IMPROVING SECURITY IN INITIAL NETWORK ENTRY PROCESS OF IEEE 802.16

Prof. Pranita K. Gandhewar
Computer Science & Engineering Department
NYSS College of Engineering & Research
Nagpur, India
E-mail: pranita.gandhewar@gmail.com

Prof. Prasad P. Lokulwar
Computer Science & Engineering Department
J. D. Institute of Engineering & Technology
Yavatmal, India
E-mail: prasadengg16@gmail.com

Abstract: **IEEE 802.16 basically designed to provide more security as compared to other wireless networks. It provides many security features to protect the information in the network as well as to protect the network from unauthorized access, still it vulnerable to many attacks. The process, where attack or threat is possible, is the initial network entry process of IEEE 802.16. This is because many of the MAC management messages, which are used in this process, are not encrypted. The initial network entry process is very important as this is the first gate to establish connection between MS and BS. The solution to this problem provided by some paper is to use Diffie-Hellman key exchange algorithm, but the algorithm we are going to use here is elliptic curve Diffie-Hellman key exchange algorithm. This paper provides the solution to the initial network entry process by using elliptic curve Diffie-Hellman key exchange algorithm as it is faster than the Diffie-Hellman key exchange algorithm. Hence it also improves the performance of IEEE 802.16.**

Keywords: IEEE 802.16; Security; Network entry; Threats; Encryption; ECDH.

I. INTRODUCTION

IEEE 802.16 is the standard used for Wi-MAX (Worldwide Interoperability for Microwave access). The main aim of IEEE 802.16 is to provide more security in the network. It provides several security features such as scalability, mobility, strong security, access control, data privacy, data integrity, robust user authentication and strong QoS guaranteed service. Many sophisticated authentication and encryption techniques have been embedded into IEEE 802.16 but it still exposes to various attacks. WiMAX basically operates on two layers: physical layer (PHY) and MAC layer (MAC), of which security is implemented at the security sub layer of the MAC. Both the layers of WiMAX are vulnerable to several attacks.

The paper [4] describes several security issues of IEEE 802.16 with the possible solution. One of which is threats to the initial network entry process in the IEEE 802.16. Initial network entry is one of the important processes, as it is the first phase to establish connection to the network. Initial network entry is the major issue, as it directly influences the delay in the network [5].

This paper provides solution for this security issue of IEEE 802.16 network. The solution to this problem provided by the several papers is to use Diffie-Hellman key exchange algorithm in initial network entry process, but the algorithm we are using for this problem is elliptic curve Diffie-Hellman (ECDH) key exchange algorithm. The reason behind using this algorithm is that ECDH algorithm is much faster than Diffie-Hellman algorithm, hence improving the security as well as performance of the IEEE 802.16.

The rest of the paper is organized as follows: Section II gives the basics about the initial network entry process of IEEE 802.16. In section III, we summarize the threats that are possible to the initial network entry process. Section IV presents the proposed mechanism which provides the solution to the initial network entry issues. Elliptic curve Diffie-Hellman key exchange algorithm is discussed the Section V. Finally we conclude in the section VI.

II. INITIAL NETWORK ENTRY BASICS

The network entry process is a set of procedures that MS must follow in order to enter the network and to get the network services. The initial network entry procedure mainly consists of four processes [1]: initial ranging process, MS basic capability negotiation process, PKM authentication process and registration process. The important point that is to be noted here is that, depending on the current status of the MS, the network entry process can be different. This process is the most security sensitive process in IEEE 802.16 network. Fig. 1 given below describes the initial network entry procedure.

A mobile station which is just powered on must perform initial network entry process. The steps for initial network entry process are given below:

Step 1: When it is powered on, it firsts scans the downlink channel to determine whether it is currently in the coverage of base station.

Step 2: Each MS stores the list of optional parameters, such as DL frequency. So in next step MS synchronizes with the stored DL frequency of most suitable BS [7].

Step 3: Once the DL synchronization is completed, MS can listen to the various control messages from which it obtains the UL parameters. Based on these UL parameters, MS decides whether the channel is suitable or not.

Step 4: If the channel is suitable MS performs next step, otherwise it goes back to the scanning step that is step 1.

Step 5: Next step is to perform ranging process. Ranging is the process to acquire timing and power level adjustment to maintain the UL connection with the BS. To perform initial ranging, MS send a RNG-REQ message to the BS with the CID parameter [2].

Step 6: In response to this message, BS sends the RNG-RSP message to the MS with the basic and primary CID.

Step 7: After initial ranging, next step is to perform basic capability negotiation process. Here MS firsts sends the SBC-REQ message to the BS through which MS informs the BS about its basic capabilities.

Step 8: When BS receives this message, it responds with the SBC-RSP message consisting of the parameters required for the UL and DL transmission.

Step 9: After negotiating the basic capabilities, authentication and key exchange process will be performed.

Step 10: Once the key exchange process is completed, MS registers itself with the BS, for which it sends the REG-REQ message to the BS.

Step 11: In response to this message, BS sends the REG-RSP message to the MS. When MS receives this message, it can obtain the IP address.

Step 12: Finally the service flow will be established, which is either initiated by the MS or BS.

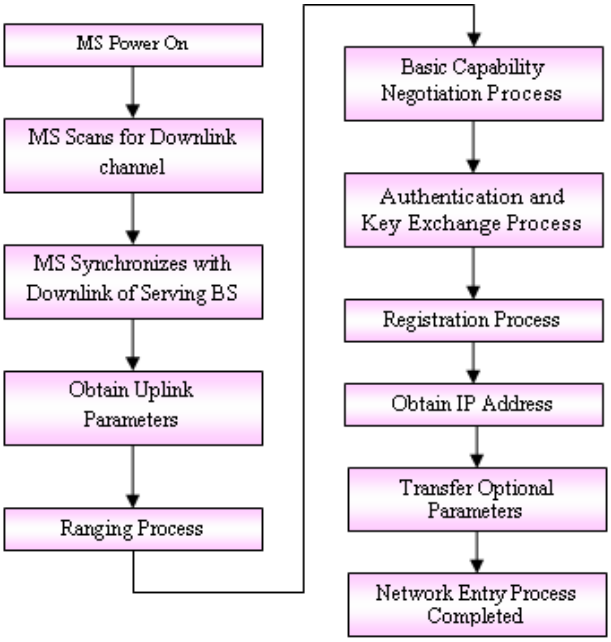

Fig. 1: Initial Network Entry Procedure

III. THREATS TO INITIAL NETWORK ENTRY PROCESS

The threats that are possible to initial network entry process are given below [1, 6]:

(1) RNG-RSP vulnerability
(2) Auth-Request and Invalid vulnerability
(3) Rogue BS

A. RNG-RSP vulnerability

The messages that are used in the initial ranging process are RNG-REQ and RNG-RSP. RNG-REQ message is used by the MS for requesting the BS to join the network [3] and RNG-RSP message is used by the BS in response to the RNG-REQ message to the MS containing basic and primary CID. These ranging messages are not encrypted and hence the attacker can access it and modify it accordingly.

In RNG-RSP vulnerability, the attacker can modify this message and set the status as failed. The attacker can resends this message to the MS, which indicates the MS that it has to go for initial ranging again. An attacker may intercept the RNG-RSP message again and again with the status providing as failed [1, 6]. Hence, the MS cannot join the network and leads to the DoS attack. The solution to this problem is to use Diffie-Hellman key exchange algorithm.

B. Auth-Request and Invalid vulnerability

In Auth-Request and Invalid vulnerability, the attacker intercepts the Auth-Request message and resends it to the BS continuously. As the BS gets Auth-Request message continuously, it would be confused and sets the Auth-Response message as failed. In some cases, an attacker may intercept the Auth-Response message and resend it to the MS after time out period [1, 6].

The solution to this problem is to use the time-stamps. By adding time-stamps to the authorization messages, MS and BS can verify that whether the authorization message is proper. Hence the attacker also cannot modify the message. Use of time stamps avoids the replay attack.

C. Rogue BS

In rogue BS attack, the MS cannot verify that any authorization messages it receives were generated by an authorized BS. So any rogue BS can create an authorization response message and send it to the MS [1, 6]. To solve this problem, the MS has to authenticate the BS for the messages it receives from the BS.

IV. PROPOSED MECHANISM

The suggested solution for the initial network entry process in some paper is to use Diffie-Hellman key exchange algorithm. In this paper the mechanism is given which uses Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm, which is explained in the next section, instead of Diffie-Hellman algorithm. The reason behind using ECDH algorithm is to improve the security as well as to improve the performance of the system. The performance will be increased because ECDH is much faster than the simple Diffie-Hellman algorithm.

The proposed model for initial network entry is shown in fig. 2. This proposed mechanism solves two issues of initial network entry: RNG-RSP vulnerability and Rouge BS [6]. Here, the ECDH algorithm is used to generate a common secrete key called as pre-TEK. This key is used to encrypt the RNG-RSP message. Hence the intruder cannot modify the message. Hence MS and BS can perform secure ranging process. In the ranging process the secure channel will be established, because of which the SBC parameter and authentication messages are securely exchanged. As the complete initial network entry process is secure, the authentication vulnerability gel also solved.

This mechanism works as follows:

Step 1: As soon as the MS turns on, it scans for the DL channel and performs other required operation explained in section 2.

Step 2: Next it receives the initial ranging codes from the BS and select the appropriate initial ranging code.

Step 3: Then it generates the domain parameters of ECDH algorithm, p and G. Here, the p is a prime number and G is the generator.

Step 4: Using these parameters, it generates the public key of MS and sends the RNG-REQ message to the BS with the selected ranging code, domain parameter and MS public key.
Step 5: BS then verify the parameter p, generates the BS public key and sends the RNG-RSP message to the MS with the public key of BS.
Step 6: Then in next step the key called pre-TEK will be generated and secure communication channel will be established.
Step 7: The secure ranging process will be performed using pre-TEK.
Step 8: SBC parameters and authentication messages are exchanged securely.

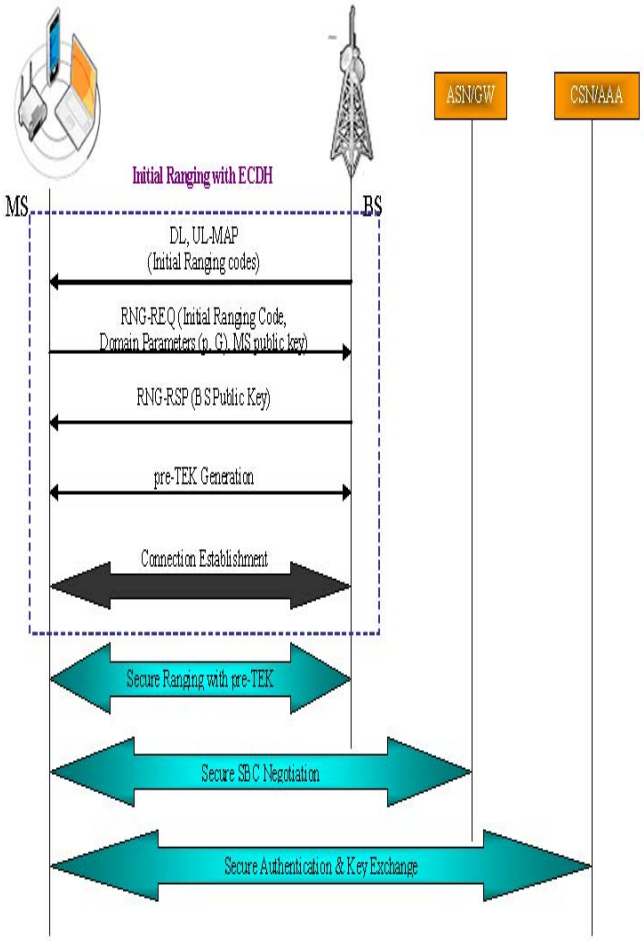

Fig. 2: Proposed Mechanism for Initial Network Entry

V. ELLIPTIC CURVE DIFFIE-HELLMAN ALGORITHM

Elliptic Curve Diffie-Hellman (ECDH) algorithm is a key agreement protocol that allows two parties to establish a shared secret key [1]. Both the parties first exchange some public information with each other and using this public data and their own private data, these parties calculates the shared secret key. The public data and private data is nothing but the public and private key respectively. Any third party, who doesn't have access to the private details of each device, will not be able to calculate the shared secret key from the available public information.

For generating a shared secret key between MS and BS using ECDH, both have to agree up on Elliptic Curve domain parameters. The domain parameters for Elliptic curve over Fp are *p, a, b, G, n and h.* Where,

- p is the prime number defined for finite field Fp .
- a and b are the parameters defining the curve $y^2 \bmod p = x^3 + ax + b \bmod p$.
- G is the generator point (xG, yG), a point on the elliptic curve chosen for cryptographic operations.
- n is the order of the elliptic curve. The scalar for point multiplication is chosen as a number between 0 and n – 1.
- h is the cofactor where h = number of points on an elliptic curve / n.

Both ends have a key pair consisting of a private key d (a randomly selected integer less than n) and a public key Q = d * G. Let (d_A, Q_A) be the private key - public key pair of A and (d_B, Q_B) be the private key - public key pair of B. The algorithm works as follows.

Step 1: MS selects its private key d_A randomly and calculates the public key $Q_A = d_A * G$.

Step 2: Similarly, BS selects its private key d_B randomly and calculates the public key $Q_B = d_B * G$.

Now, MS as well BS have the pair of private and public key.

Step 3: MS and BS then exchanges their public key.

Step 4: MS then computes $K = (X_K, Y_K) = d_A * Q_B$.

Step 5: Similarly, BS computes $L = (X_L, Y_L) = d_B * Q_A$.

Step 6: Since K = L, the shared secret is K.

Since it is practically impossible to find the private key d_A or d_B from the public key Q_A or Q_B, it is not possible for a third party to obtain the shared secret key.

VI. CONCLUSION

The IEEE 802.16/WiMAX provides more security as compared to other wireless technologies, but it still vulnerable to various attacks. The most security sensitive process of IEEE 802.16 is initial network entry process, because it is the first process performed by MS to join the network. The solution suggested in some of the paper is to use Diffie-Hellman key exchange algorithm.

In this paper, we have proposed a model which uses Elliptic Curve Diffie-Hellman key exchange algorithm. As the proposed model uses this algorithm, security as well as performance will get improved, because ECDH is faster than the Diffie-Hellman algorithm. Using ECDH not only solves the RNG-RSP vulnerability but also solves the authentication vulnerability. Still various threats are possible at the MAC as well PHY layer of the IEEE 802.16, hence more work is required to solve the several issues.

REFERENCES

[1] A.K.M. Nazmus Sakib, Dr. Muhammad Ibrahim Khan, Mir Md. Saki Kowsar, "IEEE 802.16e Security Vulnerability : Analysis and Solution", Global Journal of Computer Science and Technology Vol. 10 Issue 13 (Ver. 1.0), October 2010.

[2] Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, Toshiaki Tanaka, "Security Vulnerabilities and Solutions in Mobile WiMAX", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.11, November 2007.

[3] John Kok Han Hong, Mohamad Yusoff Alias and Bok Min Goi, "Simulating Denial of Service Attack Using WiMAX Experimental Setup", International Journal of Network and Mobile Technologies, ISSN 2229-9114 Electronic Version VOL 2 / ISSUE 1 / JANUARY 2011.

[4] Ms. Pranita K. Gaandhewar and Prof. Kapil N. Hande, "A Survey on IEEE 802.16: Security Threats and Solutions", 2011 International Conference on Network Communication and Computer, 21-23 March 2011.

[5] Pero Latkoski, and Borislav Popovski, "Communication Protocol Engineering and Optimization of Network Entry Process in IEEE 802.16 Based Systems", International Journal of Multimedia and Ubiquitous Engineering Vol. 4, No. 2, April, 2009.

[6] Perumalraja Rengaraju, Chung-Horng Lung, Yi Qu and Anand Srinivasan, "Analysis on Mobile WiMAX Security", IEEE TIC-STH 2009, Information Assurance in Security and Privacy, September 27-29, 2009.

[7] V V Girish, V K Govindan, Shakeel Baig, Vijaya Yajnanarayana, "A Novel Initial Ranging Algorithm for mobile WiMAX (802.16e)", 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 3, 2010.