Security Challenges in WiMAX Technologies

Daniel Simion, Mihai-Florentin Ursuleanu, Adrian Graur and Alin Dan Potorac
"Stefan cel Mare" University
str.Universitatii nr.13, RO-720229 Suceava
Suceava, Romania

***Abstract*—With the help of the Internet today we can communicate with anyone from anyplace to access all types of data with a high level of QoS. This mobility is available for legitimate users, as well as for illegitimate ones, for this reason we need extra data security. The wireless industry continues to change at very high speeds, tending to use the equipment more easily and safely and with a connection speed that tends to be higher and higher. This paper is an overview of most threats involved in infrastructure and WiMAX deployment.**

***Index Terms*— Limitations, Security, WiMAX, Wireless.**

I. Introduction

WIMAX is short for Worldwide Interoperability for Microwave Access. In essence WiMAX is Wi-Fi with a greater range on action and higher data transfer speed. But these two technologies are different.

It seems that all roads lead to WiMAX (Figure 1), the standard has known an impressive evolution over a short amount of time, being that is a software upgrade to the HSPA standard.

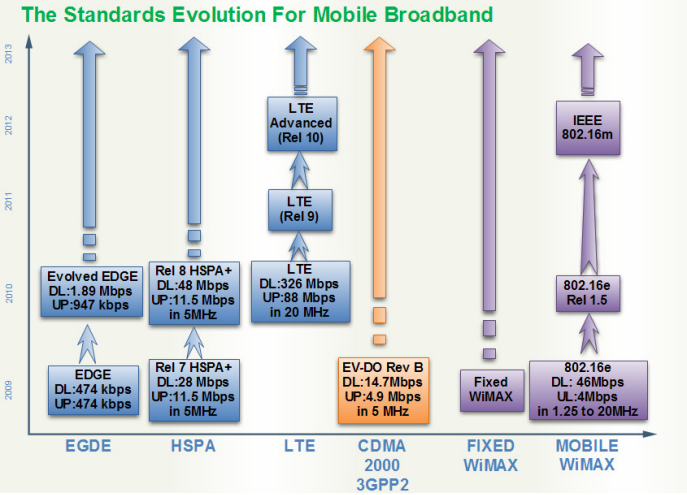

Fig. 1. The standards evolution for mobile broadband [1].

This paper was supported by the project "Knowledge provocation and development through doctoral research PRO-DOCT - Contract no. POSDRU/88/1.5/S/52946", project co-funded from European Social Fund through Sectoral Operational Program Human Resources 2007-2013.

Everyone has experienced the thrill of the high announced new standard WiMAX, supported by Intel, and the disappointed that turned out to be.

WiMAX is the abbreviation for Worldwide Interoperability for Microwave Access, and "Max" is used in order to express the very broad coverage provided by this standard. WiMAX is similar to Wi-Fi and different all together, but it offers higher speeds and greater area coverage. This technology was designed to offer the same broadband access to wireless networks as the traditional cable connection. There are many advantages of using the WiMAX standard: the ability for easy install on areas in which cable interfaces technology is hard to implement, low installation costs and the possibility to overcome the physical limitations traditional cable land line.

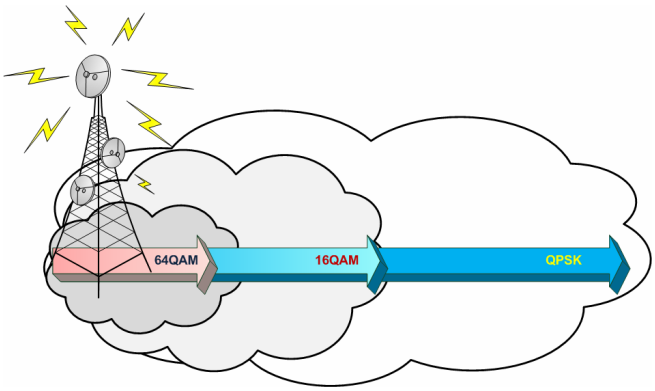

Fig. 2. Adaptive Modulations and Coding (AMC).

WiMAX offers a set of technological improvements to wireless performance (throughput, coverage, indoor penetration). These improvements are: AMC (adaptive modulation and coding) which offers the highest available data rate based on link quality, sub channel division using SOFDMA (Scalable Orthogonal Frequency Division Multiple Access) – support bandwidths between 1.25 – 20 MHz, H-ARQ (Hybrid Automatic repeat Request), FEC (Forward Error Correction) and smart antennas that use MIMO and AAS (Adaptive Antenna System) [2]. WiMAX has the advantage of using NLOS (Non-Line-of-Sight) technology, giving it grater coverage in rough terrain and indoors (supports high mobility up to 125 Km/h) [3].

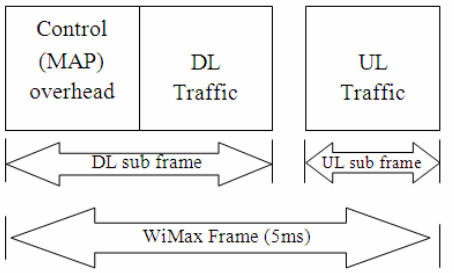

Fig. 3. Frame structure for WiMAX [4].

WiMAX supports five physical layer interfaces depending on the modulation technique:

WirelessHUMAN – TDD is used as a duplexing technique, it is used for the free frequency between 2-11GHz.

WirelessMAN-OFDM – provides NLOS transmission.

WirelessMAN-OFDMA – uses 2048 subcarriers for NLOS operation.

WirelessMAN-SC – uses single carrier modulation technique in 10-66 GHz frequency band for LOS transmission.

WirelessMAN-SCa – the same as WirelessMAN-SC with the difference that it operates in 2-11GHz.

The MAC layer is used as a transport layer between the physical layer and the upper layers. A key feature of the MAC layer is the support for transmission of variable length frames. There are three sub layers: SS (Security Sublayer), CPS (Common Part Sublayer), SSCS (Service Specific Convergence Sublayer).

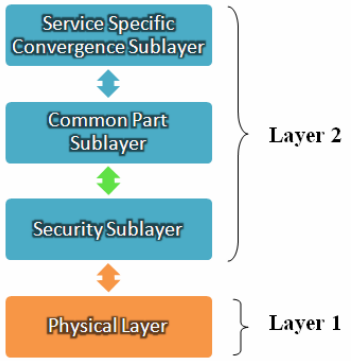

Fig. 4. Stack architecture of WiMAX [4].

WiMAX supports two forms of MIMO systems. Open loop MIMO is used in order to increase the capacity and the range of WiMAX. Closed loop MIMO contains information about the propagation channel and makes use of MRT (Maximum Ratio Transmission) to further enhance capacity and coverage area of WiMAX.

QoS functions allowing low latencies make Mobile WiMAX appropriate for VoIP streams, therefore a direct competitor to GSM solutions. WiMAX technology offers bit rates up to 75 Mbps over 20 MHz channels using 64 QAM and coverage areas up to 50 km.

The data rate decrease with distance but typically 10 Mbps are possible over 10 km. WiMAX is used for "last mile" backhaul data services distribution over residential areas.

High speed mobile wireless networks tend to rich a speed of 1 Gb/s, as shown in Figure 5 [6].

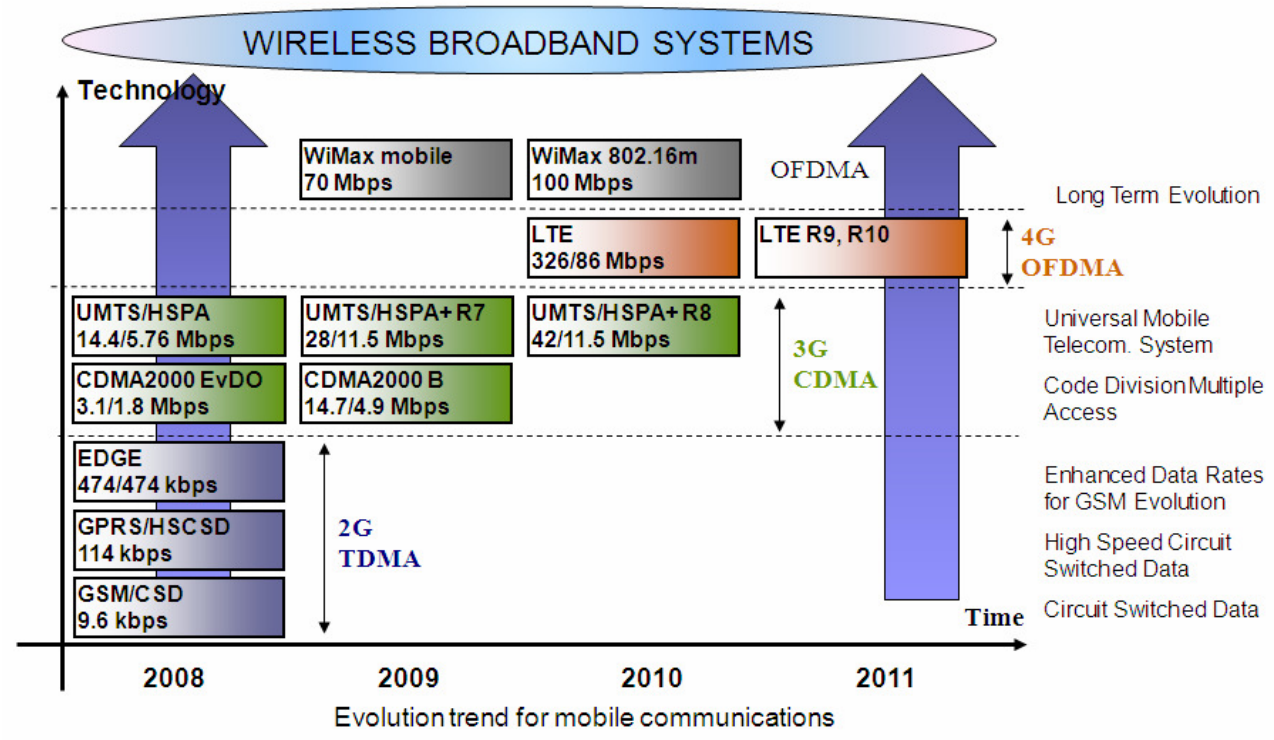

Fig.5 Evolution trend for mobile communication.

II. WiMAX ACCESS NETWORK

In order to have a WiMAX wireless network we need a base station which provides network add-on to the WiMAX CPEs and WiMAX Customer Premise Equipments.

WiMAX Customer Premise Equipment (WiMAX CPE) selects the bases station with the strongest signal. All the system can be viewed like a computer system with the subscriber being a user and WiMAX Customer Premise Equipments (WiMAX CPE's) being the system.

In CPS (Common Part Sub layer) bandwidth is managed, connections are established and PDUs (MAC Protocol Data Units) are developed. The Convergence layer exchanges SDUs (MAC Service Data Units) with CP (Common Part).

CP has as an integrated part the privacy sub layer, which establishes encryption, authentication and keys.

MAC PDUs are exchanged between Security sub layer and the Physical layer.

MAC SDU format are adapted to a lower level of data units by the Convergence layer which sorts by connection the incoming MAC SDUs. "Physical layer is a two-way mapping between MAC PDUs and Physical layer frames received and transmitted through coding and modulation of radio frequency signals" [7].

Security challenges and threats in WiMAX

Being a new technology WiMAX networks have a high operational and installation costs.

WiMAX technology offers bit rates up to 70 Mbps over 20 MHz channels using 64 QAM and coverage areas up to 50 km. The bit rate is affected if we increase the distance range further than 50 Km, in order to obtain a higher bit rate we must shorten the distance range. For example if a user is close to the base station he can have a data transfer speed up to 30Mbit/s and another user in the same network that is at the edge of the covering area by the broadcasting tower, may get a data transfer speed up to 14Mbit/s (see Figure 6).

Like Wi-Fi, WiMAX suffers from lack of quality when is dealing with massive requests from many users trying to access the same base station in a communication cell.

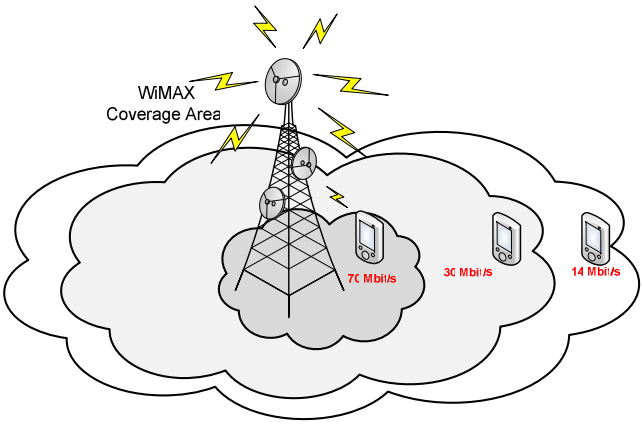

Fig 6. WiMAX Bandwidth Range.

Being a wireless technology WiMAX, data transfer speed is affected by wireless radio interference from other wireless sources and by the weather.

WiMAX is a big power consumer because of its equipments and in compartment to other communication mediums (satellite or fiber optics) it has a lower data rate.

Denial of Service (DoS) Attacks is one of the most powerful on a wireless communication network. Using a two phased model service flow can be established. First is admitted a service flow with provisioned resources after which the service flow is activated on an on-demand basis. To conserve network resources the service flow can be activated or turned off after a certain time limit.

When a WiMAX network is either in Idle/Sleep Mode, with no uplink or downlink, the power consumption of the mobile station is lowered.

Once the data is available, the base station establishes a connection with the mobile station using ranging parameters; ranging parameters that will be adjusted for the connection. In the end the mobile station returns to normal state with the activation of the service flow that permits data transfer.

In some cases the mobile station will perform a series of operations to authenticate, to manage keys, to negotiate, to register and to reestablish IP connectivity.

So, attackers may lunch different signaling attacks to the WiMAX base station to overload it with state transitions operations resulting in a denial of service attack [8].

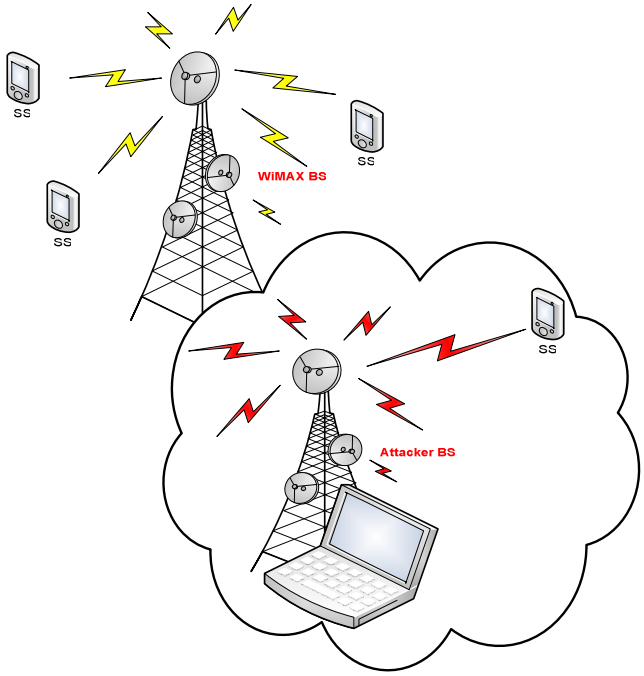

Fig. 7. Attacker BS uses Water Torture to create DoS attack.

Another threat in WiMAX wireless networks is when the attacker sends a series of frames to consume the receiver's battery; this kind of attack is called **Water Torture** (see figure 7).

Like most wireless networks, the signal may be highjacked using a RF receiver so a measure to prevent this type of behavior is required (maybe a cryptographic security

mechanism which can be maintained while a mobile Subscribed Station (SS) changes between WiMAX BS).

Data authenticity technology is required in order to prevent an attacker with a RF Sniffer to capture, change and retransmit data frames to the WiMAX BS.

When the transmission range is longer, a detection mechanism for relayed frames is needed to prevent attackers to forward data frames, from authorized stations that can't communicate directly.

WiMAX standard has two types of certificates, one for SS and one for the manufacturer, and not for BS. This becomes a problem. Subscriber certificate identifies a subscriber by its MAC address. SS certificates are normally created and signed by the manufacturer using public key, this enables the BS to validate a SS certificate and so identify a certain device as genuine. This type of drawback is called **mutual authentication problem**.

The major disadvantage for WiMAX is the lack of a BS certificate. Creating a scheme for mutual authentication is the only way that attackers can't forger or replay attack on a BS for example with X.509 certificate you can verify EAP encryption.

I. Conclusion

In conclusion we can say that permanent evolution of wireless networks determines that WiMAX technology will be available on different platforms (PDA, Smartphone, Desktop PC, Laptops, Tablet PC, etc.)

In our opinion an architectural solution which can cover different technologies and geographical areas without any bandwidth problems and high costs is a combination of WiMax, Bluetooth and Wi-Fi.

WiMAX include "best-effort" and priority based QoS scalable solutions [6].

A minus for WiMAX is the fact that we must choose between long range and high bit rate.

There are and there will be ways to study security challenges for new wireless technologies until this communications will be 100% safe.

In this paper we have presented a few of many security floss found in new wireless technologies. We hope that in the future they will become fewer and resolvable.

References

[1] Rysavy Research and 3G Americas, "EDGE, HSPA & LTE. The Mobile Broadband Advantage", September 2008 (whitepaper).

[2] WiMAX Forum, "Mobile WiMAX – A Technical Overview and Performance Evaluation", whitepaper February 2006.

[3] Alim O. A., Elboghdadly N., Ashour M.M., Elaskary A.M., "Simulation of channel simulation and equalization for WiMAX PHY Layer in Simulink ", Computer Engineering & Systems, ICCES, 07.International Conference on Volume, Issue, 27-29 Nov. 2007, Pages 274-279.

[4] Mihai-Florentin URSULEANU, Daniel SIMION, Adrian GRAUR, Alin Dan POTORAC, "A Comparative Approach on WiMAX and LTE Technologies", International Conference on Development And Application Systems, 10th Edition May 27-29, 2010 - Suceava, ROMANIA, ISSN 1844-5039,pages 170-174.

[5] Derrick Boom, 10th May 2004, "Denial of Service Vulnerabilities in IEEE 802.16 wireless networks", Naval Postgraduate School Monterey, Ca 93943

[6] Potorac A.D., Graur A., Popa V., „QoS Challenges in Modern Communications Networks", ECUMICT 2010, 4th Edition, March 25th -26th 2010, Gent

[7] Michel Barbeau, "WiMAX/802.16 Threat Analysis", School of Computer Science, Carleton University, Ottawa, Ontario, Canada.

[8] Ramana Mylavarapu, August 2005, *Security Considerations for WiMAX-based converged network*, Cardiff Publishing Company, USA