A NEW MECHANISM TO SOLVE IEEE 802.16 AUTHENTICATION VULNERABILITIE

Abdelrahman Elleithy, Alaa Abuzaghleh, Abdelshakour Abuzneid

Computer Science and Engineering Department
University of Bridgeport
Bridgeport, CT 06604

Abstract- Wi-Max (Worldwide) Interoperability for Microwave Access is a new technology that can provide broadband access at a high bandwidth. The availability of microwaves towers provides a very cost effective for delivering high bandwidth in metropolitan. Wi-Max is a multi-hop network where security is a major issue in designing such networks. Designing a secure Wi-Max is a major research challenge that has been approached in recent publications. In this paper we are discussing security changes of Wi-Max and suggesting a new authentication protocol.

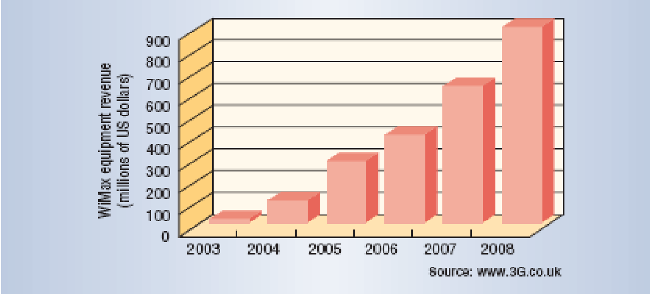
1. Introduction

The next generation of the IEEE802.16/WiMAX will be the most important component of the wireless system. The standard version of IEEE 802.16/WiMAX employed advanced radio transmission technology for example OFDM (orthogonal frequency division multiplexing), adaptive modulation and coding, and EFC (adaptive forward error correction). The main purpose of using IEEE802.16/WiMAX is to provide well defined quality-of-service broadband wireless capabilities.

IEEE 802.16/WiMAX technology needs a high rate transmission (about tens of Mbps), and strict quality-of-service for both indoor and outdoor medium. IEEE802.16 security weakness comes from the key length of DES of 56-bit. In addition to the IEEE802.16 link because the developers of the IEEE802.16 standard tried to avoid the problem in IEEE802.11 standard they tried to incorporate the existing standard into the IEEE802.16.

The IEEE802.16 physical layers have a lot of flexibility in its four shapes. Hence, the operation on the spectrum allocation will have a wide range in its channel bandwidth, frequency division duplex, and time division duplex. These four modes layers have significant tasks such as initial ranging, bandwidth requests, connection channel, and registration. Although there is a variation types for the physical layer, the security protocol will be the same.

The use of Wi-Max has increased significantly since its introduction in 2003. Figure 1 shows the exponential growth of Wi-Max between 2003 and 2008.



Source: www.3G.co.uk

Figure1: Increase of Wi-Max revenues from 2003 – 2008[7]

2. Security Vulnerabilities

A. Intrusion Detection Systems

IDS became an important tool for network administrators after the rising level of sophistication and automation of intrusive attacks. However, a poor choice in IDS systems can do more harm than good by providing a false sense of security. Research in IDS systems has flourished in the last decade and has attracted extensive efforts in the recent years.

IDS systems attempt to provide a safety net to other network security systems. An effective IDS implementation makes no assumptions about the effectiveness of other network security services. All activity is suspect and monitored to assess the perceived threat of the actions. Threatening behavior is responded to via logging, reporting or some action on the part of the IDS or related systems.

The value of an IDS system lies in its ability to accurately determine if an action is a result of an intrusion or normal behavior. Intrusion detection systems fall into two broad categories. The first approach is Statistical Anomaly Detection. The underlying premise of this approach is that an intruder's activity will differ from that of a legitimate user. Legitimate user behavior is derived by analyzing past activity. Aberrations that are outside expected deviations are reported as the act of an intruder. The strength of statistical approaches is that attacks are defined as any non-normal activity, so it can theoretically guard against any type of attack.

The second approach is Rules-Based Detection. A rules-based detection system defines specific activity as being an intrusion. The system looks for known attacks or defined behaviors and reports when these are observed.

B. Denial of Service Attacks (DOS)

Denial of services attacks (DOS) is a constant danger to web sites. DOS has received increased attention as it can lead to a severe lost of revenue if a site is taken offline for a substantial amount of time. There are many types of denial of service attacks but two of the most common are Ping of Death and TCP SYN Flood.

In a Ping of Death attack, a host sends hundreds of ping requests (ICMP Echo Requests) with a large or illegal packet size to another host in attempt to knock it offline or to keep it so busy responding with ICMP Echo replies that it cannot service its clients.

A TCP SYN Flood attack takes advantage of the standard TCP three-way handshake by sending a request for connection with an invalid return address.

3. Automatic Vulnerability Checking of IEEE 802.16 WiMax Protocols

In [1] the authors discuss several issues in the security of WiMax. They fear that there are some protocols that could interfere with the security of the WiMax network. The issue of the vulnerability of any analysis that is made by human is that they are lengthy and may have some errors that are not detected which may cause problems regarding security in WiMax. In the recent years, the IETF had concluded that researchers shall focus on what causing these attacks and that they need to find a way through security, to make WiMax network much secure.

There would still be issues in the security of WiMax, because these attacks are coming from complex protocols. In many cases of the attacks on the WiMax network sometimes it become difficult for a human mind to solve the problem. To solve the attacker problem we need to analyze its interaction, concurrently using this type of analysis it becomes an extremely difficult task.

Although this type of analysis may require a lot of time to solve the problems in the protocols, the researchers are trying to develop other methods – that can become formal in the future - that makes the analysis of a complex protocol to be time efficient and easy.

In [6], the authors proposed use of TLA+ as a formal technique to secure the network. There are many advantages of using TLA+ or using (TLA/TLC). TLA stands for Temporal Logic of Actions and it is defined as the following a program logic that expresses both programs and properties with a single language, then the paper gives a detailed example of TLA. Figure 2 shows TLA modeling process.

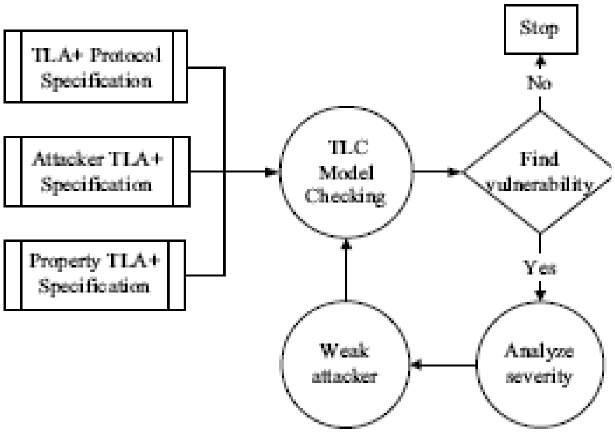

TLA+ Protocol Specification
Attacker TLA+ Specification
Property TLA+ Specification
TLC Model Checking
Find vulnerability
Stop
No
Yes
Analyze severity
Weak attacker

Figure 2: TLA modeling process[6]

4. Routing in Wi-Max

Wi-Max (Worldwide) Interoperability for Microwave Access is a new technology that can provide broadband access at a high bandwidth. The availability of microwaves towers provides a very cost effective for delivering high bandwidth in metropolitan. Wi-Max is a multi-hop network where security is a major issue in designing such networks. Designing a secure Wi-Max is a major research challenge that has been approached in recent publications.

Wimax provides high data rate communications in metropolitan networks (MANs). IEEE 802.16 Standard published in 2001 works in the 10-66 GHz band while IEEE 802.16a Standard published in 2003 works in the 2-11 GHz band. The current 802.16e standard works for mobile applications.

Wi-Max Network Architectures:

There are two network architectures considered for Wi-Max

(1) Point-to-multi-point (PMP)

.

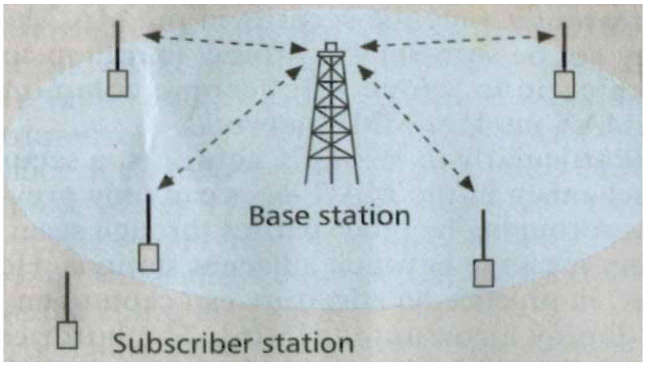


Figure 3: PMP Wi-Max Architecture[1]

(2) Mesh

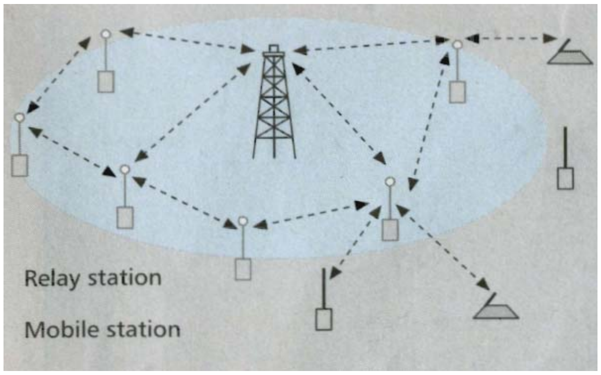


Figure 4: Mesh Wi-Max Architecture [1]

5. Wireless Broadband with Wi-Max

In [3], the paper discusses how wireless broadband can be achieved with WiMax. The authors explain the differences between wire-line infrastructure and wireless infrastructure. Furthermore, they show that the use of wire-line infrastructure is more time and money consuming than wireless infrastructure. Companies do not want to spend time and money to build an infrastructure that does not exist in some places because they think that these places will not make them the profit the company desired to get. The companies are trying to solve this issue; one of the approaches is the use of wireless infrastructure like the use of WiMax.

6. 802.16 Protocol

When two machines will be communicating using the IEEE802.16, the sender frames header will have two cells, one for the sender machine called DL_MAP, and the other for the receiver machine called UL_MAP. Each one of these frames will have information about the address, size, and encoding used in both of the two machines. Each cell of the MAC connection oriented belongs to specific connection, and each one of the entire connections is known by it's ID. Therefore, IEEE802.16 has two main types of connection; one of them is primary connection handles initialization of the connection, request the bandwidth, and broadcast the data. The other secondary connection uses the IP management packet in each receiving machine. The other connections are used for carrying propose and are created by the IEEE802.16 link as needed. The IEEE802.16 carrying, and secondary connections are secure.

Due to the variation of the MPDU header, IEEE802.16 packet will have two formats as it is shown in figure 5.

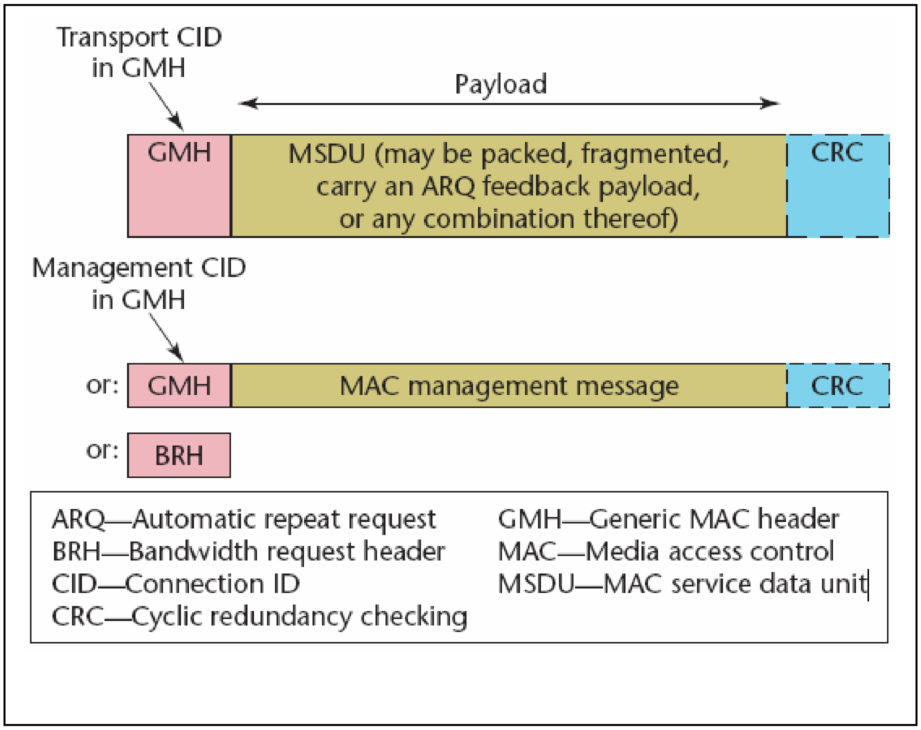

Transport CID
in GMH
Payload
GMH
MSDU (may be packed, fragmented,
carry an ARQ feedback payload,
or any combination thereof)
CRC
Management CID
in GMH
or:
GMH
MAC management message
CRC
or:
BRH
ARQ—Automatic repeat request
BRH—Bandwidth request header
CID—Connection ID
CRC—Cyclic redundancy checking
GMH—Generic MAC header
MAC—Media access control
MSDU—MAC service data unit

Figure 5: IEEE802.16 packet shape[5]

As it is clear from Figure 5 one the IEEE802.16 has the following packet shapes:

- Bandwidth request header: the header is in the packet.
- Generic MAC header: the payload is followed by CRC (Cyclic Redundancy Checking).

The management packet is controlled by the connection ID; each management packet is containing single MAC management information. The transport (carrying) connection is handling the data through stack over the MAC. Hence, IEEE802.16 has an easy way to carry MSDU by MPDU.

The network entry has a lot of sequential operation occurs when the connection between two station is needed; firstly the SS (subscriber station) will try to find BS (base station) signal to establish the connection parameter After that the initial ranging will help the SS to define the physical layer in good way. In this phase, authorization and key management will occur. Next the SS is authorized to BD by PKM (privacy key management). After that the SS will send message to the BS so BS will assign connection ID for secondary management connection. Finally, both SS and BS will create the transportation connection.

The function of the security algorithm which is build under the MAC layer is to provide confidentiality, and access control to the data link.

The five significant parts of the IEEE802.16 security algorithm are security association, X.509 certificate profile, PKM authorization, privacy and key management, and encryption.

To authorize SA authorization by the standard:

- Define the SS by X.509 certificate.
- 160-bit for authorizing key.
- 4-bit to define the AK (authorization key).
- The AK age vary between one and 70 days.
- a 112-bit Triple-DES key
- download and upload hash function

X.509 certificate profile requires the following fields to work correctly:

- X.509 certificate format version 3.
- Certificate serial number.
- Certificate issuer's signature algorithm Public Key
- Cryptography Standard 1—that is, RSA encryption with SHA1 hashing.8
- Certificate issuer.
- Certificate validity period.
- Certificate subject—that is, the certificate holder's
- Identity, which, if the subject is the SS, includes the station's
- MAC address.
- Subject's public key, which provides the certificate holder's public key, identifies how the public key is used, and is restricted to RSA encryption.
- Signature algorithm, which is identical to the certificate issuer's signature algorithm.
- Issuer's signature, which is the digital signature of the Abstract

PKM authorization consists from three messages that transport between SS and BS. Privacy and key management is also consisting of two or three messages between SS and BS. Encryption is important for the data part of the MPDU; in other hand it does not cipher the header of MPDU.

7. A new authentication mechanism to solve 802.16 Protocol Authentication Problems

The IEEE 802.16 lacks means for authenticating the BS to the SS which leaves the PKM protocol open to forgery attacks. The SS cannot verify that any authorization protocol messages it receives were generated by an authorized BS. The BS constructs the authorization protocol responses it sends to an SS using entirely public information, so any rogue can create a response. Requiring the SS to authenticate to the BS can eliminate this vulnerability. The authorization protocol subjects the SS to replay attacks. [5]

New suggested Authentication Protocol

In order to prevent the replay attach between the SS and the BS we suggest the following authentication protocol:

1. SS→KDC: $ID_{SS} \| ID_{BS} \| N1$

2. KDC→SS: $E_{Kss}[Ks \| ID_{BS} \| N1 \| E_{Kbs}[Ks \| ID_{SS} \| TS_1]]$

3. SS→BS: $E_{Kbs}[Ks \| ID_{SS} \| TS_1]$

4. BS→SS: $E_{Ks}[N2]$

5. SS→BS: $E_{Ks}[f(N2)]$

Figure 6 shows the state diagram of the proposed protocol.

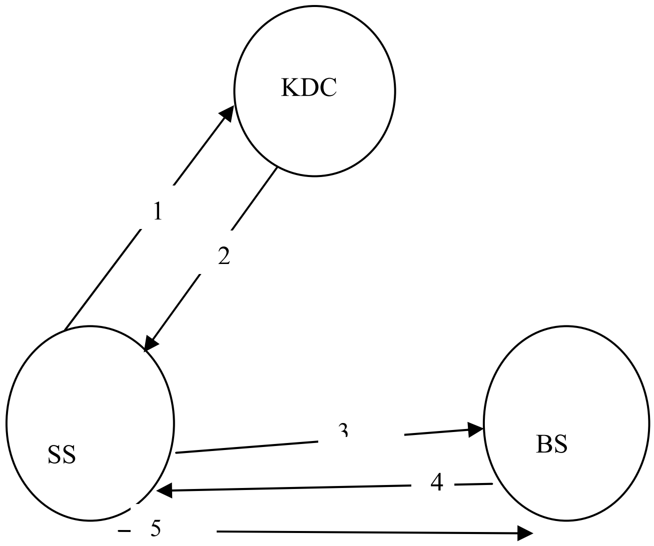


Figure 6: the state diagram of the proposed protocol.

8. Conclusions

In this paper we have studied the security vulnerabilities of Wi-Max. It was found that Wi-Max is subject to replay attacks. We have suggested a new protocol for authentication of the Base Station (BS) to the Subscriber Station (SS) to prevent reply attacks. We believe incorporating this modification in future versions of IEEE.16 can improve the security of Wi-Max.

References

1. Kejie Lu, Yi Qian, and Hasio-Hwa Chen, “A Secure and Service Oriented Network Control Framework for Wi-Max Networks,” IEEE Communications Magazine, May 2007.

2. Qiang Ni, Alexey Vine, Yang Xiao, Andrey Turlikov, and Tao Jiang, “Investigation of Bandwidth Request Mechanisms under Point-to-Point Mode of Wi-Max Networks,” IEEE Communications Magazine, May 2007.

3. Dusit Niyato and Ekram Hossain, “Integration of Wi-Max and Wi-Fi, Optimal Pricing for Bandwidth Sharing,” IEEE Communications Magazine, May 2007.

4. Ekram Hossain, “IEEE802.16/WiMAX-Based Broadband Wireless Networks: Protocol Engineering, Applications, and Services”, Fifth Annual Conference on Communication Networks and Services Research, 2007.

5. David Johnston and Jesse Walker, “Overview of IEEE 802.16 Security”, IEEE Security and Privacy, 2004, pp. 40 - 48.
6. Prasad Narayana, Ruiming Chen, Yao Zhao, Yan Chen, Zhi (Judy) Fu, and Hai Zhou, “Automatic Vulnerability Checking of IEEE 802.16 WiMAX Protocols through TLA+ “ , 2006.

7. Steven J. Vaughan-Nichols, “Achieving Wireless Broadband with WiMax “, Computer, June 2004, pp. 10 – 13.

Biographies

Abdelrahman Elleithy has received his BS degree in Computer Science from the University of Bridgeport in May 2007. Currently he is pursing his MS degree in Computer Science from the University of Bridgeport. Abdelrahman has research interests in computer networks and mobile communications. He has received special training in the fabrication technologies of micro-electro-mechanical systems in the New Jersey Institute of Technology in summers of 2006 and 2007.

Ala'a Abuzaghleh is a MS student in the department of Computer Science and Engineering at the University of Bridgeport. He has research interests in object oriented programming and web applications.

Abdelshakour Abuzneid has received his BS degree in Computer Engineering and Control from Yarmouk University and MS degree in Computer Engineering from the University of Bridgeport in May 2007. Currently he is pursuing his PhD in Computer Science & Engineering from the University of Bridgeport. His research interest is in Data / computer / wireless / mobile communications. He has published few journal and conference papers. Abelshakour has 12 years of experience in this field.