

СИГУРНОСТ В WIMAX МРЕЖИ, ИЗПОЛЗВАНИ В СИСТЕМИ ЗА ЕЛЕКТРОННО ОБУЧЕНИЕ

ABOUT SECURITY OF WIMAX USED FOR E-LEARNING SYSTEMS

Александър Милев

Шуменски университет „Епископ Константин Преславски“

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 elearning solutions, especially when WiMAX technology is used.

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

ВЪВЕДЕНИЕ

Електронното обучение е изключително разпространено в наши дни на различни нива в образованието: редовно обучение, обучение в компании, академични курсове и др. Процесът на обучението е комплексна услуга, която включва производител (обучаващ) и потребител (обучаван). Съществуват разнообразни решения за електронно обучение (e-learning), които могат да бъдат както комерсиални така и с отворен код. В повечето случаи са необходимо поне две общности, включени в системата за електронно обучение: студентите и преподавателите.

Действията, които студентите предприемат в платформите за електронно обучение са следните:

- Участие в online курс;
- Полагане на online изпити;
- Попълване на форма за обратна връзка (feedback) и нейното изпращане;
- Разработка на курсови проекти и домашни задания и тяхното изпращане за проверка;

Дейностите на преподавателите, включени в процеса на електронното обучение са следните:

- Обработка и управление на материалите за обучение;
- Подготовка на тестове;
- Оценяване на тестове, домашни задания и курсови работи, разработени от студентите;
- Изпращане на данни и обратна връзка със студентите (feedback)
- Своевременна връзка и комуникация със студентите (forums)

Очевидно е, че всяко една от тези дейности изисква определено ниво на сигурност, която зависи от степента на важност на данните и тяхната сигурност.

За реализация на изискваната сигурност на отдалечена и мобилна комуникация са възможни множество мобилни технологии. Те осигуряват свързаност на изолирани области и общности, както в локален така и в глобален план. Такива мобилни технологии се явяват GSM/UMTS, WiMAX и др.

Една многообещаваща технология се явява технологията WiMAX. Тя осигурява висока скорост на прехвърляне на данни и може да се използва на такива места, където други технологии не могат да се използват. Типичните приложения, които използват WIMAX технологията, са свързани с т.

нар. широколентови канали за трансфер на данни, както в градски райони така и е географски отдалечени области. Възможно е също да се реализира дори предаване на глас по IP мрежа (VoIP), а дори и цифрова телевизия.

ИЗЛОЖЕНИЕ

Технологията WiMAX е базирана на стандарта за градска безжична мрежа WirelessMAN (802.16) [1]. WiMAX използва предаване на данни по безжична среда чрез различни режими на трансфер, като точка – точка, точка – много точки или пълно-клетъчен достъп. Стандартът е създаден през 2001 вследствие на съвместната работа на компаниите Intel и Alvarion и е ратифициран официално от IEEE под името IEEE-802.16.

Името и логото на WiMAX (фиг. 1) са създадени от WiMAX форум. От друга страна е създадена организация за приемане на продукти и услуги WiMAX с цел да се осигури висока степен на сигурност и взаимна оперативност между тях.



Фиг. 1. Лого за мрежа WiMAX

При фиксираната мрежа WiMAX “fixed WiMAX” (802.16-2004 и 802.16d) се реализира фиксирана връзка с монтираната на покрива антена. При този вид конекция липсва поддръжка на мобилност и това е използвано за развитие на стандарта за „мобилния WiMAX”, известен като 802.16-2005 или 802.16e.

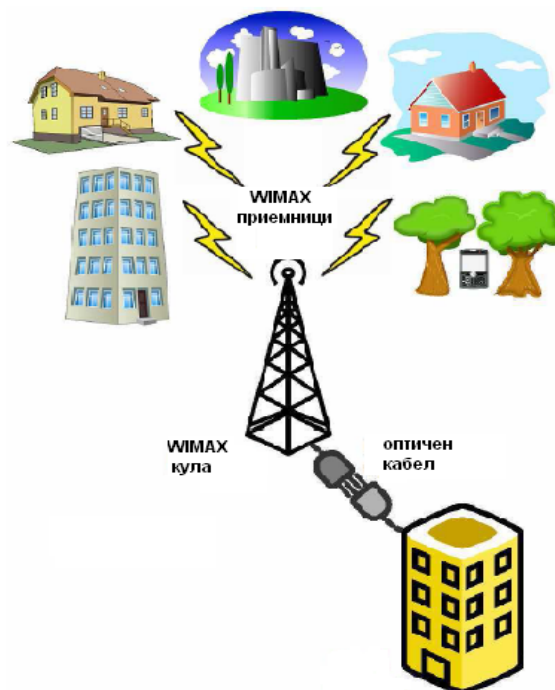
На фиг. 2 са показани компонентите на мрежа от тип WiMAX.

Мрежата WiMAX са състои от следните два компонента [2],[3]:

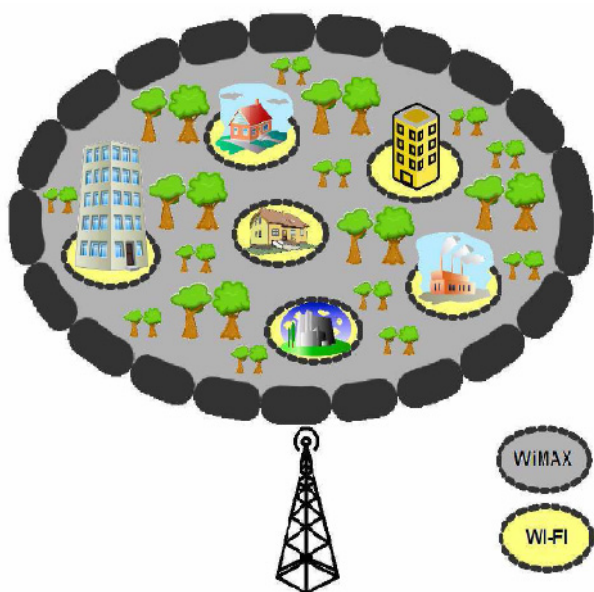
- WiMAX базова станция – място, от където WiMAX сигнала се излъчва като бродкаст (broadcast). В повечето случаи тази станция се свързва към обществената мрежа чрез оптични кабели, радио-линии или други високоскоростни технологии от

тип точка – точка. Обикновено кулата на WiMAX заедно с някакво електронно устройство играе роля на базова станция (точно както функционира кулата и на телефонната мрежа GSM). Тези кули могат да покрият разстояние в радиус до 50 км., но поради географски ограничения, разстоянията на които те се изграждат са от порядъка на 20 км. При попадане на някакво безжично устройство, съвместимо с WiMAX, в обсега на покритие на базовата станция, то ще реализира свързаност към мрежата.

- Приемници (receivers) – устройства, които се използват за приемане на сигналите от WiMAX базовата станция. Приемниците позволяват на мобилни устройства да се свържат към WiMAX мрежата. Механизмът на свързване е много подобен на този, използван в Wi-Fi мрежите. Единствената разлика е по-голямото разстояние, покривано от WiMAX (фиг.3). По принцип една базова станция може да се свърже с няколко други базови станции на висока скорост и по този начин да се увеличи разстоянието между двете крайни точки, изискващи двустранна комуникация. Тази конекция се нарича обратна доставка/превоз (backhaul) и тя позволява съществуването на роуминг чрез поддържането на конекциите при движение на свързалите се абонати.



Фиг. 2. Мрежа WiMAX



Фиг. 3. Мрежи от тип WiMAX и Wi-Fi

Мрежа WiMAX осигурява високоскоростен Интернет достъп в радиус до 50 км. Характерна особеност на тази технология е, че не се изисква приемниците да бъдат в директна видимост с базовата станция (line of sight (LOS)). Това обикновено се нарича NLOS (Non Line Of Sight). Технология WiMAX осигурява високоскоростни връзки без кабел, което прави този тип мрежа добра алтернатива вместо класическия кабел или DSL модемен достъп. WiMAX честотния диапазон дава възможност за преодоляване на малки бариери (къщи и дървета), но при наличие на хълмове и големи сгради се наблюдава голямо намаление на скоростта. Също така WiMAX е подходяща за т.нар. област на „последна миля“, която не се покрива от обичайните технологии с окабеляване. WiMAX позволява съществуването на Metro зони, притежаващи малки области за безжичен достъп. Друга интересна възможност при използването на WiMAX е, че се подсигурава свързването на две локални безжични мрежи в смесена топология, което е много близко като идея на GSM роуминг. Качеството на услугите (Quality of Service, QoS) на тази мрежа е такова, че се гарантира способността на мрежата да обслужва дадена услуга, като се поддържа нейната функционалност, когато тя се използва. Както и при всяка друга мрежа, било то жична или безжична, честотната

лента се разпределя между потребителите, което означава, че производителността на WiMAX значително ще спадне при нарастване броя на потребителите. За да се избегне такава ситуация WiMAX резервира честотна лента за дадени цели като VoIP, където закъснението в предаването на глас може да доведе безсмислени конекции.

WiMAX СИГУРНОСТ

Сигурността на WiMAX е базирана на два криптиращи стандарта DES3 и AES, което подсигурава висококачествена поддръжка и конфиденциалност [3]. Освен това стандарта изисква специализиран посветен процесор за сигурност, разположен в базовата станция. Целият трафик в WiMAX мрежата трябва да бъде криптиран чрез CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), който използва AES за да осигури криптиране с цел сигурно предаване на данните. Всяка абонатна станция трябва да използва X.509 сертификат, който е уникален и идентифицира точно абоната. По такъв начин не е възможно за атакуващи да придобият идентичност на друга абонатна станция.

Сертификатът X.509 се състои от следните полета:

- Версия;
- сериен номер;
- идентификатор на алгоритъма за подпис ID;
- име на издател;
- срок на валидност;
- име на тема (потребител);
- информация за темата на публичния ключ;
- уникален идентификатор на издателя;
- тема на уникалния идентификатор;
- разширения;
- алгоритъм за подпис;
- стойност на подписа.

Съществуват специфични изисквания на криптиране на автентикацията от край до край, която се осигурява чрез използването на протокола PKM-EAP (Extensible Authentication Protocol), базиран на стандарта TLS за криптиране на публичния ключ. Тъй като WiMAX мрежите са базира-

ни на протокола IP при тях са налични същите уязвимост, присъщи на тях, а именно атаки с отказ на услуги (Denial of Service, DoS), подправяне на адреси (IP spoofing), открадване на сесия (session hijacking) и т.н. Други типове потенциални атаки за WIMAX мрежи се явяват атаките човек в средата (Man-in-the-Middle) и мрежовото манипулиране с подмяна съдържанието на кадрите (в случай, че кадрите не са криптирани). При работа с мрежата WiMAX потребителите трябва да се чувстват сигурни, защото само оторизираните потребители би следвало да имат достъп до предлаганите услуги и предаваните данни не би следвало да се манипулират от който и да е.

На практика физическото ниво на WIMAX е несигурно. По този начин мрежата се явява уязвима на класическите атаки на физическо ниво, а именно:

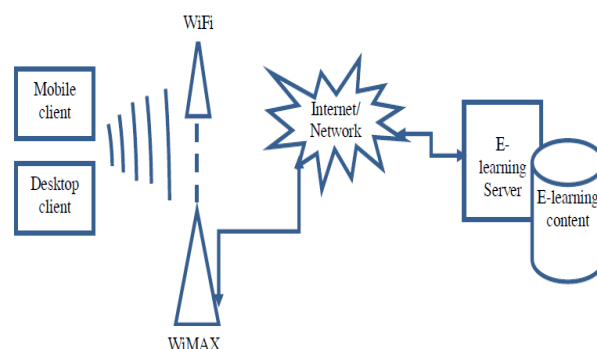
- scrambling – влияе на реда на специфични кадри. Атакующият може да принуди потребителите да препредат данните и по този начин канала да стане прекалено зает, което ще се отрази на мрежовата производителност. Крайният ефект от атаката би могъл да доведе до временна неработоспособност на мрежата, ако атаката е с по-голяма продължителност;
- jamming – наличие на източник на шум, зловреден и/или инцидентен, който намалява драстично капацитета на комуникационния канал. Такъв ефект може да се детектира и локализиран чрез използването на радио-сканиращи устройства, но като цяло трябва да бъдат отчетени и рисковете в този случай.

Атаките с отказ на услуги (Denial of Service, DoS) са твърде вероятни в WiMAX мрежата поради действията за автентикация на потребители и устройства. Процесът на тази автентикация трае дълго време, поради което атакующия може лесно да наводни потребителя чрез изпращане към него на многобройни съобщения със задача за автентикация. Потенциален сценарий може да бъде наводняване на станция с цел подмяна на акумулатор.

ИЗПОЛЗВАНЕ НА WIMAX ЗА ЕЛЕКТРОННО ОБУЧЕНИЕ

В повечето случаи системите за електронно обучение са разработвани като разпределени приложения, но това не е задължително да бъде така. Архитектурата на разпределените системи за електронно обучение включва софтуерни компоненти, като клиентско приложение, сървър за дадено приложение и сървър за база данни, както и съответните хардуерни компоненти (компютри, комуникационна структура и сървъри). Софтуерните приложения за електронно обучение трябва да бъдат разработени като се вземат предвид изискванията на потребителите. Множество автори са представили значими резултати в тази насока с цел постигане на мобилност на клиентите [6],[8].

Фигура 4 показва архитектура на система за електронно обучение, базирана на WIMAX технология.



Фиг. 4. Електронно обучение с използване на WiMAX

Клиентите от електронното обучение се свързват към платформата за електронно обучение чрез WiFi мрежи или директно към WIMAX мрежата, ако притежават съответния хардуер. Това решение за електронно обучение може да бъде вградено в архитектура тип облак (cloud) [4],[5]. В този случай съществува голям проблем за сигурността на данните, тъй като софтуера и данните са разположени на отдалечени сървъри, които могат да се окажат недостъпни без предупреждение поради срив или атаки [6],[7].

С цел подобряване на основните мерки за сигурност за отделните потребители, компютри и тази на компанията е препоръчително да бъдат използвани и доразвивани

решения за електронно обучение, които могат да бъдат следните:

- подобрена невъзможност – почти невъзможно е за всяко заинтересовано лице (крадец) да определи къде е разположена машината, която съхранява желаните данни (тестове, въпроси за изпити, резултати) или да разбере кой е физическият компонент, който може да бъде открадне за да придобие достъп до цифровите данни;
- виртуализация – дава възможност за бърза подмяна на компрометиран сървър без големи инвестиции. Много лесно е да бъде създаден клонинг на виртуална машина, така че времето за временна неработоспособност да бъде сведено до минимум;
- централизирано съхранение на данни – загубата на клиент не представлява голям проблем, докато главната част на приложенията и данните, съхранявани в облака (cloud) оборудване трябва да бъде подсикурена с резервираност и засилена физическа защитеност. Очевидно е че всеки нов клиент бързо би получил оторизиран достъп до съответните изисквани данни, докато ако се наложи подмяна на устройствата, съхраняващи голям обем информация и данни, ще коства както време, така и ресурс. Логичен е извода, че данните не трябва да се съхраняват на един лаптоп, който може лесно да бъде откраднат;
- наблюдението на достъпа до данни става все по лесно от гледна точка на факта, че се наблюдава и администрира само едно място, съхраняващо данните, а не множество компютри принадлежащи на даден университет. При промяна степента на сигурност може лесно да бъде тествано поведението на мрежата при различно поведение на потребителите, било то оторизирани или не за конкретен вид дейност. Всичко това в WIMAX мрежите е предимство, тъй като съществува само една единствена дочка за вход за всеки един клиент.

Таблица 1 представя някои ключови елементи за сигурността по отношение на електронното обучение.

Табл. 1. Изисквания за сигурността в системите за електронно обучение

Действие	Изисквания за сигурността
On-line изпити	Висока
Управление на съдържанието	Висока
Обратна връзка (Feedback) и управление Форуми	Ниска/Средна
Оценка на проекти/ домашна работа	Висока

Представените изисквания за сигурността могат да бъдат управлявани чрез използванети на редица методи и техники като: различни нива за автентикация, управления на паролите, контролиране на привилегии и др.

Безжичните комуникации и прехвърляните по тях данни могат лесно да бъдат наблюдавани, като по този начин може да се подсикури необходимото високо ниво на сигурност според стандарта. Например, ако се използва WiFi се препоръчва прилагането на алгоритъм за криптиране по стандарт WPA2 комбиниран с други WiFi техники за сигурност.

ЗАКЛЮЧЕНИЕ

WiMAX е подходящо решение за платформи за електронно обучение в случай, че местоположението на обучаваните е в отдалечени райони и на изолирани географски области.

Един от основните проблеми при мобилното обучение е сигурността, както на данните така и на участващите в него.

По настоящем липсват ефективни решения за предотвратяване на атаките на физическо ниво в WIMAX мрежа.

Въпреки това WIMAX се счита за сигурна мрежа, която осигурява:

- силна потребителска автентикация;
- контрол на достъпа;
- конфиденциалност на данните;
- цялостност на данните чрез използване на усъвършенствани технологии на автентикация и криптиране.

С използването на технологията WiMAX ще се предостави възможност за електронно обучение и мобилност. Това би довело до развитие и подобряване на отделни компоненти в образователната система в България.

ЛИТЕРАТУРА

- [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] Brodtkin J., Gartner: Seven cloud-computing security risks, Infoworld, July 2008, <http://www.infoworld.com/d/securitycentral/gartner-seven-cloud-computingsecurity-risks-853>, retrieved on August 2009
- [8] Pocatilu P., Boja C., Quality Characteristics and Metrics related to MLearning Process, Amfiteatru Economic, Year XI, June 2009, No. 26, pp. 346-354