

Mutual Authentication Between Base and Subscriber Station Can Improve the Security of IEEE 802.16Wimax Network

Mohammad Hossain

*Telecommunication Systems
Blekinge Institute of Technology
Karlskrona, 37179, Sweden*

reganmh8@gmail.com

Mohammad Zavid Parvez

*Signal Processing
Blekinge Institute of Technology
Karlskrona, 37179, Sweden*

zavidparvez@hotmail.com

Mohammad Hamidul Islam

*Information and Communication Systems Security
Royal Institute of Technology
Stockholm, 10044, Sweden*

rubeldiu@yahoo.com

Abstract

High throughput broadband connection over long distance is greatly demanded in the present web application. IEEE 802.16/WiMax technology is one of the latest additions on internet broadband. When wireless devices are connected to the broadband wireless access, security comes on the front line to ensure the communication safe and protected from any kind of attacks or threats. Strong and effective security must be confirmed to make the wireless environment reliable and risk less. Base station authentication is an important part of WiMax security which must be confirmed to make the environment more secure. This paper derived the technique to secure the environment by confirming the authentication of base station.

Keywords: WiMax, Authentication, Base Station, Broadband Connection, Security.

1. INTRODUCTION

Since the last decade of twentieth century, data networks have successfully acknowledged a progressive expansion and getting update with time. The whole world is the prime target to come under the coverage of fixed internet to facilitate the communication easier and faster. For this extra large coverage, wireless access is chosen because of its last end focusing power and reaching ability rather than that of wired network. The expansion of high speed wireless data access i.e., in MB/s, is going to make wired network a history which is just a matter of time in the present twenty first century.

The world telecommunication became instantly prosperous in consideration of its high speed data transmission and coverage to the end user when WiMax added to it. The resource scarcity has been eliminated instantly which was concerning present service providers even some few years before. All of the major telecommunication services like as voice (mobile and static), video and data sharing got the new shape in true market based competition.

WiMax provides fixed, portable or mobile non line-of-sight (NLOS) service from a base station (BS) to subscriber station (SS) and so also known as customer premise equipment (CPE). Fig. 1 shows the transmission of WiMax between point-to-point and point-to-multipoint scenario. With a throughput of 72 Mbps it covers 30 miles of area around it in point-to-point communication. In the case of point-to-multipoint scenario it covers 6 miles NLOS range with a throughput of 40 Mbps.

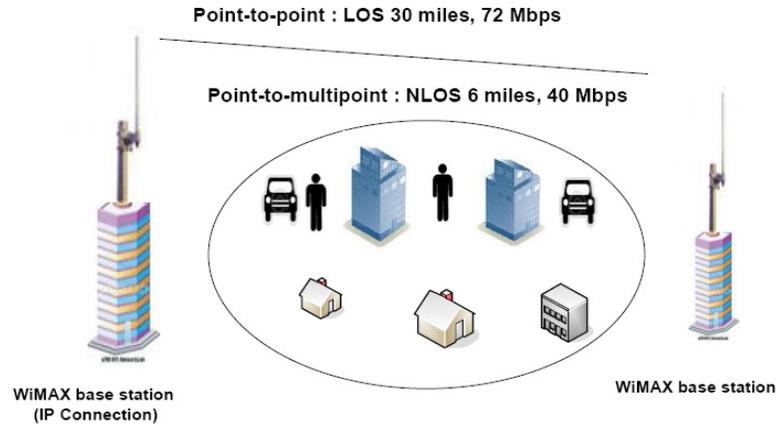


FIGURE 1: Fixed WiMAX showing point to point and point to multipoint communication [1].

During the time of designing of IEEE 802.11 wireless standard, scientist and manufacturer considered the security issues after all other infrastructure and implementation [8]. So the security of this standard familiarized as part of one of most vulnerable wireless protocols. In the case of IEEE 802.16 standard, security was thought to be implemented within the protocol but the depressing thing is that it was also left aside and not considered as a front line topic. The consequence is that, there are still questions about the transmission security of this standard. Many papers published on different security issues and researchers are still working to make it robust, secured and trustworthy.

2. DIFFICULTY CLASSIFICATION

It is not always unreachable for the attackers to intercept the wireless network as because it is based on radio waves which keep the medium open more or less during transmission. A secured radio transmission was always a concerning issue to the protocol designers. The different issues which primarily considered during the designing time were handling with intrinsic untrustworthiness of wireless medium, good mobility, featuring of protocol to be confirmed while delivering frames in mobility and also power saving [2]. In the former specification IEEE 802.11 wireless standard, security proved to be an inadequately considered issue which was not mentioned in the frontage line. The implementation of the wireless network was also not secured enough so that it can easily handle service disruption and theft. Different kind of attacks took place by the intruders which make the network poorly secured due to the various attacks like as interception, fabrication, modification, interruption and so on. Although in IEEE 802.16 standard designing in MAC layer was especially focused on the security mechanism, yet it might provide inadequate security in multihop scenarios and demand the needs of rising applications in WiMax networks [3]. Paper [4] mentioned that WiMax is suitable to physical layer attacks like as jamming which is a source of noise and so strong that it significantly reduce the capacity of transmission channel. It also mentioned of scrambling which is kind of jamming occurs to specific frames for short intervals of time. In IEEE 802.16 standard securities are implemented as a sub-layer at the bottom of MAC layer in order to protect the data exchange between the MAC and PHY layer but does not protect the PHY layer itself against the attacks which intends to malfunction the internally built weakness of the wireless links [5]. So, security is such an important issue in data transmission of wireless network that a little mistreat or falsification of data may generate huge chaos and disable the complete system for long run and cause immeasurable sufferings.

3. BASE STATION SPOOFING

When a rogue BS gets credentials from a legitimate SS to process further transmission and so cheat the SS called BS spoofing. Initially the SS tries to get authorization and traffic keying material from the BS. For this, it uses the PKM (Key Management Protocol) protocol. The

protocol has the necessary features to support the periodic reauthorization and key refreshment. This protocol also uses the RSA public key encryption algorithm and X.509 digital certificates. The key exchanging between the SS and the BS takes place in presence of some strong encryption algorithm like as DES (Data Encryption Standard), AES (Advanced Encryption Standard) etc. A client-server model is performed during transmission by the PKM protocol. The SS acts as a PKM client and the BS acts a PKM server. Being a client, the SS requests keying materials from the BS and the BS provides the requested keying materials to the SS. When the SS is authorized, it gets keying materials from the BS. MAC management messages of the protocol are used between the BS and the SS which are PKM-REQ and PKM-RSP as already mentioned. To establish a shared and secret Authentication Key (AK) between the SS and the BS, the protocol uses public key cryptography. Consecutive PKM exchanges happened by maintaining a secure traffic encryption keys (TEKs) using the authentication key. A BS authenticates an SS during the initial authorization.

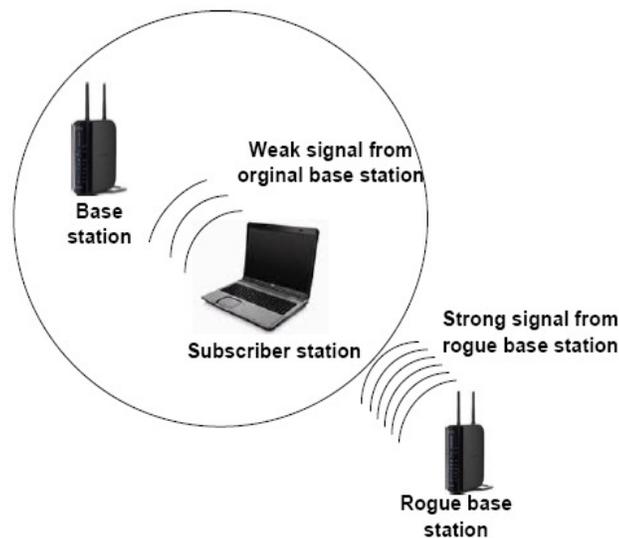


FIGURE 2: Base Station spoofing by a rogue node.

The manufacturer issues X.509 digital certificate for each SS which are given to them. The certificate has the SS's public key and MAC address. The SS presents its digital certificate to the BS when requesting an AK. After verifying the digital certificate the BS uses the verified public key to encrypt an AK and transmits to the SS. This way exchanging the AK, the BS established an authenticated identity of a client SS. Now, the SS is authorized to proceed for further services. Because of this authorization process, it is very difficult for an attacker to get inside into the network being a false SS. But, there is no way of BS authentication. That is the place where the attacker starts its working. Fig. 2 shows how an attacker disguised himself as a rogue BS and creates BS spoofing.

4. MAC ADDRESS SPOOFING

Each SS uses an SS certificate during the time of authentication. This certificate is issued and signed by the manufacturer. The subject field of a certificate contains the MAC address and identifying credentials of an SS. 48-bit MAC address is used in IEEE 802.16 standard. Using this subject field documents the BS and the SS identifies each other during the time of initial ranging and authentication process. SS includes the MAC address while sending Ranging Request (RNG-REQ) to the BS. The BS sends back the MAC address again in its Ranging Response (RNG-RSP). An eavesdropper may try to get the MAC address of the authorized SS by intercepting either the uplink or the downlink of the connection. But, it becomes difficult for the attacker because of maintaining a private key public key method between the BS and the SS. The attacker compromises it with the BS as the BS is not authorized like the SS. There is no way

of authentication or BS certificate that the BS sends to the SS to introduce it as a legitimate BS and not the false one.

5. SECURITY IMPROVEMENT

In IEEE 802.16 network, an SS must be authenticated and verified by the BS to obtain the network credentials and to be a part of the network as a legitimate node. But, there is no such verification or authentication procedure by which an SS can verify and authenticate a BS before it starts to give all its credentials to the unknown BS. The easy thing is that a BS can also pass through some verification procedure by which the SS will understand that it is communicating with a legitimate BS and not with the rogue one. Therefore, mutual authentication is must to establish a both side secure and trustworthy transmission. It is rather an intelligent thinking to work on the process besides running behind the intruders. Different attacks are discussed so far which are related more or less only because the base station authentication is not present in the existing authentication protocol which is shown below in Fig. 3. It shows the present scenario of the SS verification and authentication but not for the BS.

Message 1: SS → BS: Cert (SS) (Auth Req message)
 Message 2: SS → BS: Cert (SS) | Capabilities | BCID
 Message 3: BS → SS: KU_{SS} (AK) | SeqNo | Lifetime | SAIDList

FIGURE 3: Authentication Protocol of IEEE 802.16 Standard.

In Fig. 3, Cert (SS) is the digital certificate which the SS obtained from the manufacturer. The basic fields which are included on it are certificate version, serial number, signature, issuer, validity, subject, subject public key info, issuer unique ID, subject unique ID, and extensions. Capabilities contain the SS supported authentication and data encryption algorithms. Basic Connection ID of SS is termed as BCID. KU_{SS} (AK) is the Authorization key generated by the BS for the SS and is encrypted with the public key of SS. SeqNo is a 4-bit sequence number. Lifetime is the number of seconds. SAIDList contains the identities and the properties of the SAs (Security Associations) due to which an SS is authorized to obtain keying information.

When the rogue BS obtained all the credentials from the SS being a legitimate BS, it can put the SS out of the network by repeating the received messages from SS to the legitimate BS again and again. When the preliminary message repeatedly comes, the BS stops receiving any more messages from the source considering it as a fraud or disturbing element. So, the existing protocol must be renewed to ensure secure and trustworthy communication especially in banking, government activities or other important sectors only to maintain high security from the intruders and hackers.

5.1 Mutual Authentication can be Established as the Proposed Algorithm

During the time of transmission, an SS initiates the session. It sends its identifications, capabilities and other requirements to the BS. After checking the documents the BS sends back Authorization Reply to the SS. This reply must be checked whether it is from the legitimate BS or rogue BS. As the SS has no ability to check it, it can get help of a trusted third party. This third trusted party is an Authentication Server (AS) which must be in the knowledge of SS. The AS and the BS know each other as they are manufactured by the manufacturer this way. After getting the Auth Reply from the BS, the SS will send it to the Authentication Server (AS). The BS will also forward information containing its own ID, SSID and SS credentials to the AS. The AS will judge both side information's received from the BS and the SS and return the confirmation to the SS. In this message, if SS finds that the BS is a legitimate one, it will continue its transmission. Otherwise, it will end further communication with the BS. The Fig. 4 shows the new authentication protocol to avoid rogue BS. Here the BS sends back the Auth Reply message to the legitimate SS where it also includes its ID which the SS will present to Authentication Server (AS). If any attacker tries to involve the network, it will be captured by Authentication Server. However,

legitimate BS will not allow any other party but the legitimate SS as it checks its ID and other credentials. DES (Data Encryption Standard) encryption can be used in all private-public key cases.

6. SIMULATION RESULT

The proposed algorithm is demonstrated in a simulation process only to represent its accuracy, perfections and way of working.

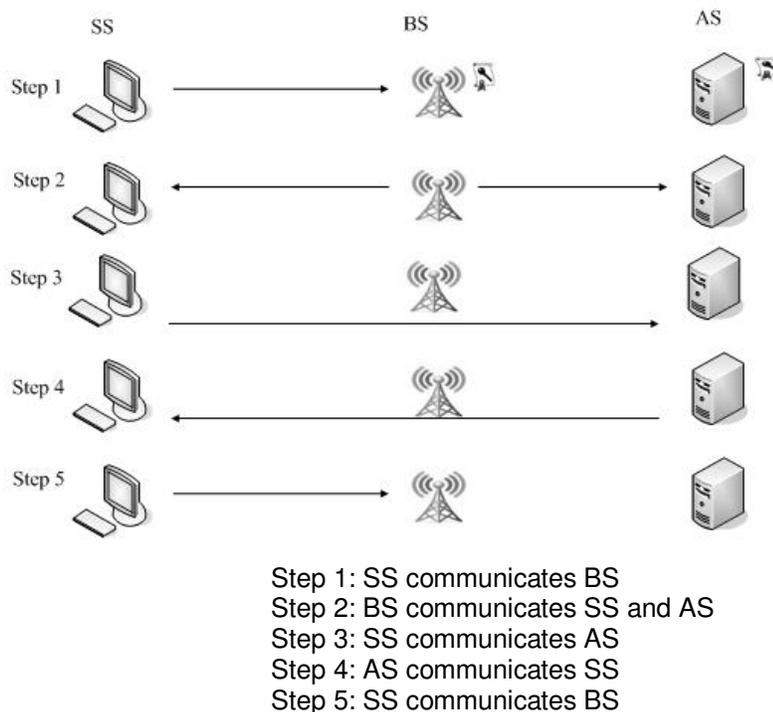


FIGURE 4: The Mutual Authentication process to avoid Rogue BS attack.

The obtained result of the simulation process confirmed that the algorithm works according to its theme and process. The testing environment of the simulation and its way of working is given below.

6.1 Testing Environment

Testing environment expressed the manipulation of the result. A simple implementation of a TCP client server relationship has been considered where the SS works as client, the BS the AS work as server respectively. The algorithm has some prerequisite conditions like as the BS and the AS are previously trusted to each other and the SS and the BS would use public key cryptography for message encryption or decryption.

The simulation process used the following things in its testing environment.

- Microsoft Windows Vista platform
- Processing power of the machine 2.0GHZ
- The Socket class in the .NET framework
- TCP/IP protocol.
- Some encryption and decryption capabilities.
- Programming language C#.NET.

6.2 Overall Communication Process

The overall communication processes are as follows:

Step 1: The BS is waiting to get someone's request like as the SS. Here the BS is running at port 8001 and the local IP is 192.168.1.73 shown in Fig. 5.



```
file:///E:/assignment project/Server/Server/bin/Debug/Server.EXE
The Base Station (BS) is running at port 8001...
The local End point is :192.168.1.73:8001
Waiting for a connection.....
```

FIGURE 5: The Base Station (BS) is waiting for the connection.

Step 2: The SS has connected to the BS with port 8001 and Local end point is 192.168.1.73. The SS is sending its subscriber ID and all necessary credentials to the BS shown in Fig. 6.

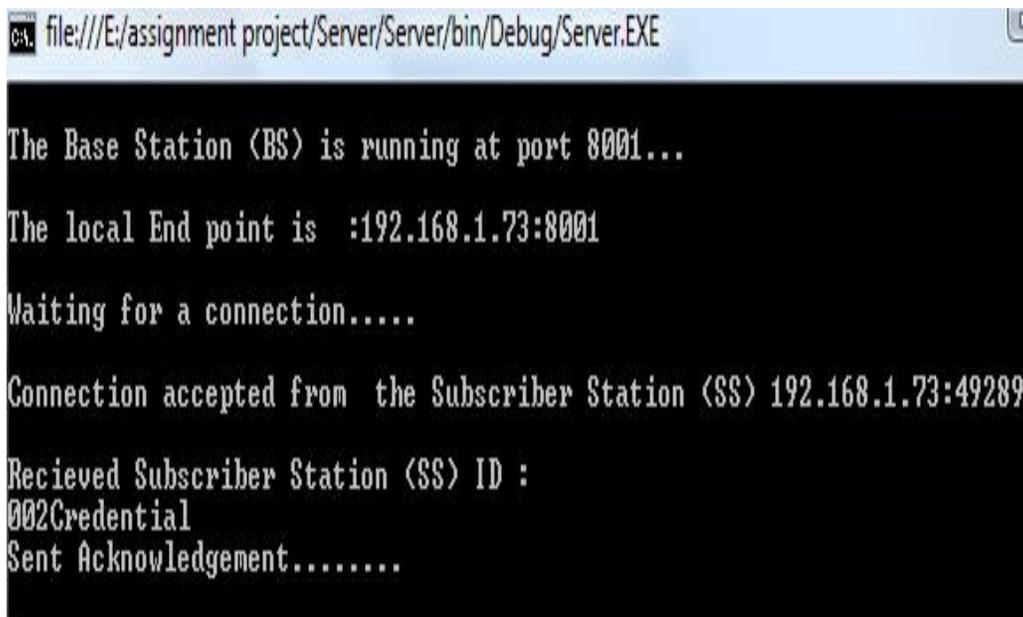


```
file:///E:/assignment project/Client/Client/bin/Debug/Client.EXE
Connecting.....
Connected to the Base Station (BS)
Enter the Subscriber Station (SS) ID to be transmitted to the Base Station (BS)
: 002Credential
Transmitting.....
```

FIGURE 6: The SS is sending information to the BS.

Step 3: The BS received successfully the SS credentials. The BS verified the SS credentials. After the verification the BS starts further communication with the SS. The BS encrypted its ID by using DES encryption algorithm and sends it to the SS shown in Fig. 7. The BS does the

verification procedure by its predefined knowledge about the SS. The ID or the information of the SS is attached inside the simulation code so that the BS can verify the SS if the correct ID or address is used otherwise would discard the SS which is shown in Fig. 7.



```
file:///E:/assignment project/Server/Server/bin/Debug/Server.EXE

The Base Station (BS) is running at port 8001...

The local End point is :192.168.1.73:8001

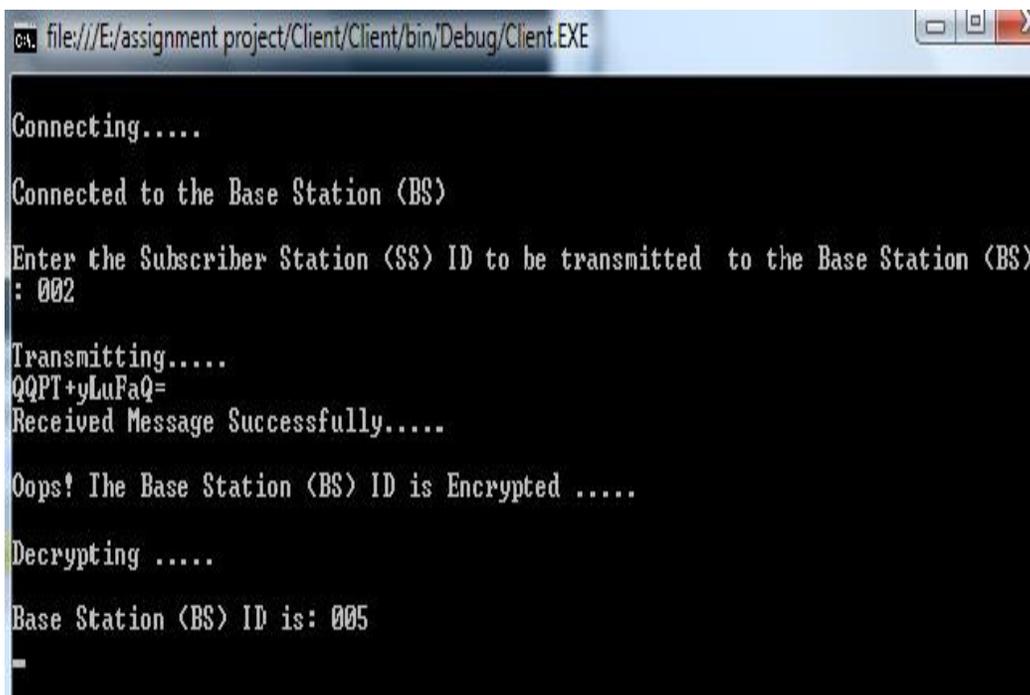
Waiting for a connection.....

Connection accepted from the Subscriber Station (SS) 192.168.1.73:49289

Recieved Subscriber Station (SS) ID :
002Credential
Sent Acknowledgement.....
```

FIGURE 7: The BS is sending information to the SS.

Step 4: The SS received encrypted information from the BS. The SS is decrypting the BS information by using DES decryption and found the BS ID.



```
file:///E:/assignment project/Client/Client/bin/Debug/Client.EXE

Connecting.....

Connected to the Base Station (BS)

Enter the Subscriber Station (SS) ID to be transmitted to the Base Station (BS)
: 002

Transmitting.....
QQPT+yLuFaQ=
Received Message Successfully.....

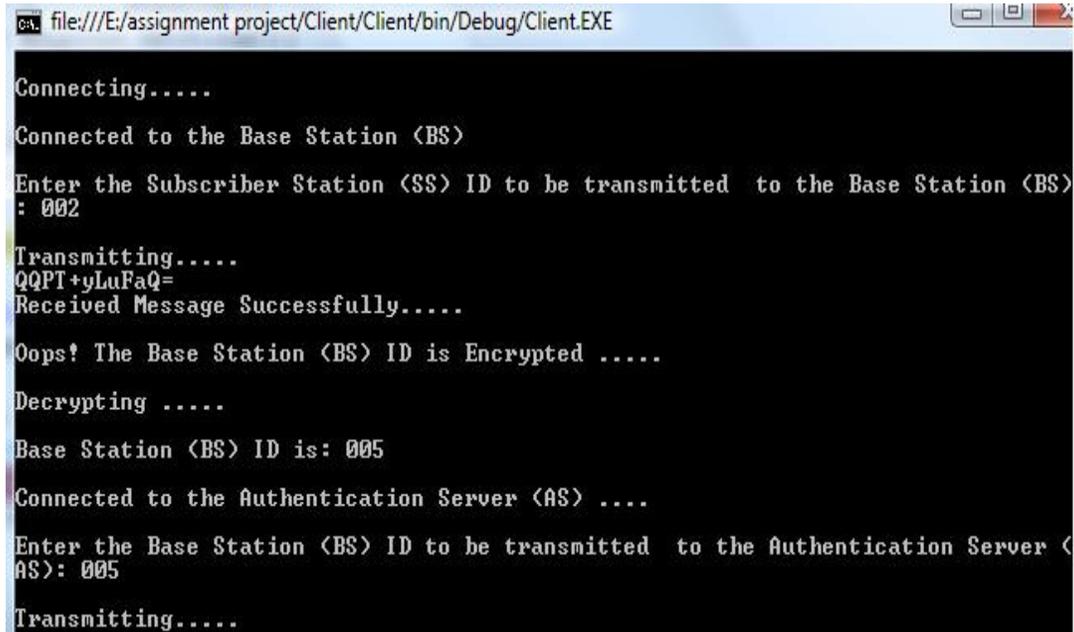
Oops! The Base Station (BS) ID is Encrypted .....

Decrypting .....

Base Station (BS) ID is: 005
```

FIGURE 8: The SS received message from the BS and decrypting the message.

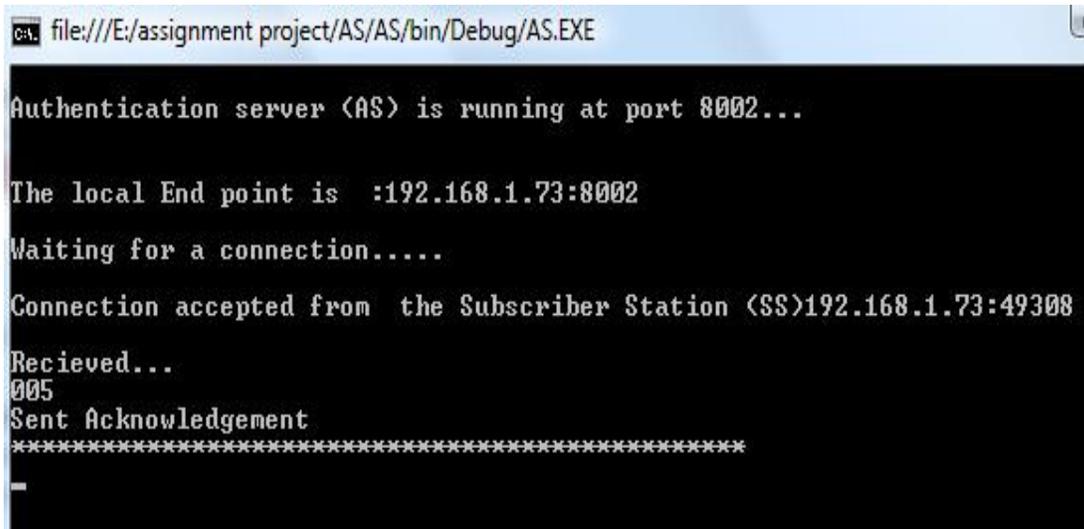
Step 5: To verify the BS, the SS is sending the BS ID to the Authentication Server (AS). Local end point of the AS is 192.162.1.73 and TCP port 8002.



```
ca. file:///E:/assignment project/Client/Client/bin/Debug/Client.EXE
Connecting.....
Connected to the Base Station <BS>
Enter the Subscriber Station <SS> ID to be transmitted to the Base Station <BS>
: 002
Transmitting.....
QQPT+yLuFaQ=
Received Message Successfully.....
Oops! The Base Station <BS> ID is Encrypted .....
Decrypting .....
Base Station <BS> ID is: 005
Connected to the Authentication Server <AS> ....
Enter the Base Station <BS> ID to be transmitted to the Authentication Server <
AS>: 005
Transmitting.....
```

FIGURE 9: The SS transmitting message to the AS.

Step 6: The AS received message from the SS, verified the BS as rouge or trusted and sent acknowledgement to the SS.



```
ca. file:///E:/assignment project/AS/AS/bin/Debug/AS.EXE
Authentication server <AS> is running at port 8002...
The local End point is :192.168.1.73:8002
Waiting for a connection.....
Connection accepted from the Subscriber Station <SS>192.168.1.73:49308
Recieved...
005
Sent Acknowledgement
*****
```

FIGURE 10: The AS verified the BS and sent message to the AS.

Step 7: After receiving the acknowledgement of the AS, the SS got the confirmation that the BS is trusted or not. If the BS is trusted then protected communication will start between the SS and the BS otherwise all communication will remain stop in this phase. In this simulation process, the SS is ID is 002 and the BS ID is 005. When the SS sends the BS ID 005 to the AS, it is accepted as a trusted BS which is shown in Fig. 11. Here any other ID except 005 for BS would have

considered as a false or unknown one as in the simulation code only 005 is inserted as a trusted BS which is in the knowledge of AS.

```

file:///E:/assignment project/Client/Client/bin/Debug/Client.EXE
Connecting.....
Connected to the Base Station <BS>
Enter the Subscriber Station <SS> ID to be transmitted to the Base Station <BS>
: 002
Transmitting.....
QQPT+yLuPaQ=
Received Message Successfully.....
Oops! The Base Station <BS> ID is Encrypted .....
Decrypting .....
Base Station <BS> ID is: 005
Connected to the Authentication Server <AS> ....
Enter the Base Station <BS> ID to be transmitted to the Authentication Server <
AS>: 005
Transmitting.....
ThisBase Station <BS> is Trusted !!!!!!!
*****
    
```

FIGURE 11: The SS verified the BS.

7. COMPARATIVE STUDY

Paper [5] said the way to save the data exchange between MAC layer and the PHY layer. It also mentioned that the PHY layer cannot save itself against the attacks which intercept inside the wireless channel. Paper [6] shown the security aspects of the IEEE 802.16 Standard and point out the security vulnerabilities, threats and risks associated with this standard shortly. [7] Examined the MAC layer of the 802.16 standard to determine the presence of the denial of service attacks and also the attacks that may be unique to the 802.16 standard. But it did not point out the way to prevent these problems. It did not solve the BS authentication to save the legitimate SS except just discussing the problems a bit detail which left curiosity to researchers to find a way to figure out a solution and make this communication environment more secured and trustworthy.

8. CONCLUSION

Although being a new technology, this standard works with strong encryption algorithm, data encryption standard (DES) and with a strong key management scheme. Attacks on privacy, integrity and authentication can be overcome by taking some few necessary steps. Besides, the standard itself provides adequate solutions to defend against others major attacks which were somewhat concerning issues in previous standards. Base station authentication will make the whole communication secure and reliable which was not defined in the architecture of the IEEE 802.16 network though different separate works have been done so far and is still a concerning issue in data transmission. This paper solved this problem by ensuring mutual authentication technique for both base and subscriber station in a way that no intruders or outsiders can penetrate the network disguising themselves as part of it and doing unnecessary activities. The simulation result proved that when mutual authentication is established, a secure and reliable transmission can be achieved in point to point or point to multipoint communication in IEEE 802.16/WiMax network.

9. REFERENCES

- [1] Frank Ohrtman, WiMAX Handbook, building 802.16 WiMAX networks, McGraw-Hill 2005.
- [2] Mahmoud Nasreldin, Heba Aslan, Magdy El-Hennawy, Adel El- Hennawy. WiMax Security, 22nd International Conference on Advanced Information Networking and Applications Workshops 2008, p. 1335- 1340.
- [3] Kejie Lu and Yi Qian, University of Puerto rico, Hsiao-Hwa Chen, National Sun Yat-Sen University. A Secure and Service-Oriented Network Control Framework for WiMax Networks, IEEE Communications Magazine, May 2007.
- [4] Michel Barbeau, School of Computer Science, Carleton University, Canada. WiMax Threat Analysis, Q2SWinet'05, October 13, 2005, Montreal, Quebec, Canada.
- [5] Hyung-Joon Kim, IEEE 802.16/WiMax Security, Dept. of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, New Jersey, Unpublished.
- [6] Jamshed Hasan, School of Computer and Information Science, Edith Cowan University, Australia Security Issues of IEEE 802.16 (WiMax), [http://scissec.scis.ecu.edu.au/conference_proceedings/2006/aism/Hasan%20-%20Security%20Issues%20of%20IEEE%20802.16%20\(WiMAX\).pdf](http://scissec.scis.ecu.edu.au/conference_proceedings/2006/aism/Hasan%20-%20Security%20Issues%20of%20IEEE%20802.16%20(WiMAX).pdf).
- [7] Derrick D. Boom "Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks" IEEE C802.16e-04/406.
- [8] Loutfi Nuaymi, WiMAX Technology for Broadband Wireless Access, John Wiley & Son Ltd.