Security issues and proposed solutions concerning authentication and authorization for WiMAX

(IEEE 802.16e)

Bart Sikkens
Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente, the Netherlands
sikkensb@cs.utwente.nl

ABSTRACT
In this paper, a research is described analyzing the solutions to the security issues in WiMAX (802.16e). At first a global overview of the technology WiMAX is given followed by an explanation of authentication and authorization for WiMAX. Then the security issues mentioned in literature are presented along with possible solutions. Next, the solutions are analyzed using criteria which are also proposed in this paper.

Keywords
WiMAX, security, IEEE 802.16, authentication, authorization

1. INTRODUCTION
The latest development in wireless metropolitan area networks is IEEE 802.16, also known as WiMAX (Worldwide Interoperability for Microwave Access) [IEEE04] [IEEE06] [Hos06]. This new standard brings us higher range and speeds compared to 802.11 (WLAN, wireless local area network). The standard is still evolving these days and many problems are not solved yet.

One major issue of WiMAX is security. Several scientific papers call this a big problem. For example [YZZ+05] tells us: "But the security problems in its original protocol may be becoming the most serious obstacle in its marketable producing process." [LL06] states: "As the mobile services supported in the standard, new security problems may be coming and becoming a serious obstacle to develop the WMAN (Wireless Metropolitan Access Network)."

The latest standard for WiMAX, IEEE 802.16e [IEEE06], already offers significant security improvements over 802.16-2004 [IEEE04]. It uses better encryption methods and has a more secure key management protocol. Also a new authentication method based on EAP (extensible authentication protocol) [DCA06] [Man03] was added. But still a lot of security issues remain to be solved. Security, and especially authentication and authorization, is crucial to every wireless technology, because without good security the technology is not usable at all.

Several researchers have published solutions on the security issues of WiMAX, but are these solutions satisfactory? A literature search showed that no study has been done yet answering this question. In this research we will answer that question with a focus on the authentication and authorization part for 802.16e. This paper gives a state of the art on security solutions for WiMAX and it provides a comparison of these solutions based on certain criteria.

1.1 Research questions
The main research question for this paper is:

- Are the proposed security solutions concerning authentication and authorization for WiMAX satisfactory based on certain criteria?

This question will be divided into the following subquestions:

- What are the main authentication and authorization aspects in WiMAX?
- What are the main security issues associated with authentication and authorization for WiMAX?
- What are the proposed solutions in literature for these security issues?
- What criteria can be used to analyze those solutions?
- Which security solutions satisfy the criteria?

1.2 Research method
The research will be done using a literature review and a qualitative analysis and a comparison of several security solutions for WiMAX. At first, in section 2, WiMAX, especially the authentication and authorization of WiMAX, will globally be explained. Next, in Section 3, we will discuss the security issues found in literature. Furthermore, Section 3 discusses the proposed solutions that could solve the security issues and/or improve the overall security of WiMAX authentication and authorization. Then in Section 4, we will make an analysis of the solutions based on certain criteria that are derived from the literature study. Finally, Section 5 will provide the conclusions and the future work activities.

2. BASIC CONCEPT OF WIMAX
WiMAX can be shortly described as: “a telecommunications technology aimed at providing wireless data over long distances in a variety of ways, from point-to-point links to full mobile cellular type access. It is based on the IEEE 802.16 standard.” from [Wik07].

There are a lot of different protocol standards for WiMAX already, varying from 802.16a to 802.16m. All standards can be found at the official IEEE website: [IEEE07]. The most relevant for this paper are 802.16d (officially called 802.16-2004) and 802.16e (802.16e-2005). [IEEE04] [IEEE06] The first is also
called fixed WiMAX, the latter mobile WiMAX. The reason for that is that 802.16d does not support mobility and 802.16e does. Mobility was added as an amendment to 802.16-2004 in 2005 and officially published in 2006.

In figure 1 we see the general WiMAX architecture represented as a network reference model (NRM). It shows the important entities and their interaction (R1-R5).

Mobile Station (MS or subscriber station, SS) is a “Generalized mobile equipment set providing wireless connectivity between one or more hosts and the WiMAX network.” from [INV07].

Network access provider (NAP) can be described as: “a business entity that provides WiMAX radio access infrastructure that is implemented using one or more ASN’s.” from [INV07].

ASN stands for Access Service Network and it “represents the point of entry for WiMAX MS equipment into a WiMAX network, and as such, must support a complete set of network functions required to provide radio access to the MS.” from [INV07]. One should think of things like network detection, radio resource management, QoS (quality of service) etcetera.

Network service providers (NSP) are business entities that provide IP connectivity and WiMAX services.

The connectivity service network (CSN) provides IP connectivity services. It consists of routers, servers, user databases and gateway devices and it delivers for example internet services, roaming functionality and peer-to-peer services.

2.1 Authentication and authorization

In this chapter we will first explain the basic security aspects of WiMAX considering authentication and authorization. Authentication addresses establishing the genuine identity of the device or user wishing to join a wireless network. Authorization addresses determining whether the authenticated user or device is permitted to join the network, see [DCA06].

When a subscriber station (SS) wants to connect to a WiMAX base station (BS), see [Aiko06], at first a connection is established between them. The next step is the authentication of the SS so it can enter the network. SS sends a so-called X.509 certificate [Hou02] to BS to identify itself. The certificate is like a signature for the SS. It contains data like a serial number, the certificates issuer, the public key of the sender, its MAC-address etcetera.

After the authentication message SS sends an authorization message to BS. This message contains SSs supported authentication and data encryption algorithms. If BS determines that SS is authorized it sends a message back containing an authentication key (AK), a 4-bit sequence number and a lifetime for it containing the number of seconds before it expires [Aiko06]. See figure 2 for a graphical representation. MS refers here to a mobile subscriber station (SS).

When all these steps have been done successfully, the SS has entered the network of BS and it can communicate with all the entities in its network.

MS | Send basic CID | BS
---|---|---

| Authentication Information |
| Authorization Request |
| Authorization Reply/Reject |
| (AK exchange) |
| Key Request |
| Key Reply/Reject |
| (TEK exchange) |

The communication between SS and BS is protected by the so-called security associations (SAs). These SAs perform encryption on the data between SS and BS using a ‘traffic encryption key’ (TEK). Different types of encryption are supported. For more details see [Aik06].

3. SECURITY ISSUES AND SOLUTIONS

In this section we will present some security issues for WiMAX found in literature and discuss which solutions are proposed for these issues.

3.1 DoS (Denial of Service) /Replay attack

In [LL06] the following DoS attack is described. If a SS sends a lot of false authorization requests to a BS, the BS will use all its resources to calculate whether the certificate is right. This will cause a DoS, because BS will not be able to serve any SSs anymore.

Another DoS attack possibility is described in [XMH06], where an adversary eavesdrops the authentication message from a SS to a BS. Then he replays this message multiple times to the BS, which will make the BS ignore the SS and thus creating a Denial of Service.

In the first type of DoS attack, the BS will not be able to serve any SSs anymore. In the second type of DoS attack, only the SS whose message got eavesdropped will experience the attack.

3.1.1 Solution [XMH06]

In this solution some modifications to the authentication protocol and the key management protocol are proposed to solve both this security issue and the authorization vulnerability issue, see Section 3.2.
As a solution, [XMH06] proposes to add a timestamp to the authentication messages of the original protocol (see figure 3) and a signature of SS and BS which provides message authentication and prevents that SS gets rejected by BS. The signature of SS uses its private key to encrypt the critical information in the message. The result can be seen in figure 4.

By adding the timestamps and signatures, freshness can be guaranteed for both messages. This way both SS and BS know that the message is fresh and not intercepted and replayed.

The key management protocol (see figure 5) is also vulnerable for these attacks. Both the message from BS to SS and vice versa can be replayed to cause DoS or other unwanted behaviour.

In figure 5 and 6, HMAC stands for Hash Message Authentication Code, see [Kra97]. [Wik07-2] defines it as following: “HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.”

What happens is that SS requests (or BS forces him to, using message 1) a new TEK in message 2. HMAC(2) can be used by SS to detect forgery attacks. HMAC(2) assures BS that the message is authentic. HMAC(3) assures SS that message 3 is from BS and has not been modified.

Figure 3. Original authentication protocol [XMH06]

In figure 3 and 4 ‘Cert’ stands for the X.509 certificates used. ‘KUss(AK)’ is the Authentication Key encrypted by SSs public key. Ts and Tb are timestamps of respectively the SS and BS. SeqNo and Lifetime are a sequence number and lifetime for the AK. SIGss and SIGbs are signatures for respectively the SS and BS. The SAIDList defines the security associations ID’s to be used for communication.

By adding the timestamps and signatures, freshness can be guaranteed for both messages. This way both SS and BS know that the message is fresh and not intercepted and replayed. The key management protocol (see figure 5) is also vulnerable for these attacks. Both the message from BS to SS and vice versa can be replayed to cause DoS or other unwanted behaviour.

In figure 5 and 6, HMAC stands for Hash Message Authentication Code, see [Kra97]. [Wiki07-2] defines it as following: “HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.”

What happens is that SS requests (or BS forces him to, using message 1) a new TEK in message 2. HMAC(2) can be used by SS to detect forgery attacks. HMAC(2) assures BS that the message is authentic. HMAC(3) assures SS that message 3 is from BS and has not been modified.

Figure 4. Revised authentication protocol [XMH06]

In figure 3 and 4 ‘Cert’ stands for the X.509 certificates used. ‘KUss(AK)’ is the Authentication Key encrypted by SSs public key. Ts and Tb are timestamps of respectively the SS and BS. SeqNo and Lifetime are a sequence number and lifetime for the AK. SIGss and SIGbs are signatures for respectively the SS and BS. The SAIDList defines the security associations ID’s to be used for communication.

3.2 Authorization vulnerability

In [LL06] is emphasized that WiMAX uses mutual authentication to protect from forgery attacks, but the authorization process is still vulnerable because there is no way to ensure integrity of the messages. Anyone with a properly placed radio receiver can catch an authorization message, modify and retransmit it. There is no digest used to prove that the message has not been modified.

3.2.1 Solution [XMH06]

As mentioned in Section 3.1.1 [XMH06]’s solution also solves the authorization vulnerability issue.

3.3 Key space vulnerability

In 802.16e, a 4-bit key sequence number is used to distinguish between successive generations of AKs. Also, a 2-bit key sequence number is used for the same purpose with TEKs. The size of the key is insufficient to protect the keying material from attacks according to [LL06].

3.3.1 No solutions

No solutions were found in literature, which is strange, because the problem can easily be solved by increasing the number of bits for both keys. They could be for example both 8 bits. This would mean a few more bits to send, but not enough to decrease the performance significantly. The main disadvantages are however that the used encryption and decryption mechanisms will have to be modified. This will probably increase the complexity and will require a standardization action.

3.4 Downgrade attack

The first message of the authorization process is an unsecured message from SS telling BS what security capabilities he has. An attacker, see [MPF07], could send a spoofed message to BS containing weaker capabilities in order to convince the BS and the attacked SS to agree on an insecure encryption algorithm. The standard does not specify a concrete solution for the situation that two valid answers are received by a BS.

3.4.1 No solutions

For the downgrade attack there are no solutions found in literature. A search to downgrade attacks in other wireless technologies gave no result as well. A possible solution could be to ignore messages with security capabilities under a certain limit. This could lead to DoS for SSs that do not have the required capabilities though.
3.5 Authorization attack

According to [HLY07] it is possible for a malicious radio receiver to make both an honest SS enter his network and to get permission to enter an honest BSs network. This can be done by recording messages and replaying them to the BS and SS. They describe the problem as “lack of clear clarification of intended receiver”.

3.5.1 Solution [HLY07]

To understand the solution, we will first take a look at the RSA-based PKMv2 authorization protocol which is used in [HLY07]. PKMv2 stands for privacy and key management protocol version 2, which is the version used in 802.16e, see [IEEE06].

RSA is a type of encryption, see [RSA02] for the official standard. It is an algorithm for public-key cryptography. It was the first algorithm known to be suitable for signing as well as encryption. It is also one of the first great advances in public key cryptography. RSA uses both a public key and a private key. Messages encrypted with the public key can only be decrypted using the private key. Information in this section comes from [Wik08].

```
MS → BS: MS_Random, MS_Cert, SAIID, Sig_MS
BS → MS: MS_Random, BS_Random, [Key]
    MS_MAC_Adr], Kms, Key_Life,
    Key_Seq, BS_cert, Sign_BS
MS → BS: BS_Random, Auth_Result, Sign_MS
```

Figure 7. RSA-based PKMv2 [HLY07]

In figure 7 the RSA-based PKMv2 authorization protocol is shown. The randoms are random numbers generated by either MS or BS. MS_MAC_Adr is MSs MAC-address. \([\{\}]\)Kms represents that the message between braces is encrypted by public key Kms. Auth_result is an acknowledge message for BS.

The protocol is similar to that given in figure 3, but the first message there, which is optional, has been left out here. Another difference is the last message given here, where the MS sends an acknowledge message to BS.

In message two, MS_MAC_Adr identifies the intended receiver, but the third message misses such a clarification of the intended receiver. The proposed solution for the authorization attack in [HLY07] is to add a BSID (base station ID) to the last authentication message. This would make clear which BS the intended receiver is, just as the MAC-address in message two does. It will not be possible then for the malicious radio receiver to let an SS enter his network and to enter another BSs network.

3.6 Other issues and solutions

This section will show other solutions that do not address the specific problems mentioned previously, but try to improve the performance and/or security in general.

The first solution avoids the need for a relatively large security key for encryption. The second makes the interception of security keys harder.

3.6.1 Wireless Public Key Infrastructure (WPKI) [LL06]

[LL06] proposes an enhancement to the 802.16e security called Wireless Public Key Infrastructure (WPKI). The two major changes are Elliptic Curve Cryptography (ECC) and Wireless Transport Layer Security (WTLS) certificates.

ECC, as defined in [Cer00], will replace RSA [RSA02] as encryption method. The advantage of ECC is that the same encryption strength can be reached with a much smaller key size. WTLS defines a compressed certificate format, similar to X.509 [Hou02] but using smaller data structures.

Simulation results in [LL06] show that the WPKI-mechanism has less delay in finishing the authentication, while security is just as good using a smaller key size (see figure 8). The X-axis shows the numbers of the simulation runs and the Y-axis the authentication delay in milliseconds. In thirty simulation runs RSA does not win once from ECC.

![Figure 8. Lower delay using ECC instead of RSA [LL06]](image)

3.6.2 Secure and service-oriented network control framework [LQC07]

[LQC07] proposes “a secure and service-oriented network control framework”. It exists of two major components, a service-aware control scheme and a unified routing scheme. The first is aware of the services available in the network. The latter forwards packages based on service and security requirements.

A security improvement for key management is the fact that keys can be sent through multiple paths to the server (see figure 9). This way intercepting the security key will be a lot harder, because in order to capture it all fragments need to be intercepted and rearranged in the right order. The framework also supports secure routing. The solution is theoretical and no simulations or other experiments have been done.

![Figure 9. Multipath routing [LQC07]](image)
4. ANALYSIS OF SOLUTIONS

This section will first introduce a set of criteria and then analyze the proposed solutions using those criteria.

4.1 Criteria

To analyze the proposed solutions we will need a set of criteria. These criteria will be the following:

- **Performance of the solution**, how does the solution perform in terms of delay and how large are the data structures used?
- **Need for modifications in standards**, does the standard need to be completely redefined or are there only small changes necessary to encapsulate the solution into the standard?
- **Scalability**, does the solution scale well (maintaining an acceptable performance rate) when it is used in a large network where many users are supported?
- **Authentication improvement**, are the authentication vulnerabilities solved?
- **Authorization improvement**, are the authorization vulnerabilities solved?

4.2 Analysis

In this section we will look, per issue, at all solutions using the criteria mentioned above.

For each solution there is a table showing how they score on each criterion. A ‘+’ means it scores well on that criterion, a ‘+/-’ that it is doubtful and a ‘-’ means a bad score. A ‘?’ means no information was available for that criterion, for example no performance information because no simulations were ran.

4.2.1 DoS/Replay attack

[XMH06] shows good improvements for authentication and authorization against replay attacks. Adding the timestamps and signatures requires a reasonable modification to the standard. No information is available about performance but our expectation would be a small drop in performance. Although the solution is decentralized, the increase in message size is not dramatically. However, due to the introduction of timestamps and signatures, scalability might be affected.

Table 1. Analysis DoS/Replay attack

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Own</td>
<td>?</td>
<td>+/-</td>
<td>?</td>
<td>+</td>
</tr>
</tbody>
</table>

4.2.2 Authorization vulnerability

The solution of [XMH06] also solves the authorization vulnerability issue. See Section 4.2.1 and table 1 for the analysis results.

4.2.3 Key space vulnerability

No solution was found for this issue even though there is a logical solution, namely increasing the security key sizes. This should effectively solve the problem with a small change to the standard. The message size will only increase with a few bits, so it might not affect performance too much. However, the increase in the security key size will require a modification on the used encryption and decryption mechanism, which might impact the scalability.

4.2.4 Downgrade attack

For the downgrade attack as well no solutions were found in literature. We proposed a solution to this problem, but it may exclude SSs with low security capabilities, thus creating a new problem. We expect that the solution will have almost no impact on performance, because only a small change to the BS certificate check has to be made. However, experiments are needed to verify this. Scalability will probably not be affected.

Table 2. Analysis Key space vulnerability

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Own</td>
<td>?</td>
<td>+/-</td>
<td>?</td>
<td>+</td>
</tr>
</tbody>
</table>

4.2.5 Authorization attack

[HLY07] gives a simple solution to the authorization attack. It only adds one ID to one message, so it will not decrease performance significantly. Experiments are however needed to define the exact impact of this change on performance. The use of the ID might imply that the encryption and decryption algorithms will have to consider all the IDs supported in the network. This might affect the scalability significantly. The need for modification of standards is small because only one ID has to be added and the vulnerability is solved effectively.

Table 3. Analysis Downgrade attack

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Own</td>
<td>?</td>
<td>+/-</td>
<td>?</td>
<td>+/-</td>
</tr>
</tbody>
</table>

4.2.6 Other issues and solutions

This section analyzes the solutions described in Section 3.6.

4.2.6.1 WPKI [LL06]

[LL06] clearly has a performance advantage over the old security, because it reduces the size of data structures. This sounds good, but it does not really solve a security issue. The size reduction of the data structures can improve the scalability of the solution. It looks like WPKI can be encapsulated without making too many changes to the standard.

Table 4. Analysis Authorization attack

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HLY07</td>
<td>?</td>
<td>+</td>
<td>?</td>
<td>+</td>
</tr>
</tbody>
</table>

4.2.6.2 Secure and service-oriented network control framework [LQC07]

[LQC07] shows a theoretical framework. Authentication and authorization could profit from keys being sent through multiple paths. Due to the fact that an additional layer is needed, this will mean that the modifications on the standard will be severe. Because of the theoretical nature of the framework nothing can be said about performance and scalability.
4.3 Complete solution
An interesting question would be if there is a complete solution possible combining multiple or even all solutions mentioned in this paper.

We think it is possible to combine all solutions mentioned together into one complete solution. The modifications to the authentication and key management protocol, the increase of key size and the solution to the downgrade attack should be able to work next to each other and together. The new encryption and certificates of WPKI should not interfere with the other solutions. The secure and service-oriented network control framework should be able to work as a layer above standard security.

Together they could be an interesting enhancement to the current 802.16e security. But is has to be said that more research needs to be done regarding the implementation complexity, performance and scalability of such an all-in-one solution.

5. CONCLUSIONS AND FUTURE WORK
This paper started by describing what WiMAX is and especially how its authentication and authorization works. Then we looked at security issues and described the solutions proposed in the literature. Finally, we analyzed those solutions and concluded that a complete solution combining all solutions mentioned should be possible.

The next conclusion to be made is that although security in 802.16e is certainly not perfect yet, not many solutions have been proposed yet in literature. The explanation for this could be that the 802.16e standard was only published in 2006 and maybe we can expect to see more solutions coming up in 2008.

5.1 Conclusions on issues and solutions
In this section we will look at all solutions and conclude whether they are satisfactory.

[XMH06] effectively solves the DoS/Replay attacks and the authorization vulnerability. It requires a reasonable modification to the standard, but it is hard to estimate the exact effect on performance and scalability. If it will score well on those criteria, we would call it a decent solution.

We proposed a personal solution to the key space vulnerability issue. However, experiments are needed to validate the behavior and performance of this solution.

We also proposed a solution for the downgrade attack that basically solves the problem, though creating another issue. For that reason this solution cannot be considered to operate satisfactorily.

[HLY07] is used to solve the authorization attack. The need for modification is low. The expectation is only a small performance drop, but more research is needed to confirm this and to investigate the scalability of this solution.

[LL06] does not really solve a security issue. What this solution however does is reducing the key size for encryption, thus reducing message size and increasing performance. So their changes to encryption and certificates score well in terms of performance and scalability, but are bad from the point of authentication and authorization improvement.

[LQC07] provides a theoretical framework that could provide several security advantages. Due to the fact that an additional layer is needed, a severe modification on the standard is required. Due to the fact that no simulation results are known, no conclusions on scalability and performance can be drawn.

Our overall conclusion is that both [HLY07], [XMH06] and our proposed solution for the key space vulnerability issue do a good job solving several issues. When combined they would certainly form a nice enhancement to WiMAX security. [LL06] disappoints a bit solving no real security issue and [LQC07] sounds promising, but simulations and other experiments need to be performed and the real value of improved security is not clear yet.

5.2 Future work
Future work activities can be related on performance experiments of the listed solutions, in order to evaluate their performance and scalability. For the solution to the key space vulnerability, it will be necessary to find key sizes that provide a balance between security and performance/scalability. Furthermore, the investigation and design of a solution that combines multiple or all current solutions into one would be very interesting. We believe that such a solution is possible, but more research is required on the implementation complexity and on the performance/scalability of this all-in-one solution.

ACKNOWLEDGMENTS
I would to thank Georgios Karagiannis for his support and good advices during the whole process. I also want to thank my fellow students for their critical reviews and advices.

REFERENCES


[Bar05] Michel Barbeau, WiMax/802.16 Threat Analysis, Q2SWinet’05, October 13, 2005, Montreal, Quebec, Canada


[CH07] Chung-Kuo Chang, Chin-Tser Huang, Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks, 2007 International Conference on Parallel Processing Workshops (ICPPW 2007)


[FHP07] Eduardo B. Fernandez, Michael VanHilst and Juan C. Pelaez, Patterns for WiMax security, Department of Computer Science and Engineering Florida Atlantic University Boca Raton, FL, USA, 2007
[Has06] Jamshed Hasan, Security Issues of IEEE 802.16 (WiMAX), School of Computer and Information Science, Edith Cowan University, Australia, 2006


[IEEE07] IEEE standards regarding the 802.16 technology, http://ieeexplore.ieee.org/xpl/standards.jsp?findtitle =802.16&letter=802.16&imageField.x=0&imageField.y=0&opentree=on


[LL06] Fuqiang Liu, Lei Lu, A WPKI-based Security Mechanism for IEEE 802.16e, IEEE Communications Society, Wuhan University, China 2006

[LQC07] Kejie Lu; Yi Qian; Hsiao-Hwa Chen, WIRELESS BROADBAND ACCESS: WIMAX AND BEYOND - A Secure and Service-Oriented Network Control Framework for WiMAX Networks, IEEE Communications Magazine • May 2007

[Man03] Jeff Mandin, Enhancement of 802.16e to Support EAP-based Authentication, Suggestion for improvement of 802.16e security on behalf of the Security Ad Hoc group, http://www.ieee802.org/16/tge/contrib/C80216e-03_71r2.pdf


