Josef Hrubý

Obsah

1. Úvod do technologie

WiMAX (*Worldwide Interoperability for Microwave Access*) podle normy IEEE 802.16 (2004) pracuje v licenčním, tak v bezlicenčním spektru v pásmu 2-11 GHz, v režimu bez požadované přímé viditelnosti (NLOS) a má maximální dosah ve venkovských oblastech do 50 km a v husté zástavbě do 3-5 kilometrů. Značný dosah signálu umožňuje jednak vyšší vysílací výkon a také použití směrových antén (nejčastěji tři sektorové antény na základnové stanici). WiMAX nabízí kapacitu do 75 Mbit/s, kterou ovšem sdílejí všichni uživatelé připojení k téže základnové stanici.

Technologie WiMAX je velmi často srovnávána s technologií Wi-Fi. Toto srovnání je plně na místě, pokud jde o aspekt "otevřenosti, "vyzrálosti", dostatečné standardizace, či třeba certifikace interoperability, při které se ověřuje že si produkty různých výrobců vzájemně rozumí. Technologie Wi- Fi již do tohoto stádia dospěla a stala se běžnou komoditou (alespoň pokud jde o její "základní" verze", na bázi standardů 802.11b a g). Tomu pak odpovídá i její nasazení, které roste opravdu velmi rychle.

Přirovnávání WiMAXu k Wi-Fi už ale nebude na místě, jakmile se začneme zabývat tím, k čemu jsou tyto technologie určeny. Wi-Fi vzniklo jako technologie pro použití "na krátkou vzdálenost". Typicky pro bezdrátové propojení či rozvedení konektivity mezi koncová zařízení, rozmístěná například v rámci bytu či kanceláře, nějaké haly, konferenční místnosti atd. Tomu pak odpovídá i dosah této technologie - příslušné přístupové body, resp. tzv. hotspoty, většinou "dosáhnou" jen na několik málo desítek metrů uvnitř objektů, či několik málo stovek metrů v otevřeném prostoru. Navíc pracují v tzv. bezlicenčním pásmu, kde sice není potřeba žádná individuální licence, ale také zde může probíhat více přenosů na stejných frekvencích, které se mohou vzájemně rušit. Navíc Wi-Fi funguje stylem "best effort" (na principu maximální snahy), a nemá žádné mechanismy pro poskytování garantovaných služeb (resp. pro podporu tzv. kvality služeb, QoS). Takže jako technologie pro poskytovatele (operátory, providery), kteří chtějí poskytovat garantované služby a na větší vzdálenost (nikoli jen v rámci objektů), se moc nehodí. I když se i v této roli používá - ale spíše z nouzových důvodů, kvůli tomu že nic lepšího a vhodnějšího není k dispozici. Technologii Wi-Fi je tedy vhodné řadit spíše mezi technologie, určené pro realizaci bezdrátových lokálních sítí (sítí WLAN, resp. Wireless LAN). S dovětkem, že je určena jak poskytovatelům, tak i samotným koncovým uživatelům. Ti si ji mohou nasadit sami, například v rámci svého bytu. Naproti tomu technologie WiMAX je určena pro oblast bezdrátových metropolitních sítí (sítí WMAN, Wireless MAN), a tedy na větší vzdálenosti. Navíc patří již pouze do rukou poskytovatelů (operátorů, providerů). Ti ji mohou využít k přímému připojování svých zákazníků, ať již firemních či rezidenčních (domácností). Nebo pro napojení svých hotspotů, které pak šíří jejich konektivitu dále, prostřednictvím Wi-Fi. Případně k dalším účelům, včetně poskytování klasických hlasových služeb.

2. Normalizace

2.1 802.16

První norma pro bezdrátovou metropolitní síť (WMAN) byla schválena už v roce 2001 jako IEEE 802.16. Vloni schválená norma pro WiMAX původní specifikaci nahradila. Je zajímavé podívat se na důvody neúspěchu původního záměru řešení WMAN.

Původní norma 802.16 „*Standard Air Interface for Fixed Broadband Wireless Access Systems*“ schválená v roce 2001 nabídla řadu rádiových rozhraní (*air interface*) se stejným protokolem MAC**,** ale s různým řešením fyzické vrstvy **(**TDM/TDMA**).**

Norma definovala použitelné kmitočty od 10 do 66 GHz, z čehož vyplýval požadavek přímé viditelnosti mezi rádiovým vysílačem a přijímačem. Na fyzické vrstvě nabídla norma díky vyšším kmitočtům kapacitu až 268 Mbit/s. 802.16 používala samoopravný protokol pro přístup k rádiovému kanálu. Topologie WMAN je *point-to-multipoint* (PMP), kdy základnová stanice v centru komunikuje s mnoha připojenými uživateli současně.

Největším problémem první otevřené specifikace pro bezdrátové přístupové sítě byla volba kmitočtů, která vyžadovala přímou viditelnost. Ani antény přijímače na střechách domů totiž nemusí přímo „vidět“ na anténu základnové stanice, např. kvůli stromům, proto dochází k odrazům a cestě signálu mnoha směry, s časově rozptýleným příjmem původního signálu. Navíc jsou vnější antény pro domácího uživatele zbytečně nákladné kvůli ceně hardwaru i instalace.

Přímá viditelnost a použité kmitočty tedy neudělaly z první verze 802.16 ideálního kandidáta pro širokopásmový bezdrátový přístup. Pro něj se hodí až nová specifikace 802.16a, schválena v roce 2003 pod základním označením 802.16**,** která původní normu zcela nahradila a ve světě se ujala pod označením WiMAX (*Worldwide Interoperability for Microwave Access*.

2.2 802.16a

V lednu roku 2003 byla schválená norma IEEE 802.16a, která rozšiřuje původní normu o nižší kmitočty v intervalu 2-11 GHz (zahrnující kmitočty jak bez licence, tak s licencí). Tyto kmitočty ve srovnání s vyššími umožňují levnější pokrytí pro více uživatelů, i když s nižšími přenosovými rychlostmi. Toto řešení bude více vyhovovat jednotlivým koncovým uživatelům, domácím kancelářím nebo malým podnikům pro připojení k Internetu.

Kromě využití 802.16a jako řešení první míle, tedy přístupu k Internetu pro koncové uživatele a sítě (domácnosti i podniky), bude specifikace pravděpodobně zajímavým řešením pro propojení veřejných WLAN (tzv. hot spots) podle IEEE 802.11, protože dovoluje vytvořit bezdrátovou páteřní síť těchto přípojných míst poskytovatelů bezdrátového přístupu k Internetu (WISP, Wireless Internet Service Provider). Tak by přestaly být veřejné WLAN pouze osamocenými ostrůvky pro uživatele, ale dosáhly by lepšího pokrytí (v souvislosti s řešením otázek roamingu). Pro mobilní profesionály je stále důležitější rychlý přístup k Internetu a podnikovým sítím a využívání širokopásmových služeb i mimo kancelář.

2.3 802.16e

Další schválenou normou v rámci WiMAX je 802.16e, která do WiMAX doplní podporu pro mobilní uživatele, takže umožní rychlé předání uživatelů mezi základnovými stanice při pohybu až rychlostí rychle jedoucího auta. Právě tato specifikace je často diskutovaná, protože se očekává značný konkurenční boj mezi ní a připravovanou normou IEEE802.20, která je specificky určena na podporu širokopásmové komunikace mobilních uživatelů. Ta má podporovat IP komunikaci různorodých přenosných a mobilních zařízení, nejen laptopů ale i mobilních telefonů a PDA, a to až pro rychlosti kolem 250 km/h (odpovídá rychle jedoucím vlakům). 802.20 bude používat spektrum mezi 500 MHz a 3,5 GHz, takže kapacitně bude o něco slabší než 802.16. Na druhé straně bude plně konkurenční mobilním sítím třetí generace.

2.4 Další normy standardu WiMAX

V rámci 802.16 se pracuje ještě na dalších specifikacích. Schvaluje se norma 802.16f pro bázi informací pro management (MIB). Začalo se pracovat na dvou nových doplňcích: 802.16g pro záležitosti týkající se úrovně managementu (*management plane*) a 802.16h pro koexistenci systémů pracujících v bezlicenčním pásmu.

3. Vrstvy standardů 802.16

Skupina standardů 802.16 obsahuje definici dvou vrstev – fyzické vrstvy (PHY) a vrstvy přístupu k rádiovému kanálu (MAC). Složení těchto vrstev je uvedeno v tabulce č.1

Tabulka č.1 Vrstvová architektura standardů 802.16

Vyšší vrstvy	IP, přenos řeči, videa atd.		
Linková vrstva	ATM, Frame Relay		
	LLC		
	Subvrstva koordinace s protokoly služeb		
	Všeobecná subvrstva MAC protokolu 802.16		
	Subvrstva bezpečnosti MAC protokolu		
Fyzická vrstva	802.16 10.. 66 GHz	802.16a 2…11 GHz	WiMAX 802.16e 2,4… 2,483 GHz 3,4… 3,6 GHz 5,7… 5,8 GHz

3.1 Fyzická vrstva

Fyzická vrstva definuje využití kmitočtů z intervalu 2-11 GHz (zahrnující kmitočty jak bez licence, tak s licencí). WiMAX nepotřebuje přímou viditelnost (pracuje v režimu *NLOS, Non-Line-Of-Sight*), protože využívá OFDM (*Orthogonal Frequency Division Multiplexing*) Na rozdíl od jiných specifikací pro bezdrátové systémy realizuje WiMAX datový přenos po několika kmitočtových pásmech, čímž se minimalizuje nebezpečí rušení s jinými rádiovými aplikacemi. V závislosti na volbě spektra se také mění dosah i vysílací rychlost. To na druhou stranu umožňuje provozovatelům používat různé kmitočty právě v závislosti na konkrétní vzdálenosti uživatele od základnové stanice a na požadované kapacitě připojení.

OFDM se používá v bezdrátových systémech již delší dobu (např. ve WLAN typu 802.11a/g) všude, kde je potřeba docílit vysoké propustnosti a přitom podmínky na kanálu mohou být ztíženy. OFDM rozděluje širokopásmový signál do více úzkopásmových kanálů, z nichž každý přenáší kolem 280 kbit/s. Kanály jsou velmi blízko u sebe, ale nepřekrývají se, takže nehrozí jejich vzájemné rušení. Přenos pomocí OFDM také nepodléhá rušení způsobenému různými cestami signálu (*multipath distortion*), a vůbec útlumu signálu právě ve venkovním prostředí.

802.16 specifikuje tři varianty fyzické vrstvy: OFDM (*Orthogonal Frequency Division Multiplexing*) s 256 kanály pro nejběžnější použití (na rozdíl od 64-OFDM u WLAN) – vybraný profil pro první vlnu testování, pro speciální sítě modulaci s jednou nosnou a speciální OFDMa (*OFDMA advanced*) s 2.048 kanály pro aplikace skupinového vysílání. Nabízí časový duplex TDD (*Time-Division Duplexing*) a kmitočtový duplex FDD (*Frequency-Division Duplex*), kde FDD podporuje režim vysílání v plném nebo poloviční duplexu.

Rádiové kanály mají šířku pásma od 1,5 do 20 MHz. Použité kmitočty ve srovnání s vyššími umožňují levnější pokrytí pro více uživatelů s přenosovými rychlostmi až 75 Mbit/s, ale tuto kapacitu sdílejí všichni uživatelé připojení k téže základnové stanici.

Kapacita 75 Mbit/s znamená v 2,5 GHz pět kanálů po 20 MHz, kanály lze ovšem rozdělit až na 1,5 MHz, nebo naopak sdružit. Takže ve výsledku lze podporovat např. 375 uživatelů po 1 Mbit/s, nebo 750 uživatelů s kapacitou 500 kbit/s (konkurence vůči DSL nebo kabelovce, cenově zajímavá zejména v případě budování širokopásmového připojení na zelené louce). Nebo to mohou být např. 3 podnikoví uživatelé, každý s 75 Mbit/s, a zbývající dva kanály s celkovou kapacitou 150 Mbit/s lze rozdělit po 1 Mbit/s na 150 domácích uživatelů.

3.2 MAC vrstva

Protokol MAC (*Media Access Control*) pracující nad fyzickou vrstvou používá TDM (*Time Division Multiplex*) pro dopředný směr (od základny k uživateli, *downstream*) a TDMA (*Time-Division Multiple Access*) pro zpětný směr (od uživatele k základně, *upstream*), s centralizovaným plánovačem, který se stará o efektivní a přednostní přidělení šířky pásma. Proto je vhodný pro provoz citlivý na zpoždění, jako hlas nebo video v reálném čase.

802.16 podporuje čtyři úrovně kvality služby (QoS): pro hlasové přenosy (VoIP), přenos v reálném čase na základě výzvy (MPEG video), přenos na základě

výzvy nikoli v reálné čase (FTP) a základní službu bez jakéhokoli upřednostňování dat (*best effort*).
Na rozdíl od technik náhodného přístupu s možnými kolizemi, CSMA/CA, používaných v jiných bezdrátových sítích (802.11), zajišťuje 802.16 MAC přístup k rádiovému kanálu bez jakýchkoli potenciálních kolizí a navíc garantuje určité maximální zpoždění. TDM/TDMA také zajišťuje jednodušší podporu pro skupinové vysílání. MAC také podporuje mechanizmy pro úsporné napájení pro přenosné terminály.

802.16 podporuje pružné přidělování šířky pásma rádiových kanálů a opětovné využívání kanálů (*spectrum reuse*) pro zvýšení kapacity buňky při růstu sítě. Specifikuje také řízení vysílacího výkonu (*TPC, Transmit Power Control*) a měření kvality kanálu, jako doplňkové prostředky pro plánování buněk a efektivního využívání spektra.

Dynamický výběr kmitočtu (*DFS, Dynamic Frequecy Selection*) je povinný pro práci v bezlicenčních pásmech. Provozovatelé mohou spektrum efektivně realokovat prostřednictvím dělení buněk do sektorů podle rostoucího počtu uživatelů.

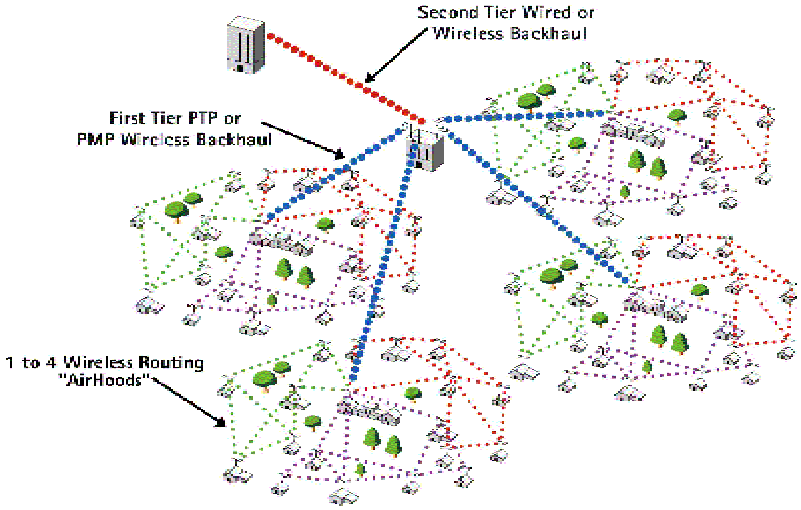
Metropolitní sítě podle 802.16 se musí, podobně jako všechny rádiové sítě, vyrovnávat s měnícími se podmínkami prostředí, protože zejména déšť může mít negativní vliv na kvalitu příjmu signálu. Specifikace proto zahrnuje řízení rádiového spoje (*RLC, Radio Link Control*) pro nastavení počátečních parametrů rádiového spojení a pro jejich změnu při změně podmínek. Zařízení podle 802.16 monitoruje kvalitu spoje po jeho inicializaci a příslušně přizpůsobuje přenosové parametry.

Zabezpečení uživatelů i vlastní komunikace ve WiMAX odpovídá současným požadavkům na síťovou bezpečnost. Autentizace a autorizace stanice v síti 802.16 probíhá na základě digitálního certifikátu X.509 přiděleného stanici ve výrobě a certifikátu výrobce. Pro ochranu dat se používá vylepšený protokol Privacy Key Management (PKM), původně specifikovaný v DOCSIS. Pro šifrování samotných přenášených dat se povinně používá Data Encryption Standard (DES) a šifrovací klíče pro přenos dat se vyměňují s použitím 3DES s klíčem pro výměnu klíčů odvozeným z autorizačního klíče.

4. Topologie

Topologie WMAN je typicky *point-to-multipoint*, kdy základnová stanice v centru komunikuje s mnoha připojenými uživateli současně. WiMAX ovšem volitelně může využít také smyčkovou topologii (*mesh*). Topologie *mesh* se jeví v bezdrátových systémech jako efektivní, protože do značné míry řeší otázky dosahu versus výkonnosti centrální základnové stanice. Koncoví uživatelé mohou využít replikace signálu bezdrátovými směrovači na cestě od základnové stanice, takže nemusí být nutně v dosahu nebo téměř v přímé viditelnosti. Signál totiž putuje nikoli přímo k cílovému přijímači, ale skok po skoku, *hop by hop.*

Kromě toho norma nabízí využití technologii moderních antén (např. antény s formováním paprsku, *beam-forming*) pro využití v BWA pro zvýšení pokrytí. Tyto moderní techniky umožňují zvýšit kapacitu, opětovné využívání spektra a průměrnou i vrcholnou propustnost na rádiový kanál.



Obrázek č. 1: Topologie mesh

5. Zabezpečení

5.1 Zabezpečení WiMAX protokolem PKM

Zabezpečení se v 802.16 provádí prostřednictvím podvrstvy *privacy*. Základnová stanice se chrání před neautorizovaným přístupem k přenosovým službám prostřednictvím šifrování toků v síti. Používá se protokol pro management klíčů mezi autentizovaným klientem a serverem, v rámci něhož základnová stanice, server, řídí distribuci klíčů klientským stanicím. Základní bezpečnostní mechanizmy zesiluje použití autentizace klienta na základě digitálních certifikátů.

Bezpečnost 802.16 je založena na protokolu pro šifrování dat přes pevnou bezdrátovou přístupovou síť, který definuje soubor podporovaných souvisejících algoritmů autentizace a šifrování dat, a na protokolu PKM (*Privacy Key Management*), který zajišťuje bezpečnou distribuci klíčů základnovou stanicí klientům.

Prostřednictvím protokolu PKM si základnová stanice a klientské stanice synchronizují klíče. Klienti používají PKM pro získání autorizace a také na podporu periodické reautorizace a obnovy klíčů. Protokol PKM verze 1 (specifikovaný pro pevný WiMAX) pro management klíčů používá digitální certifikáty podle X.509, algoritmus veřejného klíče RSA (*Rivest, Shamir and Adleman*) a silné symetrické šifrovací algoritmy pro výměnu klíčů mezi základnovou a klientskou stanicí. PKM používá model klient/server, který zajišťuje, aby na základě požadavku klienta základnová stanice (server) poslala pouze šifrovací materiál, pro který je klient autorizován. PKMv2 (specifikovaný v doplňku 802.16e) již nabízí rozšířené prvky jako novou hierarchii klíčů, AES-CMAC (*Cipher block chaining Message Authentication Code*) a MBS (*Multicast / Broadcast Service*).

5.2 Šifrování

Šifrování veřejným klíčem se používá pro nastavení sdíleného autorizačního klíče (*AK, Authorization Key*) mezi základnou a klientem, který PKM pak používá pro zabezpečení výměny klíčů pro šifrování provozu (*TEK, Traffic Encryption Key*) v délce 64 nebo 128 bitů. Tento dvouúrovňový mechanizmus distribuce klíčů umožňuje obnovit klíče pro šifrování dat bez zatížení síťových prostředků na procesně náročné operace veřejných klíčů.

Vzhledem k tomu, že WiMAX slouží pro přístup k veřejné síti, prakticky veškerý provoz je povinně šifrován pomocí 168bitového 3DES (*Triple Digital Encryption Standard*), stejného šifrování jako u VPN (*Virtual Private Network*). Volitelně lze také využít AES, podobně jako u 802.11i.

Nicméně šifrují se pouze uživatelské datové rámce, nikoli rámce určené pro management (podobná situace je v 802.11, kde se pracuje na řešení této situace prostřednictvím doplňku 802.11w *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Protected Management Frames*). Rámce pro management neochráněné šifrováním totiž dovolují útočníkům získat např. informace o uživatelích dané sítě a další charakteristiky sítě. Navíc mohou útočníci zneužít rámce managementu pro odpojení oprávněně připojených stanic v síti (obdoba záplavových útoků na sítě 802.11 prostřednictvím rámců *deauthenticate*).

5.3 Autentizace a autorizace

Základnová stanice v pevném WiMAX autentizuje klientskou stanici na základě digitálního certifikátu X.509 (RFC 3280), kterým se klientská stanice (*SS, subscriber station*) identifikuje. Certifikát obsahuje veřejný klíč a MAC (*Media Access Control*) adresu zákaznické stanice. Stanice musí certifikát předložit pro ověření základnovou stanicí a na základě úspěšné autentizace dostane autorizační klíč zašifrovaný ověřeným veřejným klíčem. Základnová stanice tak současně provede autorizaci klienta pro přístup k oprávněným (placeným službám). Díky certifikátům je obtížné zfalšovat identitu oprávněných uživatelů, takže představují dobrou obranu proti zneužití služby.

Všechny zákaznické stanice mají z výroby instalované páry veřejných/privátních klíčů RSA, nebo mají zabudovaný algoritmus pro jejich dynamické generování. V prvním případě mají také instalované certifikáty X.509, v druhém případě musí podporovat mechanizmus pro instalaci těchto certifikátů vydaných výrobcem na základě generování RSA klíčů.

Po počáteční autorizaci se musí zákaznická stanice pravidelně reautorizovat. Pouze na základě toho totiž může obnovovat stárnoucí šifrovací klíče TEK. Prvotní autorizaci zahajuje stanice vysláním zprávy *authentication information* základně (při reautorizaci se již autentizační zpráva neposílá). Zpráva obsahuje certifikát vydaný výrobcem nebo důvěryhodnou třetí stranou.

V rámci (re)autorizace pošle zákaznická stanice žádost *authorization request*, v níž žádá o autorizační klíč (AK) a také o identifikátor bezpečnostní asociace SAID (*Security Association IDentifier*). Žádost obsahuje digitální certifikát stanice a informaci o šifrovacích algoritmech, které stanice podporuje, a také identifikátor

spojení (*CID, Connection IDentifier*), který základna stanici přidělila v rámci počátečního přidružení. Na základě této žádosti základnová stanice ověří identitu stanice, určí šifrovací algoritmus a protokol, aktivuje AK pro stanici, zašifruje AK veřejným klíčem stanice a pošle zpět v odpovědi *authorization reply*. V ní ještě specifikuje životnost klíče a 4bitové pořadové číslo klíče, kterým se rozlišuje mezi generacemi autorizačních klíčů. Po sobě následující generace klíčů AK mají takovou životnost, že se jejich platnost překrývá. Je to z důvodu vyloučení přerušení služby během reautorizace.

Zásadním problémem ve WiMAX je pouze jednostranná autentizace: vedle autentizace klientské stanice chybí autentizace základnové stanice (tj. poskytovatele služby), což může snadno vést k mnoha bezpečnostním problémům. WiMAX sítě jsou proto náchylné k útokům typu *man-in-the-middle* realizovaných prostřednictvím neautorizované (falešné) základnové stanice, které mohou vystavit uživatele nepříjemným útokům.

6. WiMAX Forum

Hlavním hnacím motorem rozjezdu širokopásmových bezdrátových přípojek moderní generace je *WiMAX Forum* (*Worldwide Interoperability for Microwave Access Forum*), podpůrná organizace založená v roce 2003 a sdružující nejen výrobce čipových sad, bezdrátových a mobilních systémů a koncových zařízení, ale také provozovatele pevných i bezdrátových sítí.

Tato nezisková organizace spolupracuje s normalizačními organizacemi (především IEEE a ETSI) a také s regulátory. Práce ve Foru probíhá ve specificky zaměřených pracovních skupinách např. pro marketing, technické záležitosti, certifikace.

V současnosti počet členů Fora dosahuje 300. Mezi nimi nechybí velká jména jako *Microsoft, Nortel Networks, Motorola* či *Cisco Systems*.

WiMAX Forum se zaměřuje nejen na propagaci technologie samotné, ale zejména na certifikaci produktů podle příslušných norem. Podobně jako Wi-Fi Alliance stojí WiMAX Forum za mezinárodní certifikací zařízení WiMAX (*WiMAX Forum Certified*) na základě otestování souladu s normou a vzájemné spolupráce mezi produkty od různých výrobců.

Forum se zabývá přípravou *profilů* (souboru funkčních prvků) pro vzájemnou spolupráci systémů WiMAX. Profily se mohou týkat např. regulačních omezení spektra v různých regionech světa. Sady testů definované ve WiMAX Foru jsou formalizovány v ETSI a provozovány v nezávislé laboratoři *Cetecom*.

Plán testování a následné certifikace se ovšem mírně zdržel, a tím se posunulo i zahájení nasazení opravdu WiMAX produktů (zatím se ve světě zkoušejí a nasazují tzv. p*re-WiMAX* systémy). Vloni se na základě schválení normy 802.16 dokončila ve Foru příprava testů povinných prvků v normě. Na podzim mělo proběhnout první testování vzájemné spolupráce produktů na bázi WiMAX (*plugfest*) a na počátku letošního roku mělo začít ostré testování produktů pro získání certifikace. Nakonec se vlastní testování posunulo až na podzim letošního roku.

Pilotní nasazení certifikovaných zařízení WiMAX do bezdrátových přístupových sítí lze v souvislosti s plánem Fora očekávat koncem roku 2005. Na přelomu 2005/2006 budou patrně k dispozici první certifikované produkty pro použití

ve vnitřních prostorách, komerční projekty se rozjedou v průběhu roku 2006. Do roku 2007 by se měla objevit zařízení pro mobilní uživatele.

7. Realita WiMAXu v ČR

WiMAX v ČR je provozován v licencovaném pásmu 3,5 GHz na technologiích splňujících standard 802.16d-FDD (s kmitočtovou modulací). Existuje celá řada výrobců, kteří pracují na vývoji zařízení pro WiMAX. Mezi společnosti podílející se na vývoji wimaxových zařízení patří například Airspan, Alcatel-Lucent, Alvarion, Aperto Network, Axxcelera, Fujitsu, Intel, Motorola, Samsung, Siemens a další.

Výrobci samotných zařízení se spíše zaměřují na WiMAX mobilní, u kterého se očekává masovější rozšíření. Na trhu světovém i českém v současnosti dominují zařízení od Izraelského výrobce - společnosti Alvarion (zdroj: Sky Light Research). Alvarion díky tomu, že patřil mezi první výrobce a dodavatele WiMAXu na světě, získal mnoho zkušeností a především důvěru u zákazníků, kteří v současnosti plynule přecházejí na novější verzi WiMAXu - mobilní WiMAX. Ten je ale povolen pouze ve světě, v ČR v současnosti není jeho provoz povolen ČTÚ.

Od pilotního projektu WiMAXu v ČR na jaře 2005 zprovoznili poskytovatelé internetu na našem území již několik stovek základnových stanic a tisíce klientských jednotek pro WiMAX. WiMAX v současné době provozuje na území ČR několik desítek poskytovatelů internetu. Téměř všechny instalace jsou realizovány technologií BreezeMax 3500 izraelské společnosti Alvarion, která funguje v licenčním pásmu 3,5 GHz.

Provozovatelé využívají WiMAX částečně jako páteřní spoje ve svých sítích, částečně pak k přímému připojení uživatelů na internet. WiMAX přináší provozovatelům nové možnosti: poskytování garantovaného a spolehlivého bezdrátového připojení (což je např. u technologií Wi-Fi téměř nemožné), příležitost připojit vzdálenější lokality nebo zákazníky, kteří nemají přímou viditelnost na vysílač, provozování IP telefonie a videa po bezdrátové síti.

Čeští ISP si na WiMAXu pochvalují především rychlost instalace, spolehlivost a téměř nulový počet servisních zásahů. Spolehlivost technologie je srovnatelná s klasickým kabelovým připojením, jehož instalace je ale mnohem časově i finančně náročnější.

7.1 Nezávislé testy

V letošním roce provedla Katedra telekomunikační techniky ČVUT v Praze nezávislé testy zařízení Alvarion BreezeMAX 3500, které je použito téměř ve všech instalacích WiMAXu v ČR. Zde bylo zařízení podrobeno mnoha testům, při kterých byly v reálném provozu i laboratorně kontrolováno dodržení technických parametrů uváděných výrobcem, krajní možnosti použití zařízení a další specifika. Mezi hlavní testované parametry byly zařazeny přenosová rychlost, odezva, maximální dosah a také stabilita provozu. WiMAXová zařízení mají samozřejmě mnohem více parametrů, ale tyto čtyři jsou uživatelsky nejzajímavější.

Odezva u testovaného WiMAX systému se pohybovala kolem 15 ms. Při měření odezvy pomocí příkazu „ping“ udával systém hodnoty v rozmezí 35 až 40 ms. Tato hodnota byla způsobena nižší prioritou protokolu ICMP, který „ping“ využívá, takže doručení těchto paketů není upřednostňováno. Ke stejné situaci docházelo,

pokud byl se přenosová rychlost blížila šířce přenosového kanálu. Pak se rapidně zhoršila odezva „*ping*“, protože datové pakety měly opět vyšší prioritu. Nastala i situace, kdy došlo k úplnému zastavení přenosu ICMP paketů a příkaz „ping“ hlásil nedoručitelnost paketů. Uživatelská data byla přitom přenášena bez výpadků.

WiMAX systémy jsou navrženy tak, aby byly co nejvíce spolehlivé. Tato vlastnost se prokázala i u Breeze MAX 3500. Silné ochranné kódování, OFDM, ARQ, QoS a kvalitní rádiové rozhraní umožnily navázat komunikaci a přenášet data i v místech, kde stávající systémy nefungují nebo vykazují velkou chybovost.

8. Použitá literatura

[1] WiMAX.cz; www.wimax.cz
[2] WiMAX Forum; www.wimax-forum.org
[3] Encyklopedie Wikipedia; www.wikipedia.org