf{n_B}$ = $(g)^{w2}$ mod p
$\mathbf{r_B}$ = n_B mod q
$\mathbf{s_B}$=$(w2)^{-1}$ (H (m_B || K_{BA} || K_{AB}) + x_B r_B)) mod q

SS $\xleftarrow{(\mathbf{m_B}, \mathbf{n_B}, \mathbf{s_B})}$
$\mathbf{K_{AB}}$ = $(m_B)^{v1}$ mod p = $g^{x_B.v1.w1}$ mod p
$\mathbf{K_{BA}}$ = $(n_B)^{x_A.v2}$ mod p = $g^{X_A.v2.w2}$ mod p)
$\mathbf{r_B}$ = n_B mod q
Verify DSA Signature ($\mathbf{r_B}$, $\mathbf{s_B}$)
$\mathbf{r_A}$ = m_A mod q
$\mathbf{s_A}$=$(v1)^{-1}$ (H (m_A || K_{AB} || K_{BA}) + x_A r_A)) mod q
$\xrightarrow{(\mathbf{s_A})}$ **BS**

$\mathbf{r_A}$ = m_A mod q
Verify DSA Signature ($\mathbf{r_A}$, $\mathbf{s_A}$)

Figure 5: Integrated Diffie-Hellman Digital Signature Scheme

V. CONCLUSION

Although in comparison to other wireless networks IEEE 802.16e has provided more security, it still suffers some security vulnerabilities and deficiencies. There are some vulnerability both in physical and MAC layer which lead to DoS attack. In this paper we studied three deficiencies that the attackers can exploit to attack the network and all these three vulnerabilities can use the same solution to prevent DoS attack. We used a Diffie Hellman Digital Signature Scheme key exchange protocol to improve the network security. Since wireless channels are constrained in their bandwidth and most mobile devices are constrained in their computational power, memory space and battery lifetime, the proposed solution is more efficient in terms of bandwidth and computational.

VI. References

[1] The Institute of Electrical and Electronics Engineers. IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum, IEEE Std 802.16e-2005. IEEE (2005)

[2] WiMAX Forum: Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation (2006) Available at http://www.wimaxforum.org

[3] WiMAX Forum: Mobile WiMAX: The Best Personal Broadband Experience! (2006), Available at http://www.wimaxforum.org

[4] The Institute of Electrical and Electronics Engineers: IEEE Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems, IEEE Std 802.16-2009. IEEE (2009)

[5] Nasreldin, M., Aslan, H., El-Hennawy, M., El-Hennawy, A.: WiMAX Security. In: 22 International Conference on Advanced Information Networking and Applications, IEEE (2008)

[6] Han, T. Zhang, N. Liu, K. Tang, B. Liu, Y. : Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions. IEEE, 1-4244-2575-4/08/ (2008)

[7] Hoeper, K. and Gong, G. : Efficient Key Exchange Protocols for Wireless Networks and Mobile Devices, Technical Report, CARR 2005.

[8] Sikkens, B. : Security Issues and IEEE802.16. WiMAX8thTwente Student Conference on IT, Enschede, (2008)

[9] Brown, J. : Towards Efficient and Secure Rekeying for IEEE 802.16e WiMAX Networks, publish in the IEEE "GLOBECOM". (2009)

[10] Liu, J. Li, J. : A Better Improvement on the Integrated Diffie-Hellman-DSA Key Agreement Protocol, International Journal of Network Security, Vol.11, No.2, PP.114–117, (2010)

[11] Gandhewar, P. Lokulwar, P. : Improving Security in Initial Network Entry Process of IEEE 802.16, International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 9, ISSN : 0975-3397, (2011)

[12] Dadheech, R. Narang, G. Yadav, D. : Analysis and Literature Review of IEEE 802.16e (Mobile WiMAX) Security, International Journal of Engineering and Advanced Technology (IJEAT), Volume-1, Issue-3, ISSN: 2249 – 8958, 2012