# WiMAX Security Issues in E-learning Systems

**Felician ALECU, Paul POCATILU, Sergiu CAPISIZU**

*Economic Informatics Department, Academy of Economic Studies*
*Pta. Romana 6, sector 1, Bucharest, ROMANIA*
*Economic Informatics Department, Academy of Economic Studies*
*Pta. Romana 6, sector 1, Bucharest, ROMANIA*
*Bucharest Bar Association*
*Bucharest, ROMANIA*
*alecu.felician@ie.ase.ro, ppaul@ase.ro, capisizu@mb.euroweb.ro*

***Abstract***: WiMAX (Worldwide Interoperability for Microwave Access) is a point-to-multipoint wireless network based on IEEE 802.16 standard. The WiMAX signal is broadcasted from a base station to the wide-geographically spread receivers. WiMAX enabled mobile devices become very popular due to the fact the network connections can be easily maintained on move. Regarding the network security, WiMAX provides strong user authentication, access control, data privacy and data integrity using sophisticated encryption technology. WiMAX technology is the only solution for isolated locations where e-learning distributed platforms need to be used. This paper focuses on security issues for e-learning solutions, especially when WiMAX technology is used.

***Keywords***: WiMAX, security, e-learning solutions, mobile networks, cloud computing.

## 1. Introduction

E-learning is widely used today on different educational levels: continuous education, company trainings, academic courses, etc. The educational process is a complex service which involves a producer and a consumer.
There are various e-learning solutions from open source to commercial. There are at least two entities involved in an e-learning system: the students and the trainers.
The students' actions within an e-learning platform are:

- Taking online course
- Taking exams
- Sending feedback
- Sending homework, projects

The trainers involved in e-learning solutions are:

- Dealing with content management
- Preparing tests
- Assessing tests, homework, projects taken by students
- Sending feedback
- Communicating with students (forums)

Each of these actions requires a certain degree of security, depending on the importance and data sensitivity.
The e-learning solution can be implemented in inaccessible locations (isolated localities and communities) using several mobile technologies: GSM/UMTS, WiMAX etc.
One of the promising technologies is WiMAX. It provides high speed data transfer and can be used in such locations, where other communications technologies are not available.
The typical WiMAX applications are related to broadband data connections (including rural areas or geographically isolated locations), Voice over IP (VoIP), Metrozones and digital television.

*This is a post conference paper. Parts of this paper have been published in the Proceedings of the SECITC 2009 Conference (printed version).*

## 2. The WiMAX Technology

WiMAX stands for Worldwide Interoperability for Microwave Access, a telecommunication technology based on WirelessMAN standard (802.16) [1]. WiMAX provides wireless data transmission using different transmission modes, from point-to-point to complete cell access.
The standard was created in 2001 by the collaboration of Intel and Alvarion companies and ratified by the IEEE under the name IEEE-802.16.
The WiMAX name and logo (figure 1) were created by WiMAX Forum, a nonprofit organization established to promote the adoption of WiMAX compatible products,

ISSN 2067 – 4074

services and to ensure a high level of interoperability among them.

Fig. 1 The WiMAX logo

The "fixed WiMAX" (802.16-2004 or 802.16d, fixed line connection with a roof mounted antenna) has no support for mobility and it was used to develop the "mobile WiMAX" standard, known as 802.16-2005 or 802.16e. Figure 2 depicts the components of a WiMAX network.

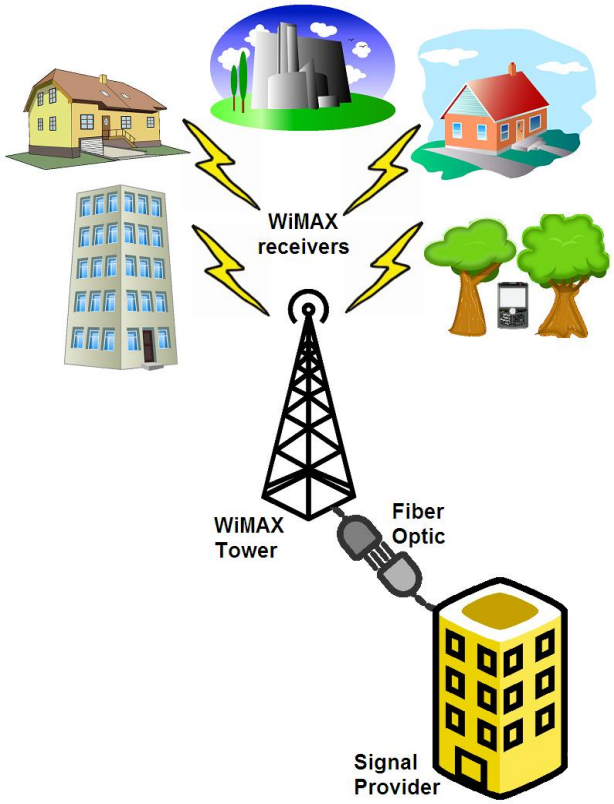


Fig. 2 WiMAX Network

A minimal WiMAX system consists of the following two components [2]:

- WiMAX base station – the place where the WiMAX signals are broadcasted from. It is connected to the public network using fiber optics, radio links or other high-speed point-to-point. Regularly the WiMAX towers (that works exactly like GSM network phones towers) are playing the role of the base station together with some electronic devices. These towers can cover up to 50 kilometers radius but due the geographic limitations the distance is just about 10 kilometers. Any wireless device that is WiMAX compliant can connect to the network if fallen into the base station range;
- receiver(s) – devices used to receive the signals from WiMAX base station. The receivers are allowing the mobile devices to connect to the WiMAX network. The mechanism is very similar to the Wi-Fi access, the only difference is the longer distance covered by WiMAX (figure 3).

Typically, one base station can connect to several other base stations by microwave links at high speed. This connection is called *backhaul* and it allows the existence of WiMAX roaming by maintaining connections on move.

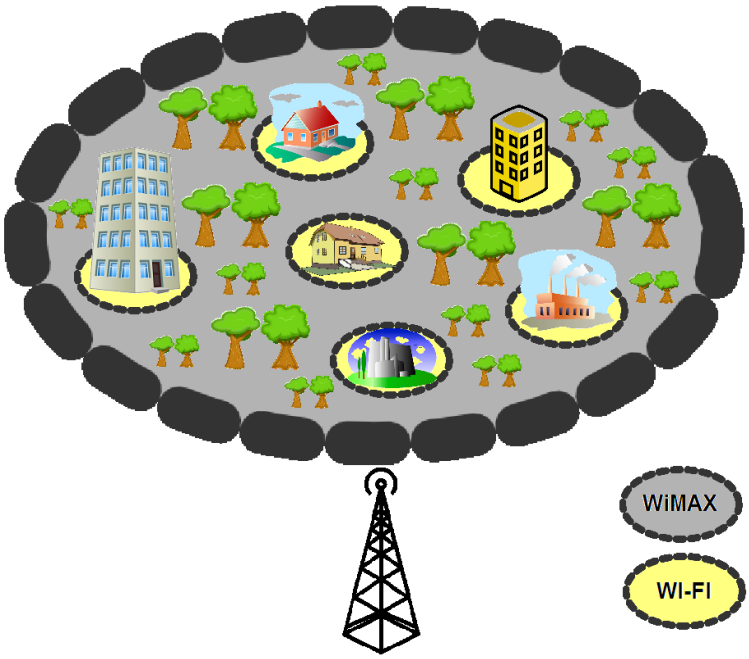


Fig. 3 WiMAX vs. Wi-Fi

The WiMAX provides high-speed Internet access on a radius around 50 kilometers. The technology doesn't require the receivers to be in a direct line of sight (LOS) with the base station. This is usually called NLOS (Non Line Of Sight).
Except the small barriers (like houses, trees), the WiMAX is not capable to bypass hills or large buildings without a significant decrease in the speed.
WiMAX provides high-speed connections without the need for cables, so it is a good alternative to classical cable or DSL access. Also, WiMAX is suitable to for the so called "last mile" areas that are not covered by normal wired technologies. WiMAX allows the existence of Metro Zones having portable outdoor wireless access.
Another interesting possibility of using WiMAX is to connect two local wireless networks into a mesh, something very similar with the GSM roaming.
The QoS (Quality of Service) represents the network capability to guarantee that a service works when it is used. As is all other wireless (and even wired) networks, the bandwidth is divided among the users, so the WiMAX performance can drop significantly when the number of users is increasing.
To avoid such a situation, WiMAX reserves bandwidth for given purposes, like Voice over IP, where the communication delays can lead to useless connections.

## 3. WiMAX Security

In order to be able to win the competition with classical cable or DSL providers, the WiMAX network should be at least as secure.
The WiMAX security is based on two quality encryption standards, the DES3 and AES that allows a high support for confidentiality [3]. Also, the standard requires a dedicated security processor located at the base station level.
The entire WiMAX network traffic must be encrypted using CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) that uses AES to provide encryption for secure data transmission.
Each subscriber station must use X.509 certificate that is uniquely identifying the subscriber, so it is not possible for attackers to get another subscriber identity.
An X.509 certificate consists of the following fields:

- version

ISSN 2067 – 4074

- serial number
- signature algorithm ID
- issuer name
- validity period
- subject (user) name
- subject public key information
- issuer unique identifier
- subject unique identifier
- extensions
- signature algorithm
- signature value

There are specific encryption requirements for the end-to-end authentication that is provided for using PKM-EAP (Extensible Authentication Protocol) based on the TLS standard of public key encryption.

Because the WiMAX network is based on the Internet Protocol, it has the same vulnerabilities as any IP network, like DoS (Denial of Service), IP spoofing, session hijacking and so on.

Other types of potential attacks for a WiMAX network are Man-in-the-Middle and network manipulation with spoofed management frames (management frames are not encrypted).

WiMAX users should feel safe because only authorized users are able to access WiMAX services and the transmitted data is manipulation free.

The physical layer is unsecured, so the WiMAX is vulnerable to classical attacks at physical level such as:

- scrambling - affects the order of specific frames, an attacker can force the users to retransmit the data, so the channel becomes very busy, affecting the overall network performance; the impact can be considered as being low since it is enough to retransmit the data in order to recover the network status;
- jamming - presence of a source of noise, malicious or accidental, that drastically reduces the capacity of the communication channel; fortunately, the jamming can be easily detected and located by using radio scanning devices, but the risks can be considered as major.

A Denial of Service attack (DoS) is very likely to occur in a WiMAX network because the authentication operations (users or devices) need long procedures to be executed, so an attacker can easily flood an user by sending him numerous messages to authenticate. A potential scenario could be the flooding of a station in order to drain its battery.

## 4. Using WiMAX Technology for e-learning solutions

Usually, e-learning systems are developed as distributed applications, but this is not necessary so. The architecture of a distributed e-learning system includes software components, like the client application, an application server and a database server the necessary hardware components (client computer, communication infrastructure and servers).

E-learning clients have to be developed having in mind users' requirements, several studies in this area being made for mobile clients in [7], [9].

Figure 4 presents an architecture of an e-learning solutions based on WinMAX technology.

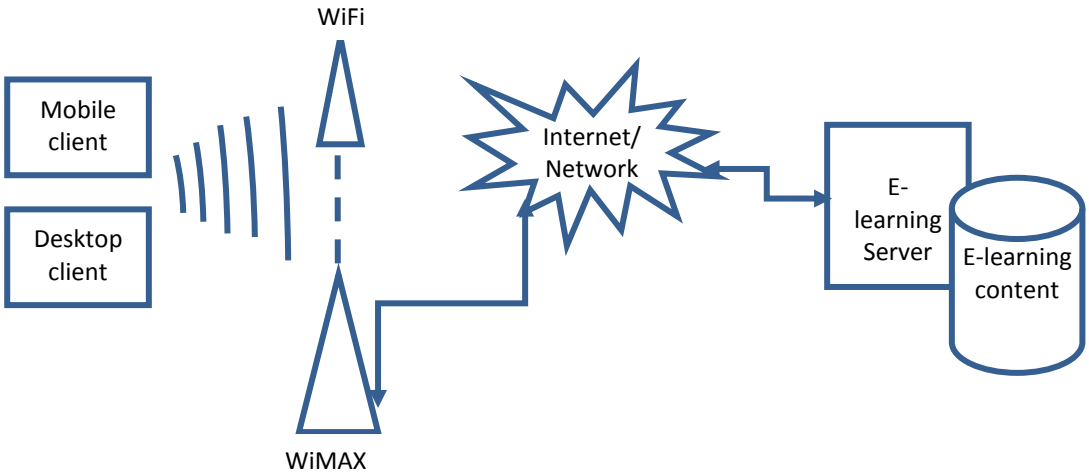


Fig. 4 An e-learning solution using WiMAX

The e-learning clients connect to the e-learning platform by using WiFi networks or connecting directly to the WiMAX network (if appropriate hardware is available).

The e-learning solution can be integrated into cloud architecture [4]. A very big concern is related to the data security because both the software and the data are located on remote servers that can crash or disappear without any additional warnings [8]. Even if it seems not very reasonable, the cloud computing provides some major security benefits for individuals and companies that are using/developing e-learning solutions, like the following:

- improved improbability – it is almost impossible for any interested person (thief) to determine where is located the machine that stores some wanted data (tests, exam questions, results) or to find out which is the physical component he needs to steal in order to get a digital asset;
- virtualization – makes possible the rapid replacement of a compromised cloud located server without major costs or damages. It is very easy to create a clone of a virtual machine so the cloud downtime is expected to be reduced substantially;
- centralized data storage – losing a cloud client is no longer a major incident while the main part of the applications and data is stored into the cloud so a new client can be connected very fast. Imagine what is happening today if a laptop that stores the examination questions is stolen;
- monitoring of data access becomes easier in view of the fact that only one place should be supervised, not thousands of computers belonging to a university, for example. Also, the security changes can be easily tested and implemented since the cloud represents a unique entry point for all the clients.

Table 1 – Security concerns of e-learning platforms

| **Action** | **Security requirements** |
|---|---|
| Online exam | High |
| Content management | High |
| Feedback management (forums) | Low-Medium |
| Homework/Projects Assesment | High |

Table 1 presents some security concerns regarding the e-learning solutions. These can be managed using several methods and techniques: different authentication

ISSN 2067 – 4074

levels, password management etc.
Wireless data communication can be easily monitored, so high security need to be assured by using specific standards. For example, if WiFi is used, it is recommended to use WPA2 standard combined with other WiFi security techniques.

## 5. Conclusions

WiMAX is an appropriate solution for e-learning platforms when the trainee location is isolated. One of the main concerns is related to security.
Currently there are no efficient solutions to prevent the attacks at the physical layer of a WiMAX network but, despite of all issues and threats, WiMAX is considered to be a secure network that provides:

- strong user authentication
- access control
- data privacy
- data integrity

using sophisticated authentication and encryption technology.
WiMAX technology will be used in Romania on a large scale in the near future. This will help the e-learning solutions and that will lead to a better education system in Romania.

## Acknowledgements

This paper presents some results of the research project IDEI 2673: Project management methodologies for the development of mobile applications in the educational system financed within the framework of IDEI research program.

## References

[1] Jeffrey G.Andrews, Arunabha Ghosh, Rias Muhamed, *Fundamentals of WiMAX*, Prentice Hall, 2007

[2] Deepak Pareek, *WiMAX – Taking Wireless to the MAX*, Auerbach Publications, New York, 2006

[3] Syed Ahson, Mohammad Ilyas, *WiMAX – Standards and Security*, CRC press, 2006

[4] DeCoufle B., The impact of cloud computing in schools, *The Datacenter Journal*, http://datacenterjournal.com/content/view/3032/40/, July 2009

[5] Creeger M., CTO Roundtable: Cloud Computing, *Communications of the ACM*, vol. 52, no. 8, august 2009, pp. 50-56

[6] Boja C., Bătăgan L., Software Characteristics of M-Learning Applications in *Proc. of. 10th WSEAS International Conference on Mathematics and Computers in Business and Economics (MCBE'09),* Prague, Czech Republic, March 23-25, 2009, ISSN: 1790-5109, ISBN: 978-960-474-063-5, pp. 88-93;

[7] Danail D., Ivo H., Mobile Learning Applications Ubiquitous Characteristics and Technological Solutions, *Cybernetics and Information Technologies*, Volume 6, No 3, Sofia, 2006, ISSN: 1311-9702;

[8] Brodkin J., Gartner: Seven cloud-computing security risks, *Infoworld*, July 2008, http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853, retrieved on August 2009

[9] Pocatilu P., Boja C., Quality Characteristics and Metrics related to M-Learning Process, *Amfiteatru Economic*, Year XI, June 2009, No. 26, pp. 346-354