Volume 4, No. 4, April 2013

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

FAST AND SECURE HANDOVER IN IEEE 802.16e NETWORKS

M. Deva Priya[1], K. Jaya Bharathi [2], M.L.Valarmathi[3]

[1]Department of Computer Science and Engineering, India.
[1]mail2devapriya@gmail.com
[2]Department of Computer Science and Engineering, India
[2]jayabharathi@outlook.com
[3]Department of Computer Science & Engineering, India.
[3]ml_valarmathi@rediffmail.com

Abstract: Wireless communication systems aim at supporting multimedia services with different Quality of Service (QoS) and bandwidth requirements. Effective management of limited resources is vital to enhance the network performance. Moreover, Mobile WiMAX should meet the expectations of mobile users to provide secured and seamless services. Lengthy delay due to the time-consuming authentication procedures in IEEE 802.16e handover schemes seems to be a bottleneck. It may lead to service disruption when a mobile user moves between Base Stations (BSs). The proposed ElGamal based authentication scheme overcomes the Denial of Service (DoS) attack, involving less computational cost and communication resources and achieving fast and secure inter-ASN handover.

Index terms: Handover, Authentication, DoS attack, WiMAX, Security, Delay.

INTRODUCTION

IEEE 802.16 standard, Worldwide Interoperability for Microwave Access (WiMAX) is based on Broadband Wireless Access (BWA) systems. It is an air Interface for fixed BWA Systems ratified by IEEE as a Wireless Metropolitan Area Network (WMAN) Technology.

It aims at providing broadband wireless- last mile access in a MAN with easy deployment, high speed, high data rate, large spanning area and high Quality of Service (QoS) supporting all kinds of real - time applications.

Digital Subscriber Line (DSL) can cover 3 miles, while Wi-Fi can only cover 30 meters. WiMAX, in contrast has coverage of 50 kms.

The IEEE 802.16 standards have defined the specifications for both MAC (Media Access Control) layer and PHY (Physical) layer. It defines two network topologies namely PMP (Point-to-Multipoint) topology and Mesh topology.

Five service types are defined in IEEE 802.16e-2005 standard, which includes UGS (Unsolicited Grant Service), ertPS (Extended Real-time Polling Service), rtPS (Real-time Polling Service), nrtPS (Non Real-time Polling Service) and BE (Best Effort).

IEEE 802.16e, the mobile WiMAX network includes hybrid mobility management scheme comprising of two layers. The first layer is ASN anchored mobility or Link layer mobility. ASN refers to the procedures associated with the movement of MSs between BSs. It provides wireless radio access to the WiMAX subscribers. In ASN Anchored mobility handover, the mobility anchor points for data transfer before and after handover are attached to the same ASN. Relocation of ASN does not take place as part of handover. ASN serves as the Foreign Agent (FA).

The second layer of mobility management in WiMAX is at the IP layer. CSN handles mobility and provides the Home Agent (HA) functionality. During this process, the CSN Anchor point remains unchanged, whereas the ASN Anchor point in Network Access provider (NAP) is relocated to different ASN-GW.

IEEE 802.16e supports handover, allowing a Mobile Station (MS) to find a Base Station (BS) from the same or different Access Service Network (ASN) and establish connection when moving out of coverage of the current serving BS (home BS or hBS).

To meet the security requirement, the MS should authenticate itself with the target BS (tBS) or target ASN-GW (tASN) before the MS accesses the network.

One authentication mechanism supported by the IEEE 802.16e is the Extensible Authentication Protocol (EAP) - based authentication. EAP based authentication uses a backend Authentication Server (AS) like an Authentication, Authorization, and Accounting (AAA) server, which allows the users to choose an authentication method suitable for the existing credentials without requiring the authenticator to be updated to support each new authentication approach. This flexibility makes the EAP - based authentication a popular authentication method for mobile WiMAX systems.

To design an interworking system, two main issues should be addressed: (1) handover and (2) authentication during handover. The former is called vertical handover which aims at providing the roaming devices with connectivity wherever available.

To end this, IEEE 802.21 [1] is specified for Media Independent Handover (MIH) among different types of networks. This standard also defines layer-2 triggers allowing for higher layer mobility management protocols such as Fast Mobile IP [2, 3].

In an idealized no-loss network, blind flooding is wasteful since individual nodes are likely to receive the same broadcast multiple times. In practice, however, blind flooding is a commonly used technique, since its inherent redundancy provides some protection from unreliable wireless networks. Still, blind flooding is vulnerable to attacks.

This work aims at overcoming the Denial of Service (DoS) attack. In DoS, a malicious node may induce its neighboring nodes to perform excessive computations through an algorithmic attack preventing the nodes from retransmitting a broadcast in a timely fashion; or consume excessive battery power, dramatically weakening or eliminating the node's ability to transmit messages [11].

RELATED WORK

Handover is essential for networks which support mobile subscribers. Users receiving mobile services expect handover to be completed at the earliest so they do not experience any service degrading [12, 13].

In Mobile WiMAX networks, optimization of handover mechanism is one of the most important research areas. During handover, data packets may be delayed and connections may be dropped. The main drawbacks of Mobile WiMAX handover mechanisms are wastage of channel resources, handover latencies and loss of data packets [14 - 16].

Significant research is carried out in handover in IEEE 802.16e networks and several schemes for pre-authentication and selection of suitable target BS are proposed.

In [4], a cross layer based handover scheme in mobile WiMAX is proposed. This scheme uses layer 3 to transmit MAC control messages between the MS and the BS during handover to speedup layer 2 HO. Although this scheme reduces scanning and ranging latency and eliminates network re-entry latency, it introduces synchronization latency.

In [5], authors have proposed link-layer HO scheme called Passport Handover with a Transport CID mapping strategy for real-time applications. With the help of this CID assignment strategy, conflictions of CIDs for handing over services with that of ongoing services in the target BS are avoided. Yet this scheme is complex when deployed.

In [6, 7], the authors have presented two schemes for authentication during handover in Mobile WiMAX. These schemes try to avoid the MS re-authentication. In the first scheme, whenever the MS enters the network for the first time, it is authenticated by AAA through EAP authentication. Later, whenever the MS needs to be authenticated by the AAA server, then instead of standard EAP method used in handover authentication, an efficient shared key-based EAP method is used. In the second scheme, the standard EAP method is skipped and the MS authentication is done by SA-TEK three-way handshake in PKMv2 process. This scheme is not suitable for implementation because it avoids the standard procedures.

In [8], the authors have discussed about a pre-authentication mechanism that follows the least privilege principle to solve the domino effect and this handover protocol guarantees the backward and forward secrecy. But this pre-authentication scheme is not efficient and secure.

The straight forward way to deal with any attack is to verify each message before forwarding it. The fake messages should be dropped at the first-hop neighbors of the malicious nodes so that other nodes beyond do not get affected. Although this is preferable when dealing with fake messages, it has significant penalty on legitimate broadcast messages, because it takes time for nodes to conduct message authentication. For example, signature verification using 160-bit elliptic curve keys on at mega128, a processor used in Mica motes, may take as much as 1.6 seconds [9, 10]. If every node verifies the incoming packets before forwarding them, there will be a long delay for remote nodes

to obtain an authentic message. For time-sensitive broadcast messages this is not affordable.

NETWORK MODEL

The proposed Network Reference Model (NRM) consists of three logical parts:

1. The Mobile Stations (MSs),
2. An ASN owned by a Network Access Provider (NAP) and
3. A Connectivity Service Network (CSN) owned by Network Service Provider (NSP).

An ASN is formed by BSs and an ASN-GW to offer radio access to the MSs. An ASN-GW is placed at the boundary of the ASN and connects the BSs to the CSN which provides IP connectivity service to the MSs. The ASN-GW acts as a proxy for the authentication.

The AS supporting authentication for the MSs resides in the CSN. There are two types of HOs in the specified mobile WiMAX systems. One is the intra-ASN HOs which happen when a MS moves between BSs of the same ASN.

The other is the inter-ASN HOs which happens when a MS moves from the hBS of the home ASN (hASN) to another BS of a different ASN.

THE EAP-BASED AUTHENTICATION

The procedure of the EAP-Transport Layer Security (EAP-TLS) based authentication as shown in Fig. 1 is one of the EAP-based authentication approaches that can provide strong mutual authentication [17].

It is selected as one of the options of the authentication schemes between the MS and the AS by the WiMAX forum. Initially, the MS issues a link-up requesting message to the BS. The BS then relays the EAP message to the authenticator in the ASN. The EAP message is carried to the AS over the RADIUS [18].

After the authentication process, the MS and the AS generate a MSK which is transferred to the authenticator in the ASN. The MSK is used by both the authenticator and the MS to generate PMK and authorization key (AK).

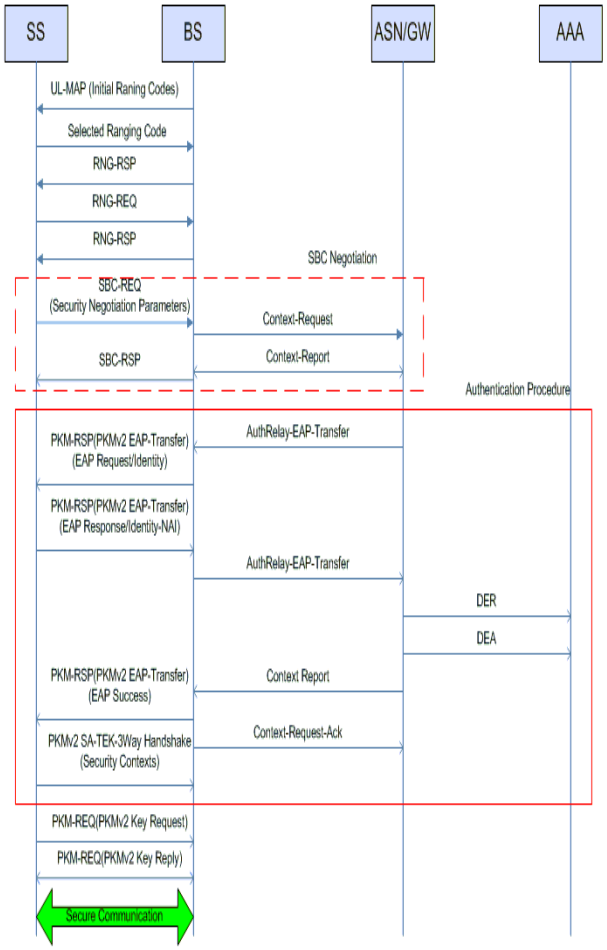

Figure 1: Authentication protocol

The AK is transferred to the hBS. It is used for SA-TEK 3-way handshake and key exchange. At the end of the authentication, both the MS and the BS share the Traffic Encryption Key (TEK) for data encryption.

In a typical network connection, a MS asks a server to authenticate it. The server returns the authentication approval to the MS, the MS acknowledges this approval, and then the MS is allowed to connect to the server.

In a Denial of Service (DoS) attack, a MS sends multiple authentication requests to the server. All the requests have false return addresses. So the server is in a predicament unable to find the MS when it tries to send the authentication approval. When the server closes the connection, the DoS attacker sends a new batch of forged requests and the process begins again causing the server to be unavailable for legitimate connections.

A common method of blocking a DoS attack is to set up a filter in the network that looks for attacks by noticing patterns or identifiers contained in the information. If a

pattern comes in frequently, the filter can be instructed to block messages containing that pattern, thus protecting the server from being overloaded by malicious attacks.

ELGAMAL ALGORITHM

This public key cryptosystem requires a modular exponentiation operation. The size of the modulus determines the security strength of the cipher (Fig. 2).

Key generation requires large strong random prime number 'p' to be chosen and the product computed. The steps involved are listed below.

- Select d to be a member of the group
- G = < Zp*, X > such that $1 \leq d \leq p-2$.
- Select 'e_1' to be a primitive root in the group G = < Zp*, X >.
- Compute $e_2 = e_1.d \bmod p$. {e_1, e_2, p} is the public key while {d} is the private key.
- To encrypt a secret 'm', represent it as a binary integer < n and also select the random integer r in the group G = < Zp*, X>.
- To decrypt the resulting cipher text c_1, c_2, raise it to the power 'd modulo p'.

$c_1 = e_1.r \bmod p$

$c_2 = (m*e_2r) \bmod$ {Encryption}

$m = [c_2 (c_1d)\text{-}1] \bmod p$ {Decryption}

The following figure shows Elgamal Encryption algorithm.

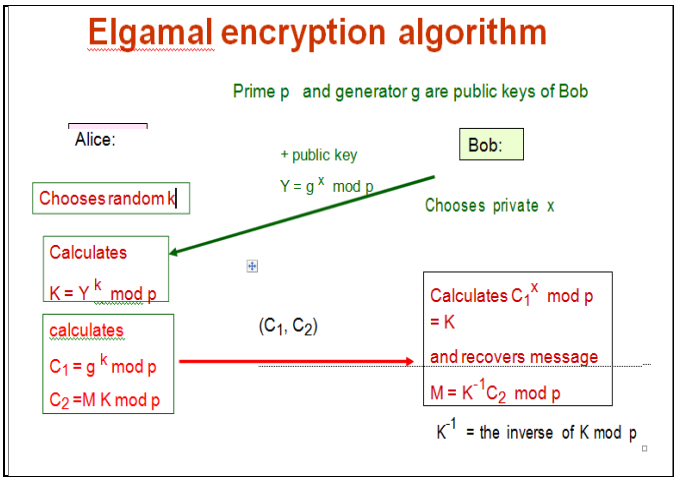

Figure 2: ElGamal Algorithm

5.1 Merits of ElGamal Algorithm

- The same plaintext is converted to a different cipher text (with near certainty) every time it is encrypted.
- The key generation is much quicker for ElGamal, taking less time than encryption or decryption.

5.2 Demerit of ElGamal

- The cipher text in ElGamal is twice as long as the plaintext.

6. Performance Analysis

The Performance of ElGamal is better when compared to EAP in terms of Authentication Delay, Message Overhead, Number of messages that can be stored and also in terms of throughput as shown in Fig. 3 - Fig. 6.

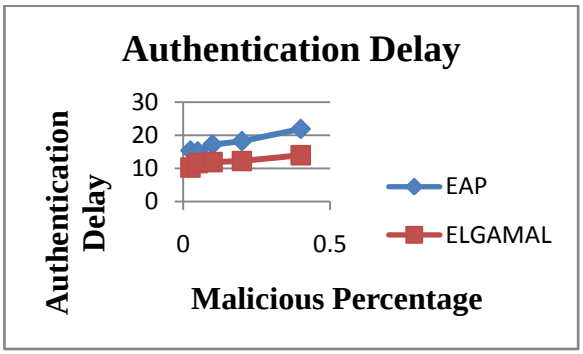

Figure 3: Authentication Delay

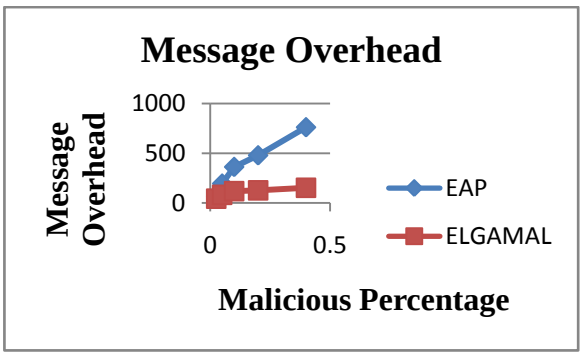

Figure 4: Message Overhead

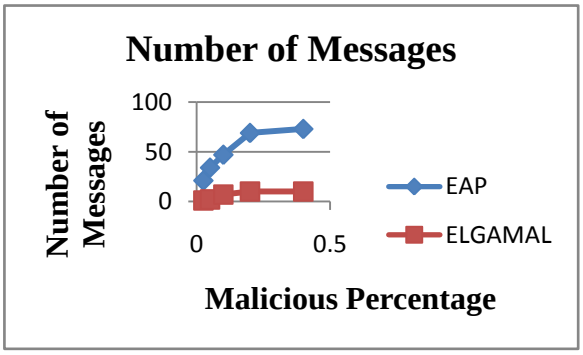

Figure 5: Number of Messages

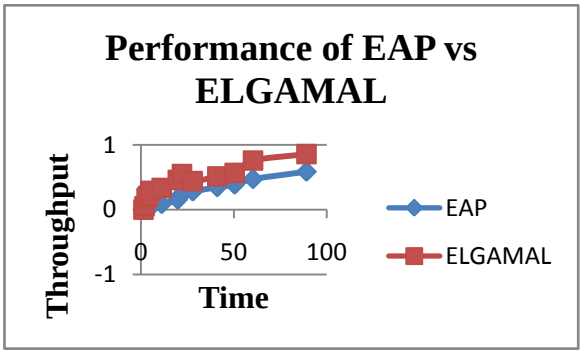

Figure 6: Throughput

CONCLUSION

ElGammal not only prevents the DoS attacks but also significantly reduces the authentication delay which is the bottleneck in the current handover process. This scheme also reduces the computations. It is both secure and efficient and can be qualified to be a competitive replacement of other secure handover schemes.

REFERENCES

[1.] Kuei-Li Huang, Kuang-Hui Chi, Jui-Tang Wang and Chien-Chao Tseng, A Fast Authentication Scheme for WiMAX - WLAN Vertical Handover, *Wireless Pers. Commun., Springer*, Sep. 2012.

[2.] Melia T, Bajko G, Das S, Golmie N and Zuniga J. C, IEEE 802.21 mobility services framework design (MSFD), *RFC 5677, IETF Network Working Group*, 2009.

[3.] Fernandes S and Karmouch A, Vertical mobility management architectures in wireless networks: A comprehensive survey and future directions, *IEEE Communications Surveys & Tutorials*, Vol. 14, No. 1, 45 - 63, 2012.

[4.] L. Chen, X. Cai, R. Sofia and Z. Huang, A Cross-Layer Fast Handover Scheme for Mobile WiMAX, *In Proc. International Conference Vehicular Technology*, pp. 1578 - 82, Sep. 2007.

[5.] Wenhua Jiao, Pin Jiang and Yuanyuan Ma, Fast Handover Scheme for Real-Time Applications in Mobile WiMAX, *In Proc. IEEE International Conference on Communications, ICC '07*, June 2007.

[6.] Ejaz Ahmed, Bob Askwith and Madjid Merabti, Pre-authentication and Selection of suitable target Base Station during Handover procedure in Mobile WiMAX Network, *In Proc. International Conference MobiHoc'07,* 2010.

[7.] H-M. Sun, S-Y. Chang, Y-H. Lin and S-Y. Chiou, Efficient Authentication Schemes for Handover in Mobile WiMAX, *In Proc. of 8th International Conference on System Design and Applications*, 2008.

[8.] J. Hur, H. Shim, P. Kim, H. Yoon and N-O. Song, Security Considerations for Handover Schemes in Mobile WiMAX Networks, *In Proc. of International Conference on Wireless Communication and Networking*, 2008.

[9.] Ronghua Wang, Wenliang Du and Peng Ning, Containing Denial-of-Service Attacks in Broadcast Authentication in Sensor Networks, *In Proc. International Conference MobiHoc'07*, Sep. 2007.

[10.] N. Gura, A. Patel, A. Wander, H. Eberle and S. Shantz, Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs, *In Proc. International Conference CHES 2004*, Cambridge, MA, August 11-13 2004.

[11.] Jonathan M. McCune, Elaine Shi, Adrian Perrig and Michael K. Reiter, Detection of Denial-of-Message Attacks on Sensor Network Broadcast, *In Proc. of the IEEE S & P*, May 2005.

[12.] Ahmed Ejaz, Bob Askwith and Madjid Merabti, Pre-authentication and selection of suitable target Base Station during Handover procedure in Mobile WiMAX Network, *Whitepapers of Mobile and Wireless*, Tech Republic, June 2011.

[13.] Kamran Etemad, Overview of Mobile WiMAX Technology and Evolution, *IEEE Communications Magazine*, Oct. 2008.

[14.] Chuang, M-C., J-F. Lee and M-C. Chen, SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks, *IEEE systems Journal*, pp. 1, 2013.

[15.] Tom Karygiannis and Les Owens, Wireless Network Security 802.11, Bluetooth and Handheld Devices, *In Proc. International Conference Vehicular Technology, NIST*, 2002.

[16.] Ejaz Ahmed, Bob Askwith and Madjid Merabti, Handover Optimization for Real-Time Application in Mobile WiMAX / IEEE 802.16e, *In Proc. 11th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*, UK, June 2010.

[17.] D. Simon B. Aboba and R. Hurst, The EAP-TLS Authentication Protocol, *RFC 5216*, Dec. 2009.

[18.] G. Zorn, RADIUS Attributes for IEEE 802.16 Privacy Key Management Versions 1 (PKMv1) Protocol Support, *RFC 5904*, Dec. 2010.