VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

PRINCIPY ZABEZPEČENÍ BEZDRÁTOVÝCH STANDARDŮ

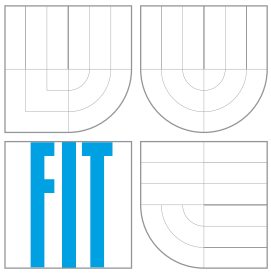
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. MARTIN VOKÁL

BRNO 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

PRINCIPY ZABEZPEČENÍ BEZDRÁTOVÝCH STANDARDŮ

PRINCIPLES OF THE WIRELESS STANDARDS SECURITY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. MARTIN VOKÁL

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. PAVEL OČENÁŠEK

BRNO 2007

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav informačních systémů Akademický rok 2006/2007

Zadání diplomové práce

Řešitel: **Vokál Martin, Bc.**
Obor: Informační systémy
Téma: **Principy zabezpečení bezdrátových standardů**
Kategorie: Počítačové sítě

Pokyny:

1. Seznamte se s bezdrátovými standardy třídy 802.xx.
2. Nastudujte jejich specifika, zejména pak principy jejich zabezpečení.
3. Vzájemně jednotlivé standardy porovnejte z bezpečnostního hlediska a vyzdvihněte vlastnosti specifické pro danou oblast.
4. Pro každý standard uveďte aktuální stav bezpečnostních mechanismů a zaměřte se především na aktuální řešené problémy (open problems).
5. Původní textová zpráva bude mít přehledový charakter. Vlastní dílo bude realizování formou elektronického dokumentu s provázáním na významné informační zdroje a popisy poskytovaných služeb.
6. Diskutujte získané znalosti a možnosti dalších směrů studií jednotlivých standardů.

Literatura:

- Dle doporučení vedoucího práce.

Při obhajobě semestrální části diplomového projektu je požadováno:

- Body 1 - 3.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci ročníkového a semestrálního projektu (30 až 40% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním paměťovém médiu (disketa, CD-ROM), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Očenášek Pavel, Ing.**, UIFS FIT VUT
Datum zadání: 28. února 2006
Datum odevzdání: 22. května 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Ing. Jaroslav Zendulka, CSc.
vedoucí ústavu

LICENČNÍ SMLOUVA
POSKYTOVANÁ K VÝKONU PRÁVA UŽÍT ŠKOLNÍ DÍLO

uzavřená mezi smluvními stranami

1. **Pan**

Jméno a příjmení: **Bc. Martin Vokál**
Id studenta: 49330
Bytem: Zborovecká 17, 678 01 Blansko
Narozen: 13. 12. 1982, Boskovice
(dále jen "autor")

a

2. **Vysoké učení technické v Brně**

Fakulta informačních technologií
se sídlem Božetěchova 2/1, 612 66 Brno, IČO 00216305
jejímž jménem jedná na základě písemného pověření děkanem fakulty:

.....
(dále jen "nabyvatel")

Článek 1
Specifikace školního díla

1. Předmětem této smlouvy je vysokoškolská kvalifikační práce (VŠKP):
diplomová práce

Název VŠKP: Principy zabezpečení bezdrátových standardů
Vedoucí/školitel VŠKP: Očenášek Pavel, Ing.
Ústav: Ústav informačních systémů
Datum obhajoby VŠKP: .....

VŠKP odevzdal autor nabyvateli v:

tištěné formě počet exemplářů: 1
elektronické formě počet exemplářů: 2 (1 ve skladu dokumentů, 1 na CD)

2. Autor prohlašuje, že vytvořil samostatnou vlastní tvůrčí činností dílo shora popsané a specifikované. Autor dále prohlašuje, že při zpracovávání díla se sám nedostal do rozporu s autorským zákonem a předpisy souvisejícími a že je dílo dílem původním.
3. Dílo je chráněno jako dílo dle autorského zákona v platném znění.
4. Autor potvrzuje, že listinná a elektronická verze díla je identická.

Článek 2
Udělení licenčního oprávnění

1. Autor touto smlouvou poskytuje nabyvateli oprávnění (licenci) k výkonu práva uvedené dílo nevýdělečně užít, archivovat a zpřístupnit ke studijním, výukovým a výzkumným účelům včetně pořizování výpisů, opisů a rozmnoženin.
2. Licence je poskytována celosvětově, pro celou dobu trvání autorských a majetkových práv k dílu.
3. Autor souhlasí se zveřejněním díla v databázi přístupné v mezinárodní síti:
   - ☐ ihned po uzavření této smlouvy
   - ☐ 1 rok po uzavření této smlouvy
   - ☐ 3 roky po uzavření této smlouvy
   - ☐ 5 let po uzavření této smlouvy
   - ☐ 10 let po uzavření této smlouvy

   (z důvodu utajení v něm obsažených informací)
4. Nevýdělečné zveřejňování díla nabyvatelem v souladu s ustanovením § 47b zákona č. 111/ 1998 Sb., v platném znění, nevyžaduje licenci a nabyvatel je k němu povinen a oprávněn ze zákona.

Článek 3
Závěrečná ustanovení

1. Smlouva je sepsána ve třech vyhotoveních s platností originálu, přičemž po jednom vyhotovení obdrží autor a nabyvatel, další vyhotovení je vloženo do VŠKP.
2. Vztahy mezi smluvními stranami vzniklé a neupravené touto smlouvou se řídí autorským zákonem, občanským zákoníkem, vysokoškolským zákonem, zákonem o archivnictví, v platném znění a popř. dalšími právními předpisy.
3. Licenční smlouva byla uzavřena na základě svobodné a pravé vůle smluvních stran, s plným porozuměním jejímu textu i důsledkům, nikoliv v tísni a za nápadně nevýhodných podmínek.
4. Licenční smlouva nabývá platnosti a účinnosti dnem jejího podpisu oběma smluvními stranami.

V Brně dne: .....

....

Nabyvatel Autor

Abstrakt

Počítačové sítě jsou v rámci organizace IEEE normalizovány výborem 802, jehož součástí je v současnosti šest pracovních skupin vyvíjejících specifikace pro bezdrátové komunikace. Těmi jsou IEEE 802.11 pro bezdrátové lokální sítě, IEEE 802.15 pro bezdrátové osobní sítě, IEEE 802.16 pro bezdrátové metropolitní sítě, IEEE 802.20 pro mobilní širokopásmový přístup, IEEE 802.21 pro vertikální handover a IEEE 802.22 pro bezdrátové regionální sítě. Diplomová práce se zaměřuje na bezpečnostní analýzu jednotlivých standardů, uvádí hrozby, zranitelná místa, aktuální bezpečnostní opatření a provádí vzájemné srovnání bezdrátových norem z bezpečnostního hlediska s vyzdvižením vlastností specifických pro danou oblast. Závěr práce je věnován celkovému zhodnocení projektu, jeho přínosům a možnostem dalšího vývoje ve formě navazujících studií.

Klíčová slova

bezpečnost, standard, IEEE, bezdrátová komunikace, bezdrátová lokální síť, bezdrátová osobní síť, bezdrátová metropolitní síť, mobilní širokopásmový přístup, vertikální handover, bezdrátová regionální síť, WLAN, WPAN, WMAN, MBWA, MIH, WRAN, IEEE 802.11, IEEE 802.15, IEEE 802.16, IEEE 802.20, IEEE 802.21, IEEE 802.22, Wi-Fi, Bluetooth, WiMedia, ZigBee, WiMax, Mobile-Fi

Abstract

Computer networks are in the scope of the IEEE organization normalized by the 802 board which currently comprises six working groups for wireless communications. IEEE 802.11 for wireless local area networks, IEEE 802.15 for wireless personal area networks, IEEE 802.16 for wireless metropolitan area networks, IEEE 802.20 for mobile broadband wireless access, IEEE 802.21 for media independent handover and IEEE 802.22 for wireless regional area networks. This master's thesis focuses on a security analysis of particular standards, describes threats, vulnerabilities, current security measures and mutually compares wireless specifications from a security point of view. The conclusion is devoted to overall evaluation of the project, to its contributions, possible enhancements and continuation in the form of consequential studies.

Keywords

security, standard, IEEE, wireless security, wireless local area network, wireless personal area network, wireless metropolitan area network, mobile broadband wireless access, media independent handover, wireless regional area network, WLAN, WPAN, WMAN, MBWA, MIH, WRAN, IEEE 802.11, IEEE 802.15, IEEE 802.16, IEEE 802.20, IEEE 802.21, IEEE 802.22, Wi-Fi, Bluetooth, WiMedia, ZigBee, WiMax, Mobile-Fi

Citace

Martin Vokál: Principy zabezpečení bezdrátových standardů, diplomová práce, Brno, FIT VUT v Brně, 2007

Principy zabezpečení bezdrátových standardů

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením Ing. Pavla Očenáška. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Martin Vokál
22. května 2007

Poděkování

Děkuji Ing. Pavlu Očenáškovi za odborné rady, připomínky a vedení celé diplomové práce.

© Martin Vokál, 2007.
Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

Kapitola 1

Úvod

Počátky té nejprimitivnější formy *bezdrátové komunikace* sahají několik století nazpět až do doby před průmyslovou revolucí. Informace byly tehdy šířeny především pomocí různých kouřových, zvukových a světelných signálů. Skutečný zrod bezdrátových technologií však bývá často spojováván až se jménem italského vědce *Guglielma Marconiho*. Ten roku 1895, několik desetiletí po vynálezu telefonu, uskutečnil první *rádiový přenos* informace na vzdálenost více než jedné míle a v roce 1901 pak první transatlantické vysílání. Zpočátku se sice informace přenášely pomocí *Morseovy abecedy*, ale už roku 1904 proběhla první demonstrace bezdrátového přenosu *hlasu*. Postupem času docházelo k výraznému zlepšování rádiových technologií, především co se týká zvyšování kvality a dosahu signálu, což přispělo k pozdějšímu rozvoji *rádiového* (1920, první komerční stanice), a *televizního* (1930, první experimenty BBC) vysílání. Zásadní zdokonalování rádiových přenosů nastalo dále po druhé světové válce. Roku 1947 se objevily první teoretické návrhy moderních *buňkových rádiových systémů*, které byly založeny na pokrytí většího území pomocí základnových stanic (jako u pozdějšího GSM). První analogový buňkový radiotelefonní systém byl pak vyzkoušen v roce 1961. Za významný milník pro *digitální komunikaci* lze považovat rok 1971, kdy pod názvem *ALOHANET* vznikla první *bezdrátová datová síť*. Byla založena na *paketech* (tzv. *Packet Radio*) a spojovala počítače rozmístěné na několika havajských ostrovech. V osmdesátých letech sice stále dominovaly technologie využívající analogové signály (*1G*), na jejich konci se však začaly objevovat první digitální radiotelefonní systémy (*2G*), přičemž největší úspěch z nich zaznamenal *GSM*. Ačkoliv se v osmdesátých letech několik firem začalo zabývat bezdrátovým digitálním přenosem dat a vyvinuly proprietární, na sobě nezávislá řešení, přenosová rychlost se pohybovala jen v řádech jednotek kilobitů. Další pokrok v bezdrátovém přenosu dat nastal v letech devadesátých, kdy došlo k uvedení prvních komerčních produktů pro *bezdrátové lokální sítě* (1990, *AT&T WaveLAN*), později podpořené vznikajícími *mezinárodními bezdrátovými standardy* (1997, *IEEE 802.11*). Od konce minulého století pak lze pozorovat výrazný rozvoj vysokorychlostních digitálních bezdrátových komunikací, včetně těch mobilních ($2.5G - 4G$), současně s razantním ústupem analogových systémů. Další vývoj v této oblasti bude i nadále pokračovat a není ani zdaleka u konce. Dodatečné informace o technologickém vývoji různých typů bezdrátových sítí jsou uvedeny dále v rámci jednotlivých kapitol práce, jako další doplňující zdroje lze pak použít [1, 2], tématu se podrobně věnuje [3].

V současnosti bezdrátová komunikace proniká stále více do mnoha oblastí lidských činností, zvyšuje se podpora mobility a rychlosti datových přenosů. Do budoucna se pak předpokládá, že provázanost různých typů bezdrátových sítí a vzájemná komunikace mezi mobilními zařízeními povede k naprosté dostupnosti informačních zdrojů a tedy naplnění

vize tzv. *ambientní inteligence*[1]. Během posledních několika let se v oblasti bezdrátové komunikace navíc objevuje jeden významný fenomén. Nejde přitom jen o stále rozšiřující se pole působnosti bezdrátových technologií, kterým díky jejich mimořádné flexibilitě musejí stále více ustupovat původní metalické spoje. Především zatímco v minulosti byla bezdrátová komunikace využívána zejména pro přenos hlasu, nyní naopak rychle roste na významu *přenos dat* a tento trend bude dále posilovat. S novými aplikacemi a zařízeními využívajícími bezdrátové sítě sice přirozeně vznikají ryze technické otázky a problémy, jako jsou např. způsob napájení, spolehlivost přenosu dat, dosah signálu, koexistence nejrůznějších typů zařízení a sítí v daném prostoru a na určité frekvenci apod., avšak nejdiskutovanějším a nejožehavějším tématem je už delší dobu *bezpečnost*.

Bezdrátovou komunikaci lze vzhledem k přenosu dat přes *vzdušné rozhraní* považovat z bezpečnostního hlediska obecně za daleko náchylnější, než je tomu u klasických, drátových sítí. Navíc nejvíce rizikové jsou právě nejrozšířenější *rádiové sítě*, zdaleka takový problém nenastává u optických bezdrátových sítí. Na rádiové sítě lze totiž poměrně snadno provádět velké množství útoků různých typů a je tak nezbytné na odlišných úrovních věnovat velkou pozornost vhodným bezpečnostním mechanismům. Jejich úkolem je zamezit neoprávněnému využívání služeb a prostředků sítě, zajistit jejich dostupnost, ochránit připojené uživatele před tím, aby se za ně vydával někdo jiný, a v neposlední řadě také zabezpečit samotný obsah komunikace i dat uložených v síťových uzlech proti krádeži, modifikaci nebo jejich úplnému znehodnocení.

Bezpečností bezdrátových technologií je nutné se zabývat o to intenzivněji vzhledem ke skutečnosti, že stále narůstá objem (citlivých) dat přenášených ve stále více vzájemně provázanějších bezdrátových sítí různých typů a velikostí, které konvergují v jeden velký globální celek. Proto chceme-li se věnovat tématu bezpečnosti bezdrátové komunikace, pro niž v dnešní době existuje už velké množství mezinárodně uznávaných standardů a další stále vznikají, je velmi vhodné zaujmout komplexní pohled na celou problematiku. Publikace o bezdrátových sítí a jejich zabezpečení jsou sice dostupné, v převážné většině se však omezují pouze na bezdrátové lokální sítě, a to především na jejich popis, návrh, praktické nasazení a návody a postupy na jejich zabezpečení. V některých z nich lze nalézt i vysvětlení principů zabezpečení příslušných bezdrátových standardů, ale odborných prací, které by se současně zabývaly zabezpečením různých typů bezdrátových sítí v souvislostech a viděly celou problematiku v širším měřítku, je podstatně méně.

Předkládaná práce má za cíl provést důkladný rozbor a srovnání principů v současnosti dostupných bezpečnostních mechanismů vybraných bezdrátových standardů a nabídnout ucelený přehled bezpečnostních problémů v této oblasti. Primárně se zaměřuje na bezpečnost rádiových bezdrátových sítí založených na normách mezinárodní organizace IEEE a jejího výboru 802. Přestože bezdrátové standardy vyvíjené institutem IEEE a komunikace na nich založené patří mezi nejrozšířenější, představují jen malou část z celého spektra existujících bezdrátových technologií. V práci tak nejsou zahrnuty např. bezdrátové sítě institutu ETSI, klasické mobilní sítě, satelitní komunikační systémy a proprietární bezdrátové technologie. Ačkoli by bylo nepochybně přínosné a zajímavé se navíc zabývat i zabezpečením uvedených typů sítí, takto komplexně koncipovaná problematika přesahuje rámec této práce.

Práce sice připomíná, avšak neobsahuje důkladné vysvětlení elementárních pojmů a základních principů z oblastí, jako jsou počítačové sítě, bezdrátová komunikace, počítačová bezpečnost a kryptografie. Zde je čtenář odkázán na specializované odborné publikace, které danou problematiku pokrývají v dostatečném rozsahu.

[1] angl. *Ambient Intelligence*, ekvivalentním termínem je *Ubiquitous Computing*, více viz [4, 5]

Text písemného dokumentu je strukturovaný, členěný do logicky navazujících kapitol a podkapitol několika úrovní. **Kapitola 1** je úvodní. Další dvě kapitoly byly s určitými úpravami převzaty ze semestrálního projektu, na který tato diplomová práce navazuje. **Kapitola 2** představuje společné rysy bezdrátových sítí specifikovaných výborem IEEE 802 a stručně charakterizuje jednotlivé standardy. **Kapitola 3** se zabývá otázkami bezpečnosti lokálních bezdrátových sítí podle normy IEEE 802.11. **Kapitola 4** analyzuje zabezpečení bezdrátových osobních sítí IEEE 802.15. **Kapitola 5** je věnována bezpečnosti bezdrátových metropolitních sítí definovaných pracovní skupinou IEEE 802.16. **Kapitola 6** nastiňuje problematiku zabezpečení mobilních širokopásmových bezdrátových sítí podle standardu IEEE 802.20. **Kapitola 7** se zaměřuje na bezpečnostní prvky normy IEEE 802.21 pro vertikální handover. **Kapitola 8** charakterizuje standard IEEE 802.22 jako specifikaci bezdrátových regionálních sítí. **Kapitola 9** jednotlivé standardy srovnává z bezpečnostního hlediska a vyzdvihuje jejich specifické vlastnosti. **Kapitola 10** je věnována praktické části diplomové práce. **Kapitola 11** práci uzavírá, zhodnocuje dosažené výsledky a naznačuje další možný vývoj projektu.

Kapitola 2

Bezdrátové standardy IEEE

V procesu specifikace bezdrátových komunikačních protokolů mají v současné době zcela zásadní význam *mezinárodní normalizační organizace*. Právě absence všeobecně uznávaných průmyslových *standardů* znamenala v minulosti, kdy byly dostupné pouze proprietární prostředky, jednu z hlavních příčin malé rozšířenosti a špatné interoperability bezdrátových technologií. Mezi nejvýznamnější normalizační organizace s nadnárodní působností (nejen) v oblasti bezdrátové komunikace patří *ITU* (ITU-R pro radiokomunikace), *ISO*, *ANSI*, *IEEE* (viz část 2.1) a *CEPT*, z jehož iniciativy vznikl institut *ETSI*.

Dále existují také sdružení a organizace řízené *zájmovými skupinami*, jejichž činnost se dotýká vývoje norem a technologií pro bezdrátové komunikace. Ze zástupců lze uvést např. *3GPP*, *CommunityWireless*, *Freenetworks.org*, *IrDA*, *OFDM Forum*, *SIG*, *Wiana*, *WLANA*, *Wi-Fi Alliance* aj. Na lokální úrovni pak působí další skupiny (např. *WirelessAnarchy*).

Důležité jsou ale i *vládní instituce*, které regulují využívání rádiového spektra ve vlastní jurisdikci. V USA tuto roli plní *FCC* (*Federal Communications Commission*), v Kanadě *CRTC* (*Canadian Radio-television and Telecommunications Commission*) a např. v Británii *Ofcom* (*Office of Communications*). Pro ČR je to *ČTÚ* (*Český Telekomunikační Úřad*).

2.1 IEEE

IEEE (*Institute of Electrical and Electronics Engineers*, `www.ieee.org`) od roku 1963 působí jako mezinárodní organizace pro technologický rozvoj v oblasti elektrotechniky, elektroniky, počítačové vědy a příbuzných disciplín. Se 365 000 vědci, inženýry a dalšími odborníky z více než 150 zemí světa jde o největší profesní uskupení svého druhu. Náplní IEEE je vědecká, vzdělávací a publikační činnost[1], podpora a pořádání konferencí, seminářů a práce na tvorbě mezinárodních průmyslových norem (přibližně 900 schválených, 400 ve fázi vývoje), čímž se zabývá skupina *IEEE-SA* (*IEEE Standards Association*).

Vývoj každého IEEE standardu prochází následujícími etapami: nalezení sponzora, požadavek na autorizaci projektu, sestavení pracovní skupiny, hrubý návrh standardu, hlasování, provedení recenze komisí a závěrečné schválení normy. Další informace o vývoji IEEE standardů lze dohledat v [6]. Kromě samotné oblasti elektrotechniky, informatiky a telekomunikací se normy organizace IEEE o celkovém počtu téměř 1300[2] dotýkají i jiných disciplín, mezi které patří např. biomedicína, zdravotnictví, doprava, letectví, energetika aj. Komunikačním sítím včetně těch bezdrátových se věnuje výbor *IEEE 802* (viz část 2.2).

[1] autorství téměř třetiny publikací v oboru elektrotechniky, elektroniky a informatiky patří IEEE

[2] úplný přehled je dostupný na URL: `http://ieeexplore.ieee.org/xpl/standards.jsp` (květen 2007)

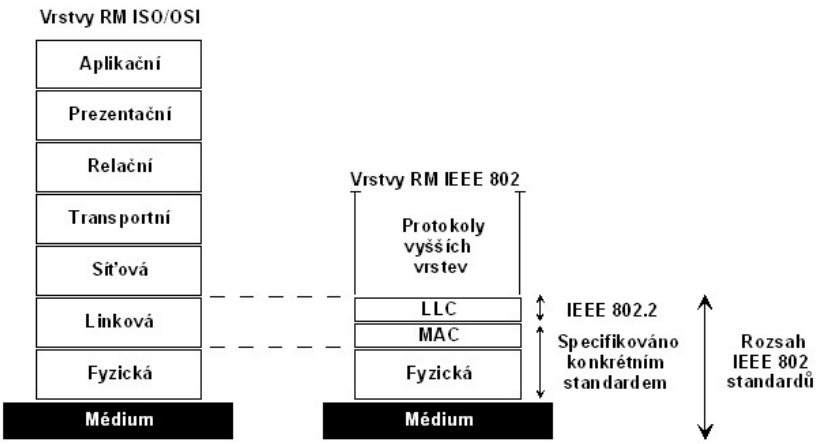
2.2 IEEE 802

Výbor *IEEE 802* byl zřízen v roce 1980[3] pro normalizaci *lokálních* a *metropolitních* sítí. Vyvíjené standardy spravuje *IEEE 802 LAN/MAN Standards Committee* (*LMSC*). Služby a protokoly definované IEEE 802 pokrývají dvě nejnižší vrstvy RM ISO/OSI, tedy *linkovou* a *fyzickou*, s vazbou na vrstvu síťovou. Linkovou vrstvu IEEE 802 chápe jako dvě podvrstvy (viz obr. 2.1). Těmi jsou *podvrstva řízení logického spoje* (*LLC*, *Logical Link Control*) a *podvrstva řízení přístupu k médiu* (*MAC*, *Medium Access Control*). Následující odstavce uvádí jen stručný popis činností jednotlivých (pod)vrstev, další informace obsahuje [7].

LLC podvrstva je stejná bez ohledu na fyzické médium (např. Ethernet, WLAN, ...) a její protokol pro sítě IEEE 802, ale i některé další, specifikuje standard IEEE 802.2 [8]. Má podobné funkce jako klasický protokol HDLC. Zodpovídá za navazování/rušení spojení, řízení toku dat, správu chyb a představuje služební rozhraní pro síťovou vrstvu.

Podvrstva MAC zabezpečuje ty funkce linkové vrstvy, které jsou vázány na konkrétní síťovou technologii. Představuje rozhraní mezi LLC podvrstvou a fyzickou vrstvou. Její hlavní úkoly jsou řízení přístupu ke sdílenému fyzickému přenosovému médiu, iniciace vysílání a příjem dat pro fyzickou vrstvu a adresování. Vzhledem k požadavku na rychlost díky přímé spolupráci s fyzickou vrstvou bývá realizována typicky hardwarově.

Fyzická vrstva popisuje fyzické vlastnosti přenosového média, tzn. jeho elektrické a mechanické charakteristiky, signály pro přenos informací, fyzikální vlastnosti konektorů a kabelů, kódování, modulační a synchronizační schémata, datovou propustnost apod.



Obrázek 2.1: Normy IEEE 802 zahrnují LLC podvrstvu, MAC podvrstvu a fyzickou vrstvu

2.2.1 Pracovní a technické poradní skupiny

Vývojový proces každé normy zahrnuje ustavení *pracovní skupiny* (*WG*, *Working Group*). Tu v rámci výboru IEEE 802 zakládá komise LMSC, která má za úkol předkládat návrhy norem, doporučené postupy a metodické pokyny. Po jejich závěrečném schválení WG pracuje na recenzi, revizi a stvrzení příslušných dokumentů. Podobně jako WG existují rovněž *technické poradní skupiny* (*TAG*, *Technical Advisory Group*) a před započetím samotné standardizace operují navíc ještě tzv. *studijní skupiny* (*SG*, *Study Group*) pro získání dostatečného množství informací z dané oblasti. Jednotlivé podvýbory[4] uvádí tab. 2.1.

[3] číslo projektu, 802, bylo v té době jen další volné k přiřazení, přesto bývá spojováno právě s rokem 1980

[4] aktuální přehled je k dispozici na URL: `http://www.ieee802.org/dots.html` (květen 2007)

Tabulka 2.1: Normy výboru IEEE 802 s názvy pracovních a technických poradních skupin

Standard	**Status**	**Pracovní (WG) / Technická poradní (TAG) skupina**
802.1	aktivní	*Higher Layer LAN Protocols WG*
802.2	neaktivní	*Logical Link Control WG*
802.3	aktivní	*Ethernet WG*
802.4	rozpuštěno	*Token Bus WG*
802.5	neaktivní	*Token Ring WG*
802.6	rozpuštěno	*Metropolitan Area Network WG*
802.7	rozpuštěno	*Broadband TAG*
802.8	rozpuštěno	*Fiber Optic TAG*
802.9	rozpuštěno	*Isochronous LAN WG*
802.10	rozpuštěno	*Security WG*
802.11	aktivní	*Wireless LAN WG*
802.12	neaktivní	*Demand Priority WG*
802.14	rozpuštěno	*Cable Modem WG*
802.15	aktivní	*Wireless Personal Area Network WG*
802.16	aktivní	*Broadband Wireless Access WG*
802.17	aktivní	*Resilient Packet Ring WG*
802.18	aktivní	*Radio Regulatory TAG*
802.19	aktivní	*Coexistence TAG*
802.20	aktivní	*Mobile Broadband Wireless Access WG*
802.21	aktivní	*Media Independent Handoff WG*
802.22	aktivní	*Wireless Regional Area Network WG*

2.2.2 Normy pro bezdrátovou komunikaci

V následujícím textu doplněném obrázkem 2.2 jsou stručně charakterizovány ty standardy výboru IEEE 802, které se týkají bezdrátové komunikace. Přehled má pouze orientační charakter, problematiku z pohledu bezpečnosti podrobně rozvíjejí navazující kapitoly práce.

IEEE 802.11 - WLAN

Bezdrátové lokální sítě (*WLAN*, *Wireless Local Area Network*) jako alternativní řešení ke klasickým (drátovým) LAN normalizuje podvýbor *IEEE 802.11* (viz kap. 3). Standard IEEE 802.11 je známý jako ***Wi-Fi***. Jeho první vydání z roku 1997 bylo ale rozšířeno již o řadu doplňků a další vývoj probíhá i v současnosti.

IEEE 802.15 - WPAN

Bezdrátové osobní sítě (***WPAN***, *Wireless Personal Area Network*) jsou specifikovány normou *IEEE 802.15* (viz kap. 4). Umožňují komunikaci přenosných a mobilních zařízení, jako jsou osobní počítače, PDA, periferie, pagery, mobilní telefony a produkty spotřební elektroniky, v tzv. *osobním operačním prostoru* (*POS*, *Personal Operating Space*). V rámci IEEE 802.15 dosud vznikly tři samostatné normy, které se liší především podporovanými rychlostmi, QoS a energetickými nároky. Jde o specifikace představující na fyzické a linkové vrstvě základ technologií ***Bluetooth*** (2001), ***WiMedia*** (2003) a ***ZigBee*** (2003).

IEEE 802.16 - WMAN

Bezdrátové metropolitní sítě (*WMAN*, *Wireless Metropolitan Area Network*) definuje pracovní skupina *IEEE 802.16* (viz kap. 5). Norma specifikuje technologii *širokopásmového bezdrátového přístupu* (*BWA*, *Broadband Wireless Access*) a je známá jako ***WiMAX***. První verze standardu z roku 2001 prošel revizí v roce 2004, nové služby přinášejí pozdější doplňky.

IEEE 802.18

Technická poradní skupina *IEEE 802.18* zajišťuje *regulaci využívání rádiového spektra*. Vzhledem k zaměření práce ale není její činnost předmětem navazujících kapitol.

IEEE 802.19

IEEE 802.19 je technickou poradní skupinou, která se zabývá *koexistencí bezdrátových standardů* výboru IEEE 802. Stejně jako IEEE 802.18 jí nebude věnována další pozornost.

IEEE 802.20 - MBWA

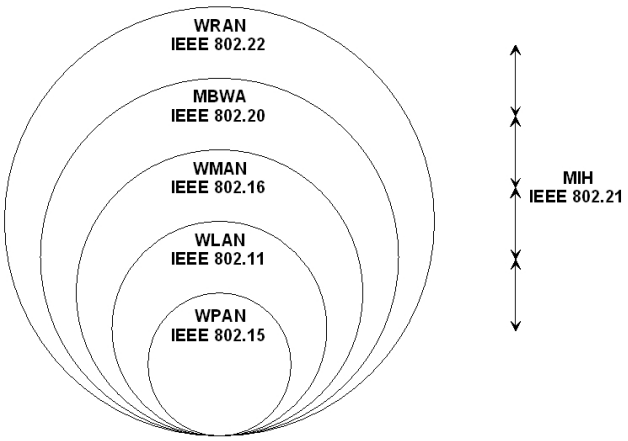
Standard *IEEE 802.20* (viz kap. 6) dosud schválen nebyl (plánováno na rok 2008). Definuje ***mobilní širokopásmové bezdrátové sítě*** (*MBWA*, *Mobile Broadband Wireless Access*), někdy označované jako ***Mobile-Fi***. Oproti normě IEEE 802.16 pro WMAN však nabídne jiná operační frekvenční pásma a implicitní podporu mobility (i při vysokých rychlostech).

IEEE 802.21 - MIH

IEEE 802.21 (viz kap. 7) řeší ***vertikální handover*** (***MIH***, *Media Independent Handoff*), a to nejen napříč sítěmi IEEE 802 (např. i GSM a GPRS). Dokončení se očekává roku 2007.

IEEE 802.22 - WRAN

Bezdrátové regionální sítě (*WRAN*, *Wireless Regional Area Network*) do budoucna umožní standard *IEEE 802.22* (viz kap. 8) s předpokládaným schválením v roce 2008. WRAN bude poskytovat širokopásmové služby na základě využití nepoužívaných TV kanálů.



Obrázek 2.2: Hierarchie bezdrátových sítí třídy IEEE 802 (uspořádání dle dosahu)

Kapitola 3

Zabezpečení WLAN IEEE 802.11

Bezdrátové lokální sítě (***WLAN***, ***Wireless Local Area Network***) v rámci výboru IEEE 802 normalizuje pracovní skupina ***IEEE 802.11***. Počátky komerčního vývoje WLAN sahají až do poloviny osmdesátých let (historicky první ale byla havajská univezitní síť *ALOHANET* již v roce 1971), kdy komise FCC poprvé zpřístupnila rádiové spektrum *ISM* (*Industrial*, *Scientific*, *Medical*), které je primárně určeno pro technologické aplikace v průmyslu, vědě a medicíně. Jedná se o kmitočty v rozsahu 902 MHz až 5.85 GHz, což je pásmo přímo navazující na frekvenční oblast využívanou mobilní telefonií. ISM pásmo přineslo zásadní výhody jak pro výrobce bezdrátových technologií, kteří mohli počítat s přiděleným spektrem při vývoji svých produktů, tak i pro koncové uživatele, jimž odpadla komplikace v podobě získávání licencí k provozu vlastních zařízení. Přestože šlo tehdy o významný impuls pro průmysl bezdrátových technologií, rozvoj WLAN nebyl v průběhu osmdesátých ani devadesátých let nijak dynamický. V situaci zapříčiněné absencí norem jednotliví výrobci vytvářeli vlastní, proprietární technologie pro bezdrátové LAN, které byly příliš finančně nákladné, nedostatečně odolávaly rušení a nenabízely ani uspokojivé přenosové rychlosti. Značného rozšíření se bezdrátové lokální sítě dočkaly postupně až během posledních deseti let díky normě IEEE 802.11 a jejím pozdějším dodatkům.

Pracovní skupina 802.11 organizace IEEE byla zřízena v září roku 1990 s cílem vytvořit specifikaci pro WLAN pracující v pásmu ISM jako alternativu ke klasickému Ethernetu. První verze standardu IEEE 802.11, schválená roku 1997, později prošla několika revizemi a byla obohacena o řadu doplňků (viz tab. 3.1), které původní normu v mnoha ohledech zdokonalují. V současnosti jsou WLAN specifikované standardem IEEE 802.11, přezdívané jako ***Wi-Fi*** (***Wireless Fidelity***), ve své kategorii zdaleka nejrozšířenější a často se používají i jako přístupová síť k Internetu, přestože za tímto účelem navrženy nebyly.

Evropská alternativa WLAN institutu ETSI v podobě standardů *HIPERLAN/1* a *HIPERLAN/2* může sice IEEE 802.11 konkurovat vyspělostí technologie (srovnatelný dosah i rychlost datových přenosů, dynamický výběr frekvence, QoS, efektivní správa spotřeby, autokonfigurace, vysoká bezpečnost, ...), její tržní podíl je ale nepoměrně nižší. Technologie WLAN založené na jiných normách pak mají z pohledu trhu význam zcela zanedbatelný.

Mimo obecných výhod[1] bezdrátových lokálních sítí významně přispěla k prosazení právě WLAN IEEE 802.11 také vzájemná kompatibilita bezdrátových zařízení nejrůznějších výrobců. Tu zajišťuje sdružení *Wi-Fi Alliance* (`www.wi-fi.org`), v minulosti známé jako *WECA* (*Wireless Ethernet Compatibility Aliance*). Produktům pro WLAN, které splňují všechna požadovaná kritéria, uděluje Wi-Fi Alliance všeobecně uznávané logo Wi-Fi.

[1] především mobilita uživatelů, flexibilita, rychlá, snadná a nenákladná instalace a rozšiřitelnost

3.1 Architektura WLAN podle normy IEEE 802.11

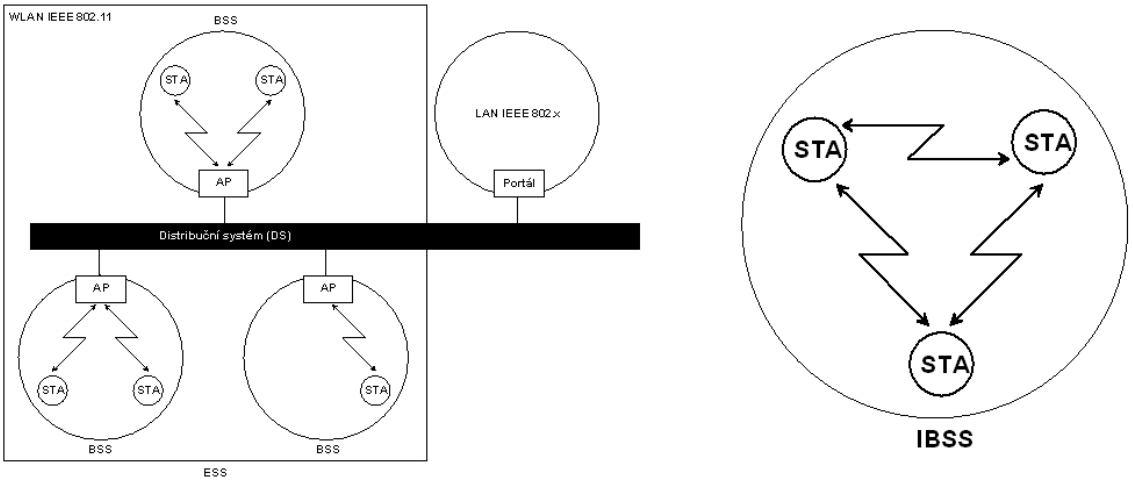
Následující text stručně charakterizuje architekturu IEEE 802.11 s cílem definice základních principů a pojmů, které budou využity dále v rámci výkladu témat věnovaných bezpečnosti. Detailní a úplný popis problematiky poskytuje norma [9], dále viz např. [10, 11, 12, 13].

3.1.1 Topologie

Dle normy IEEE 802.11 mohou mít WLAN podobu jak *buňkového systému*, kdy pracují v tzv. *infrastrukturním režímu*, tak i tzv. *Ad-Hoc sítě* (viz obr. 3.1).

V *infrastrukturní WLAN* se *stanice* (*STA*) sdružují do *buněk* (*BSS*, *Basic Service*), z nichž jedna plní roli základnové stanice - jde o tzv. *přístupový bod* (*AP*, *Access Point*). Skrz AP probíhá veškerá lokální komunikace stanic v rámci jedné buňky. Dále AP připojuje BSS k *distribučnímu systému* (*DS*, *Distribution System*), který propojuje jednotlivé buňky WLAN a současně celý komplex (*ESS*, *Extended Service Set*) napojuje přes *portál* (*Portal*) k jiné (drátové) lokální sítí. Jednotlivé přístupové body jsou odlišeny identifikátorem *SSID* (*Service Set IDentifier*). V souvislosti s BSS jde o *BSSID*, v případě ESS pak o *ESSID*.

Ad-hoc WLAN naopak žádný páteřní systém ani AP nepoužívají, komunikace stanic v buňce *IBSS* (*Independent Basic Service Set*, identifikátor *IBSSID*) probíhá přímo.



Obrázek 3.1: WLAN IEEE 802.11 v infrastrukturním (vlevo) a Ad-Hoc režimu (vpravo)

3.1.2 MAC podvrstva

MAC podvrstva WLAN IEEE 802.11 pracuje s *datovými*, *řídicími* a *management* rámci. *Řídicí rámce* (*RTS*, *CTS*, *ACK*) používá pro *přístup k médiu* - mechanismus *DFWMAC* (*Distributed Foundation Wireless MAC*). Režim *DCF* (*Distributed Coordination Function*) s využitím *CSMA/CA*, *DCF s RTS/CTS* řešící problém skryté stanice a volitelně mód *PCF* (*Point Coordination Function*) pro přenosy v reálném čase. *Management rámce* pak slouží za účelem *asociace* (*Association Request*, *Association Response*), tzn. pro připojení STA k BSS (může iniciovat stanice nebo přístupový bod - buď *aktivní*, nebo *pasivní skenování*), *reasociace* (*Reassociation Request*, *Reassociation Response*) a *disasociace* (*Disassociation*), *autentizace* (*Authentication*), *deautentizace* (*Deauthentication*), *synchronizace* (*Beacon*) a výměny informací o parametrech jednotlivých stanic (*Probe Request*, *Probe Response*).

3.1.3 Fyzická vrstva

Původní norma IEEE 802.11 nabízela realizaci fyzické vrstvy buď infračerveným zářením, nebo rádiovým signálem na bázi rozprostřeného spektra FHSS a DSSS v bezlicenčním pásmu ISM 2.4 GHz[2]. Ve všech třech případech byly podporovány rychlosti 1 a 2 Mbit/s. Infračervené přenosy dat se však ve WLAN IEEE 802.11 prakticky nepoužívají. DSSS se uplatňuje v současnosti v sítích 802.11b/g, doplňky 802.11a/g využívají i OFDM. Pozdější specifikace (viz tab. 3.1) přinášejí mj. vyšší datovou propustnost a využití pásma 5 GHz. Dosah sítí WLAN IEEE 802.11 se v závislosti na daných podmínkách pohybuje v interiérech řádově v desítkách metrů, na volném prostranství jsou to stovky metrů (speciální antény s vysokým ziskem však mohou dosah zvýšit až na několik kilometrů).

3.1.4 Doplňky standardu IEEE 802.11

Další vývoj standardu IEEE 802.11 pokračuje ve formě doplňků a doporučení,[3] jejichž přehled[4] uvádí tab. 3.1. U dokončených specifikací, jejichž obsahy jsou přístupné na URL: `http://standards.ieee.org/getieee802/802.11.html` (květen 2007), je v uveden i rok schválení, u ostatních předpokládaný rok ratifikace (s otazníkem).

Tabulka 3.1: Doplňky a doporučení k původní normě IEEE 802.11

Doplněk	**Rok**	**Popis**
802.11a	1999	5.1 až 5.3 GHz, 5.725 až 5.825 GHz, až 54 Mbit/s, OFDM
802.11b	1999	2.4 až 2.485 GHz, až 11 Mbit/s, DSSS
802.11c	2001	procedury pro komunikační mosty mezi přístupovými body
802.11d	2001	mezinárodní harmonizace frekvenčního pásma
802.11e	2005	podpora pro kvalitu služeb (QoS) na MAC podvrstvě
802.11F	2003	protokol IAPP - handover mezi AP různých výrobců
802.11g	2003	2.4 až 2.485 GHz, až 54 Mbit/s, DSSS/OFDM
802.11h	2003	doplňuje 802.11a o dynamickou volbu kanálu a řízení výkonu
802.11i	2004	nové bezpečnostní mechanismy na MAC podvrstvě
802.11j	2004	možnost použití pásma 4.9 - 5 Ghz, týká se pouze Japonska
802.11k	2007?	metody pro měření a správu rádiových zdrojů
802.11m	-	údržba a korekce dosud vydaných specifikací IEEE 802.11
802.11n	2008?	zvýšení datové propustnosti WLAN (minimálně 100 Mbit/s)
802.11p	2008?	bezdrátový přístup z pohybujících se dopravních prostředků
802.11r	2007?	rychlý a bezpečný handover mezi přístupovými body v rámci ESS
802.11s	2008?	podpora smyčkové topologie (Mesh) s autokonfigurací
802.11T	2009?	metody a metriky pro měření výkonnosti
802.11u	2008?	podpora pro spolupráci WLAN s externími sítěmi
802.11v	2008?	jednotné rozhraní pro management síťových zařízení
802.11w	2008?	zabezpečení přenosu management rámců
802.11y	2008?	možnost využití pásma 3.65 - 3.70 GHz v USA

[2] na této frekvenci operují i jiná zařízení, jde např. o mobilní telefony, Bluetooth, nebo mikrovlnné trouby
[3] zatímco doplňky se označují malými písmeny, doporučení lze rozeznat podle velkých písmen
[4] `http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm` (05/2007)

3.2 Požadavky na zabezpečení WLAN

Bezpečnostní cíle (*Security Goals*), nebo také ***bezpečnostní služby*** (*Security Services*), vyjadřují požadavky na zabezpečení WLAN, mezi které patří:

- ***Důvěrnost*** (*Confidentiality*) - ochrana proti neautorizovanému odhalení informace. Ve WLAN jsou předmětem zajištění důvěrnosti informace uložené v síťových uzlech a bezdrátově přenášená data. ***Anonymita*** (*Anonymity*) pak představuje samostatný bezpečnostní cíl, mluvíme-li o důvěrnosti osob. Anonymita je však v přímém rozporu s některými jinými bezpečnostními cíli (viz dále autentizace a nepopiratelnost).
- ***Integrita*** (*Integrity*) - ochrana proti neoprávněné modifikaci informace. Ve WLAN jde stejně jako v případě důvěrnosti o integritu přenosu dat a integritu informací uložených v uzlech bezdrátové sítě. V případě technického vybavení je odpovídajícím pojmem *fyzická integrita*.
- ***Dostupnost*** (*Availability*) - ochrana vůči neoprávněnému odepření přístupu k datům nebo službám, které WLAN poskytuje autorizovaným uživatelům.
- ***Autentizace*** (*Authentication*) - ověření identity zařízení/uživatelů WLAN.
- ***Autorizace a řízení přístupu*** (*Authorization and Access Control*) - mechanismy, které autentizovaným zařízením/uživatelům umožňují přístup do WLAN a využívání jejích prostředků na základě jim přidělených práv.
- ***Nepopiratelnost*** (*Nonrepudiation*) - neodmítnutelnost odpovědnosti za odeslání či přijetí zprávy. Entita by však měla být identifikovatelná a zodpovědná za všechny akce prováděné v rámci WLAN na základě monitorování veškerých jejích aktivit. V této souvislosti se pak lze setkat s pojmem ***účtovatelnost*** (*Accountability*).

Uvedené bezpečnostní cíle jsou obecně platné i pro jiné typy bezdrátových sítí. Vysvětlené pojmy proto budou používány bez explicitní definice i v rámci navazujících kapitol práce.

3.3 Hrozby a zranitelná místa WLAN

Zranitelným místem je chyba nebo slabina v návrhu, implementaci či provozu WLAN, jež může být využita pro narušení bezpečnosti bezdrátové sítě. *Hrozby* jsou pak takové vlastnosti prostředí (okolnosti), které využívají zranitelných míst WLAN a mají potenciál způsobit bezpečnostní incident a ohrozit tak některý z jejích bezpečnostních cílů.

Nejzranitelnějším místem WLAN, kde může dojít k narušení důvěrnosti a integrity dat, jsou (narozdíl od metalických a optických spojů) bezdrátové linky. To platí zejména při komunikaci STA a AP, zranitelným místem může být ale i distribuční systém, zejména pokud je implementován taktéž bezdrátovou technologií. Dostupnost může být narušena jak v uzlech, tak i na komunikačních linkách. Ostatní bezpečnostní služby pak napadením přístupového bodu, popř. dalších prvků, které zajišťují přístup do sítě a její audit.

3.4 Útoky na WLAN

Cílem *útočníků*, představujících hrozby, jsou *aktiva* WLAN. Mezi aktiva patří *data* (včetně přístupových hesel, kryptografických klíčů apod.), poskytované *služby*, *zařízení* a *uživatelé* WLAN z hlediska svého majetku a identity.

3.4.1 Přípravná fáze útoku - mapování nezabezpečených WLAN

Přípravnou fází útočníků bývá typicky vyhledávání existujících sítí a zjišťování úrovně jejich zabezpečení. Podle způsobu, jakým se narušitelé ve fyzickém terénu pohybují, tyto aktivity nesou názvy *WarWalking*, *WarDriving* či *WarFlying*. Značení nalezených WLAN v dané lokalitě speciálními symboly se pak označuje jako *WarChalking* [14]. Informace se však často objevují i na Internetu v podobě celých map nezabezpečených WLAN.

3.4.2 Základní typy útoků na WLAN

Následující přehled popisuje základní *typy útoků na WLAN* [12, 13, 15]. Ty se však ve většině případů principiálně týkají i ostatních bezdrátových rádiových sítí, příp. i komunikačních sítí obecně. Útoky zcela specifické pro WLAN IEEE 802.11 budou uvedeny v textu později současně s výkladem jednotlivých bezpečnostních mechanismů.

Pasivní útoky

Jako *pasivní útok* se označuje neautorizovaný přístup k WLAN, který ponechává její stav zcela neměnný, tzn. nenarušuje v jakémkoliv ohledu integritu bezdrátové sítě.

- ***Odposlouchávání*** (*Eavesdropping*) WLAN umožňuje snadno zachytitelný nosný rádiový signál při komunikaci dvou stanic (u Ad-Hoc sítí) nebo při přenosu dat mezi stanicí a přístupovým bodem. Cílem útočníka je obsah přenášených informací, jejichž *důvěrnost* je tímto narušena.
- ***Analýza provozu*** (*Traffic Analysis*) je sofistikovanější technikou odposlechu, kdy narušitel dodatečně analyzuje zachycená dat za účelem dedukce nových poznatků ze vzorů nalezených v komunikaci. Tímto způsobem je možné získat např. informace o existenci jednotlivých prvků WLAN (např. detekce přístupových bodů), aktivitách v ní probíhajících (např. aktivity uživatelů), použitých komunikačních protokolech apod. Přestože jde o pasivní útok, jenž sám o sobě narušuje pouze *důvěrnost*, bývá základem aktivních útoků i na jiné bezpečnostní cíle.

Aktivní útoky

Aktivní útoky jsou charakteristické tím, že vždy určitým způsobem narušují datovou nebo fyzickou integritu WLAN bez ohledu na skutečný motiv činu.

- ***Modifikace provozu*** (*Traffic Modification*) představuje přímý útok na *integritu*, při kterém neautorizovaná entita pozmění, přidá či odstraní v průběhu bezdrátové komunikace legitimní zprávu, příp. zasáhne do pořadí přenášených dat.
- ***Útok opakovaným přenosem*** (*Replay*) je založen na pasivním odposlechu, který doprovází ukládání uskutečněné komunikace ve WLAN za účelem opětovného vysílání zaznamenaných dat směrem k příjemci. Jako příklad lze uvést zachycení datového toku při přístupu autorizovaného uživatele k WLAN. Přestože mohou být zprávy šifrované a útočník ani nemusí znát jejich obsah (včetně přístupových klíčů a hesel), zopakování takového přenosu často postačuje k neautorizovanému proniknutí do sítě. Útok tohoto typu ale může uspět pouze tehdy, pokud nejsou implementovány účinné mechanismy pro ověření *aktuálnosti* zpráv (časová razítka, náhodná čísla aj.). Vždy narušuje *integritu* provozu, podle povahy a cíle útoku i další bezpečnostní cíle.

- ***Neautorizovaný přístup*** (*Unauthorised Access*) bývá typicky prováděn za účelem útoku proti celé WLAN, nikoli vůči konkrétním uživatelům. Zahrnuje jak neoprávněné využívání prostředků a služeb bezdrátové sítě, tak i neautorizovaný fyzický přístup k jejím technickým komponentám - v tomto případě může být následkem fyzického útoku i narušení *dostupnosti*. Velmi silně ohrožuje i ostatní bezpečnostní služby, tzn. *integritu*, *autentizaci*, *autorizaci* a *řízení přístupu* a *nepopiratelnost* (*účtovatelnost*). Narušení *důvěrnosti* závisí na tom, zda se útočník při svém přístupu k sítí dostane k utajovaným informacím. Proniknutí do WLAN obvykle probíhá na základě získání pro přístup nezbytných informací a hesel (*slovníkový útok*, *útok hrubou silou*), krádeže identity (viz dále) či narušením fyzických bezpečnostních opatření.

- ***Krádež identity*** (*Masquerade*) může umožnit neautorizované osobě (resp. zařízení) vystupovat jako legitimní uživatel (resp. síťový uzel) dané WLAN. Typickým případem WLAN je *krádež MAC adresy* (*MAC Spoofing*) na základě odposlechu nezabezpečené komunikace mezi STA a AP. Zjištěnou MAC adresu může útočník vnutit své klientské kartě a požadovat služby nárokované oprávněným účastníkem, za nějž se vydává. Stejně nebezpečné ale mohou být naopak *falešené AP* (*Rogue AP*). První případ představují neautorizované přístupové body, které jsou sice připojeny k WLAN (často přímo neznalými zaměstnanci), avšak narozdíl od ostatních komponent bez patřičného zabezpečení a vědomí síťového administrátora. Přítomnost těchto AP představuje vážnou bezpečnostní hrozbu, neboť vytvářejí nebezpečná zadní vrátka, které může narušitel využít pro provedení útoku na WLAN. Druhým případem je útočníkem zřízený falešný přístupový bod, jenž ale není skutečnou součástí dané sítě a má za cíl přimět nevědomého uživatele k připojení s následným získáním citlivých informací. Krádež identity je aktem, který už z titulu aktivního útoku narušuje *integritu*, velice silně pak *nepopiratelnost* (*účtovatelnost*) a *autorizační* a *autentizační* mechanismy. *Důvěrnost* je pak ohrožena v případě, že útočník díky odcizené identitě získá přístup k informacím legitimního uživatele, za kterého se vydává, příp. i k jiných utajovaným skutečnostem (např. data dalších uživatelů).

- ***Odmítnutí služby*** (*DoS*, *Denial of Service*) je zvláštním typem útoku v tom smyslu, že se nezaměřuje na získání přístupu do WLAN či odhalení informací, nýbrž na znepřístupnění určité služby, systému, příp. i celé sítě tak, aby byla výrazně ztížena nebo úplně znemožněna práce uživatele. Existuje několik odlišných *typů DoS útoků*, které lze provádět na různých síťových vrstvách [16]. Velmi specifické pro WLAN a bezdrátové rádiové sítě obecně jsou DoS útoky na fyzické vrstvě. Jedná se o tzv. *jamming*, neboli záměrné rušení rádiového signálu. Co se týče spojové vrstvy, tak zde mají DoS útoky podobu odmítnutí přístupu ke sdílenému médiu (např. lze využít chybného zacházení AP s diverzitními anténami k zabránění přístupu již připojených klientů). WLAN jsou obecně na DoS útoky velmi náchylné a účinná obrana proti nim není často vůbec jednoduchá, přičemž nejvíce se to týká právě linkové a fyzické vrstvy, kde účinná protiopatření prakticky neexistují. DoS útoky na vyšších vrstvách nejsou z pohledu WLAN zajímavé, poněvadž se zde od klasických počítačových sítí výrazně neliší. Jedná se např. o zahlcení sítě velkými datovými objemy, útoky nazývané jako *Ping of Death* a *ICMP floods* (síťová vrstva). Pro transportní vrstvu jsou typické DoS útoky opakovaným zasíláním požadavků na spojení (*SYN floods*). Mezi nejúčinnější útoky na dostupnost patří *distribuované DoS útoky* (*DDos*, *Distributed DoS*), které přicházejí z mnoha různých uzlů v síti. Neméně ničivou formu DoS útoků představují úmyslná fyzická poškození technického vybavení WLAN.

- ***Útok ze středu*** (*MITM*, *Man-In-The-Middle*) může mít několik podob, v principu jde však vždy o akt, kdy se mezi dvě komunikující strany (ve WLAN typicky mezi STA a AP) vloží třetí entita, která se vydává za jednoho z regulérních partnerů v probíhající konverzaci. Útočník tak může odposlouchávat, vkládat a modifikovat přenášené zprávy, aniž by si toho byl některý z poškozených vědom, a narušuje tak *důvěrnost* a *integritu* přenosu dat, *autenticitu* zpráv a jejich *nepopiratelnost*. Přesměrování provozu na útočníka se označuje jako *únos relace* (*Session Hijacking*). U WLAN je možné se dostat do role falešného prostředníka na základě zjištění MAC adres klientské stanice a přístupového bodu z odposlechnuté komunikace. Následně útočník spojení přeruší a zfalšuje svoje MAC adresy. Vůči AP pak vystupuje jako autorizovaný klient, STA ho naopak považuje za legitimní přístupový bod. Součástí MITM útoků bývá útok na ARP (*ARP Poisoning*) a DNS systém (*DNS Spoofing*).

3.5 Bezpečnostní mechanismy WLAN

V případě WLAN IEEE 802.11 je nutné rozlišovat specifické *bezpečnostní mechanismy* definované normou a jejími doplňky, které se týkají výhradně *fyzické* a *linkové* vrstvy, a bezpečnostní opatření implementovaná na *vyšších vrstvách* síťové architektury - ty mají naopak daleko univerzálnější charakter a běžně se používají i v jiných počítačových sítí. Bezpečnostní mechanismy specifikované standardem IEEE 802.11, které jsou nabízeny jako jeho volitelná součást, se navíc zaměřují pouze na *důvěrnost*, *integritu* a *autentizaci*. Přitom jen některé z nich ale poskytují všechny uvedené bezpečnostní služby současně. Naplnění ostatních bezpečnostních cílů je možné pomocí protokolů vyšších vrstev.

3.5.1 Vývoj podpory zabezpečení WLAN

Následující přehled zmiňuje nejdůležitější milníky v oblasti zabezpečení WLAN a uvádí ***bezpečnostní mechanismy vycházející z normy IEEE 802.11 a jejích doplňků***:

- ***1997*** - původní normou IEEE 802.11 definovaný protokol ***WEP*** (šifra ***RC4***), jenž měl poskytovat zabezpečení na úrovni klasických (drátových) sítí, ve skutečnosti však zajišťoval jen slabou *autentizaci*, *důvěrnost* a *integritu* dat;
- ***2001*** - zdokonalená *autentizace* a *management klíčů* podle rámce ***IEEE 802.1X*** (doplněk normy IEEE 802.1, nikoli IEEE 802.11), pro zajištění *důvěrnosti* a *integrity* dat stále jen WEP, který byl v uvedeném roce automatickými nástroji prolomen;
- ***2003*** - ***WPA*** jako dočasné řešení sdružení *Wi-Fi Alliance*, jehož cílem bylo nahradit WEP před uvedením specifikace IEEE 802.11i, ze které v předstihu převzalo některé bezpečnostní prvky - nově ***TKIP*** (šifra ***RC4***) pro *důvěrnost* a *integritu* dat, zůstává *IEEE 802.1X* pro *autentizaci* a *management klíčů*;
- ***2004*** - velmi vysoká úroveň komplexního zabezpečení jako doplněk ***IEEE 802.11i*** (***WPA2***), protokol ***CCMP*** s *šifrováním* ***AES*** pro zajištění *důvěrnosti*, *integrity* a *autentičnosti* přenášených dat, *autentizace* a *management klíčů* podle *IEEE 802.1X*;
- ***2007*** - v druhé polovině tohoto roku se očekává dokončení doplňku ***802.11r***, jenž má zajistit *rychlý a bezpečný handover* (motivací je bezdrátová IP telefonie);
- ***2008*** - předpokládaný rok schválení doplňku ***802.11w***, jehož vývoj probíhá od roku 2005 a má za cíl zavést podporu pro *zabezpečení managementu rámců*.

Navíc se současně vyvíjela i podpora zabezpečení na vyšších vrstvách síťové architektury a taktéž *fyzická*, *personální* a *administrativní* bezpečnostní opatření, která mají zejména v případě rozsáhlých sítí a větších organizací nezanedbatelný význam. Jejich výklad ale přesahuje rámec této práce a nebude jim proto ve větší míře věnována pozornost. Souběžně s tím pak procházela vývojem i nabídka komerčních řešení a služeb. Při takto komplexním pohledu na problematiku bezpečnosti lze rozlišovat několik *generací* úrovně zabezpečení WLAN IEEE 802.11 (celkem čtyři až do současnosti) [17]. V současnosti jsou k dispozici již dostatečně silná bezpečnostní opatření, která při správné kombinaci a implementaci umožňují nasazení IEEE 802.11 i v prostředích s vysokými bezpečnostními požadavky.

Bezpečnostním mechanismům je věnován celý zbytek této kapitoly. Největší pozornost je věnována zabezpečení na vrstvách fyzické a linkové (viz části 3.6 a 3.7), poněvadž právě na této úrovni se jednotlivé bezdrátové standardy vzájemně odlišují, což platí i při jejich porovnání s jinými počítačovými sítěmi. Velký význam pro zabezpečení WLAN mají ale i protokoly vyšších vrstev, proto i jim bude do určité míry věnován prostor (viz část 3.8). Závěr kapitoly nastiňuje další vývoj v oblasti zabezpečení bezdrátových lokálních sítí a zmiňuje i některé méně tradiční způsoby zabezpečení WLAN (viz část 3.9).

3.6 Zabezpečení WLAN na fyzické vrstvě

Při zajišťování bezpečnosti WLAN na úrovni fyzické vrstvy má zásadní význam správný výběr technických komponent (antény, kabely, konektory, přístupové body, ...), regulace šíření rádiového signálu a v rámci normy IEEE 802.11 specifikované techniky bezdrátového přenosu dat (frekvenční pásma, metody rozprostřeného spektra, modulační schémata, ...).

3.6.1 Antény a regulace šíření rádiového signálu

Má-li být zajištěna co nejvyšší bezpečnost WLAN, je nutné provést vhodný výběr, umístění a orientaci *antén* pro co možná nejpreciznější vertikální i horizontalní vymezení dosahu bezdrátové sítě. Základní pravidlo spočívá v používání *směrových* a nikoliv všesměrových antén. Vhodné je též snížit *vyzařovaný výkon* přístupového bodu na nejnižší přijatelnou hodnotu, jež dostačuje pro spolehlivou obsluhu všech klientů, ale zároveň minimalizuje další šíření signálu nežádoucím směrem. Identifikaci jiných signálů a zaznamenávání rušení s vazbou na místo umožňují speciální *nástroje pro analýzu spektra*.

Kromě bezpečnostních opatření, které se týkají rádiových přijímačů/vysílačů, lze šíření signálu dále regulovat *fyzickými překážkami*. To se týká především WLAN provozovaných ve vnitřních prostorách, kde je nutné zvažovat použití speciálních stavebních materiálů, nátěrů zdí a stropů, izolace oken fóliemi a metalickými zástěnami apod.

Kabely a konektory

Ztráty signálu na kabelu mezi bezdrátovým zařízením a anténou mohou značně degradovat její *zisk*. Tomu lze čelit výběrem co možná nejkratších a nejkvalitnějších *kabelů* s nízkými hodnotami *útlumu*, dodržováním tzv. minimálních *poloměrů ohybu* a nasazením *rádiových zesilovačů*. Ztráty a útlumy vznikají také u *konektorů* při přechodu signálu z kabelu na konektor. Přestože to nemusí být zcela zřejmé, volba konektorů a kabelů má nezanedbatelný vliv i na úroveň zabezpečení. Důležitou roli zde hraje citlivost přijímače a síla signálu, kdy jeho výrazné ztráty způsobené nevhodnými kabely a konektory mohou znatelně usnadnit *DoS* útoky na fyzické vrstvě, tzn. *jamming*.

3.6.2 Rozprostřené spektrum a modulace

Určitou obranu vůči *odposlechu* a *jammingu* představují techniky *rozprostřeného spektra*, které jsou založeny na myšlence vysílání signálu pomocí širšího frekvenčního pásma, než je nezbytně nutné. Fyzická vrstva WLAN IEEE 802.11 (viz část 3.1.3) implementuje typy *FHSS* (*Frequency Hopping Spread Spectrum*) a *DSSS* (*Direct Sequence Spread Spectrum*).

V případě *FHSS* je kmitočtové pásmo rozděleno na několik kanálů a vysílání probíhá na těchto pseudnáhodně se měnících frekvencích podle stanoveného schématu *skoků*, které je známé oběma komunikujícím stranám. Technika *DSSS* každý informační bit moduluje (operace *XOR*) jistým kódem, tzv. *PN sekvencí* (*PN Sequence*), nebo také *čipovací sekvencí* (*Chipping Sequence*). Původní data jsou tak nahrazena pseudonáhodnou posloupností bitů.

Pro potencionálního útočníka je klíčová znalost posloupnosti frekvenčních proskoků u FHSS a čipovací sekvence pro typ DSSS. V obou případech je nutné znát i použité *frekvenční pásmo* a metodu *modulace*. Všechny parametry jsou ale specifikovány normou IEEE 802.11 a tím i veřejně přístupné. Při jejich znalosti lze zkonstruovat rádiový přijímač za účelem odposlechu, pokud přenášená informaci není dále chráněna jiným způsobem. Proto tedy rozprostřené spektrum nepředstavuje u WLAN IEEE 802.11 skutečnou ochranu proti odposlechu na fyzické vrstvě.

Obě metody rozprostřeného spektra jsou však účinné vůči *úzkopásmovému jammingu*. DSSS dokáže informace poškozené rušením opravit na základě zabudovaných statistických algoritmů (rozhodující je délka čipovací sekvence). V případě FHSS dojde k zasažení jen malé části dat v zarušeném dílčím kanále a informace může být opakovaně přenesena v následujícím skoku na jiném kmitočtu, který není úzkopásmovým rušením postižen.

3.6.3 Fyzická vrstva založená na infračervené technologii

Jako alternativa k rádiové technologii a technikám rozprostřeného spektra byla v původní normě z roku 1997 možnost přenosu dat *infračerveným světlem* (*IR*, *Infrared*) [10, 18]. IR technologie pracují na vysokých kmitočtech, které v rámci elektromagnetického spektra předcházejí pásmu viditelného světla. Přestože infračervená technologie vzhledem k nízkým přenosovým rychlostem (1 až 2 Mbit/s) a malému dosahu (cca 10 až 20 metrů) nalezla uplatnění jen v několika málo komerčních produktech, je zajímavá z pohledu bezpečnosti.

Prvním zásadním rozdílem oproti rádiovému signálu je *neproniknutelnost* infračerveného paprsku skrz pevné neprůhledné *překážky* a tedy daleko snazší stínění a zabránění jeho šíření do nežádoucích oblastí. Velmi dobrá je také *odolnost proti šumu*. Útočník by se navíc i vzhledem ke krátkému dosahu IR technologie musel pohybovat v bezprostřední blízkosti komunikujícího zařízení. I přesto může použití infračerveného signálu pro přenos dat v otevřeném prostředí představovat bezpečnostní rizika v podobě možného *odposlechu* a *jammingu* (IR paprsek lze ovlivnit jinými zdroji tepla a světla). Proto se IR systémy (mimo běžných produktů spotřební elektroniky) používají spíše v uzavřených prostorách pro aplikace s vysokými požadavky na bezpečnost.

3.7 Zabezpečení WLAN na linkové vrstvě

Spojová vrstva má pro zabezpečení WLAN i bezdrátových sítí obecně zásadní význam. Norma IEEE 802.11 na této vrstvě implementuje důležité *autentizační protokoly* a *šifrovací mechanismy* pro zajištění *důvěrnosti* a *integrity* dat. Bezpečnostní mechanismy vycházející z normy pak posiluje několik externích opatření, které mají doplňkový charakter.

3.7.1 SSID

Identifikátor WLAN, *SSID*, odlišuje jednotlivé logické bezdrátové sítě. Jde o základní bezpečnostní mechanismus specifikovaný normou IEEE 802.11, jenž má plnit roli jednoduché *autentizace*, neboť SSID je vyžadováno od klienta ve fázi asociace k WLAN a současně zamezuje i nechtěnému připojení k jinému AP. Přestože SSID není skutečným heslem, vyžaduje si pro dosažení vyšší bezpečnosti stejné zacházení.

SSID vysílá přístupový bod implicitně v pravidelných intervalech (obvykle po 100 ms) jako součást *Beacon* rámců, což je z bezpečnostního hlediska problematické, obzvláště pokud je nastaveno na implicitní hodnotu z výroby, kdy útočník může snadno nalézt a napadnout WLAN. Proto častým doporučením bývá *Beacon* rámce s tímto identifikátorem vůbec *nevysílat*, tzn. přejít do režimu *aktivního skenování*, kdy stanice sama při znalosti SSID iniciuje přidružení rámcem *Probe Request*. Tato volba ale není definována normou a ne všechny technologie ji musí nutně podporovat. Navíc lze takovéto opatření obejít vysláním podvrženého *disasociačního rámce* (*Disassociate*), který donutí autorizovaného aktivního klienta k odpojení od WLAN. Při následné opakované asociaci stanice pak útočník může SSID odposlechnout, jelikož se SSID v otevřené podobě vysílá v rámcích *Probe Request*, *Association Request*, *Reassociation Request* a *Probe Response*.

VLAN

Další možnost zvýšení úrovně zabezpečení WLAN spočívá v budování *virtuálních lokálních sítí* (*VLAN*, *Virtual LAN*), které představují nezávislé *logické sítě* v rámci jedné fyzické sítě. Pomocí VLAN je možné oddělovat logické segmenty WLAN, mezi kterými by neměla v sítí probíhat vzájemná výměna dat. Lze např. separovat administrativní a uživatelský provoz, jednotlivé skupiny uživatelů mohou pracovat jako samostatné VLAN. SSID zde hraje roli při diferenciaci uživatelských skupin, kdy přístupový bod musí mapovat (staticky nebo dynamicky pomocí protokolu RADIUS, viz část 3.8.2) jednotlivé VLAN na SSID bezdrátové sítě. Nejpoužívanějším standardem pro VLAN je *IEEE 802.1Q* [19].

3.7.2 ESSID

Jiná *autentizační technika* je založena na identifikátoru *ESSID*, jehož hodnota je do každého AP naprogramována a určuje (pod)síť, ve které se daný přístupový bod nachází. Bez jeho znalosti (ESSID se nevysílá) není umožněna stanicím asociace k WLAN.

3.7.3 Filtrování MAC adres

Filtrování MAC adres je založeno na *přístupovém seznamu* (*ACL*, *Access Control List*) MAC adres síťových zařízení autorizovaných uživatelů dané WLAN. Má za cíl posílení *autentizace* a zabránění *neautorizovaného přístupu* do bezdrátové sítě. ACL bývají uloženy v přístupových bodech, kde lze kromě samotného filtrování často omezit i dobu připojení a šířku pásma přidělenou konkrétnímu klientovi. Problémem tohoto bezpečnostního opatření je však jeho potencionální zneužitelnost pro provádění útoků *krádeží identity*, kdy narušitel zjistí MAC adresu legitimního uživatele (typicky na základě odposlechu komunikace), vnutí ji svému zařízení (lze softwarově), získá neoprávněný přístup do WLAN a současně zabrání autorizovanému uživateli ve využívání služeb sítě. Mohou tak být následně narušeny všechny bezpečnostní služby WLAN. Implementace filtrování MAC adres se v sítích s větším počtem uživatelů i vzhledem k administrativní náročnosti spíše *nedoporučuje*.

3.7.4 WEP

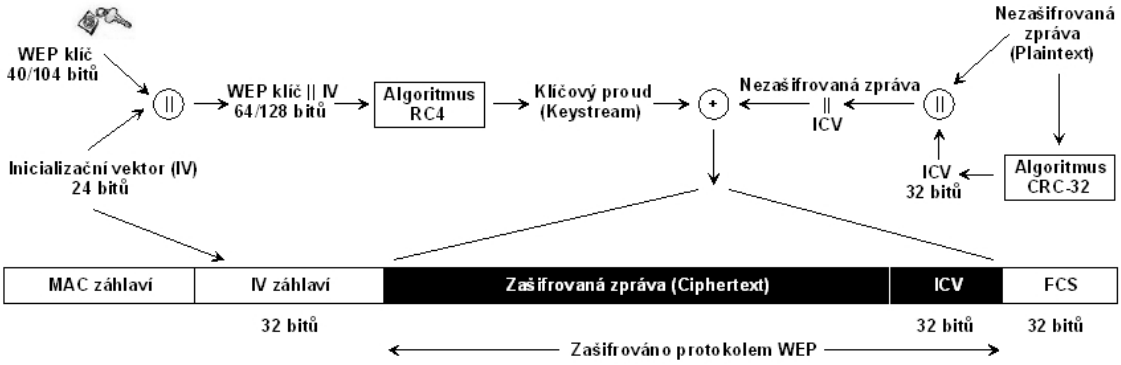
Protokol *WEP* (*Wired Equivalent Privacy*) definuje původní norma IEEE 802.11-1997 jako volitelný bezpečnostní doplněk pro zajištění *důvěrnosti* a *integrity* dat a řízení přístupu do WLAN na základě *autentizace*. Již z názvu protokolu WEP lze rozpoznat, jaký měl původní cíl, tj. zabezpečení na úrovni klasických LAN, který ale ve výsledku nesplnil.

Šifrování - důvěrnost a integrita dat

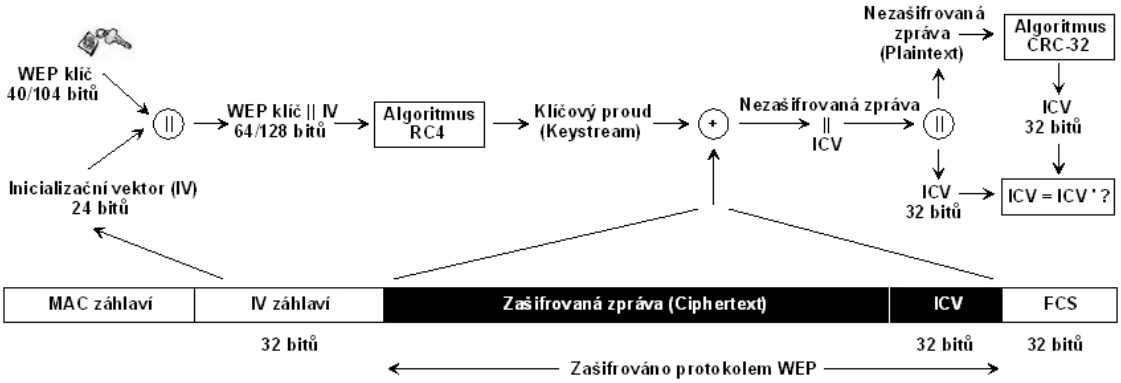
WEP využívá symetrickou proudovou šifru *RC4* (*Ron's Code No. 4*) v synchronním režimu, jež byla zvolena pro svou implementační jednoduchost a výpočetní nenáročnost. Šifrování se vždy provádí pomocí 24-bitového *inicializačního vektoru* (*IV*, *Initialization Vector*) a 40-bitového/104-bitového vlastního *sdíleného klíče* (*Shared Key*, nebo také *WEP Key*). Velikost výsledného šifrovacího klíče je buď 64, nebo 128 bitů. Norma přitom nedefinuje mechanismus managementu WEP klíčů. Sdílený klíč tak bývá v praktickém provozu typicky statický a jeho konfigurace se obvykle provádí manuálně u každého zařízení. Navíc často všechny stanice používají jeden a ten samý klíč pro šifrování veškeré komunikace ve WLAN. Účelem inicializačních vektorů je pak zmírnit statičnost WEP klíče. Norma ale ani v tomto případě nedefinuje způsob jejich generování a obnovy.

Samotný proces *WEP šifrování* (viz obr. 3.2) probíhá v několika krocích. Z *nezašifrované zprávy* (*Plaintext*) je spočten *kontrolní součet* (*ICV*, *Integrity Check Value*), který se k ní připojí. Následně *konkatenace WEP klíče a IV* vstupuje do algoritmu *RC4*, jenž slouží jako *generátor pseudonáhodných čísel* (*PRNG*, *Pseudo Random Number Generator*). Výstupem je pseudonáhodný *klíčový proud* (*Keystream*). Aplikací operace *XOR* na *původní zprávu s připojeným ICV* a *klíčový proud* pak vznikne výsledná *zašifrovaná zpráva* (*Ciphertext*). Před zašifrovanou zprávu je předřazen IV v otevřené podobě a celý rámec se následně zapouzdří. Z 32-bitového *IV záhlaví* tvoří 24 bitů samotný IV, 2 bity (*KeyID*) pak příjemci indikují, který ze čtyř možných sdílených klíčů byl použit. Zbývající bity představují výplň.

Vzhledem k použití symetrické kryptografie se *WEP dešifrování* (viz obr. 3.3) řídí stejným algoritmem jako šifrování. Adresát použije vlastní kopii WEP klíče a IV z příchozího rámce. Na straně příjemce je navíc provedeno *ověření integrity* přenesených dat porovnáním ve zprávě uvedeného *ICV* a explicitně vypočteného kontrolního součtu. Na základě shody (resp. neshody) je přijaté zpráva přijata (resp. odmítnuta). Nejde ale o kryptografické ověření integrity, poněvadž WEP implementuje ICV jako lineární kód *CRC-32*, který je do jisté míry dostatečně účinný jen vůči neúmyslným chybám.



Obrázek 3.2: WEP - šifrování (operace XOR značena jako +, konkatenace symbolem ||)



Obrázek 3.3: WEP - dešifrování (operace XOR značena jako +, konkatenace symbolem ||)

Autentizace

Protokol WEP implicitně poskytuje pouze *jednostrannou autentizaci*. V normě IEEE 802.11 jsou za tímto účelem definovány dvě metody:

- ***Otevřená autentizace*** (*Open System Authentication*) probíhá ve dvou krocích. Stanice vyšle rámec s *autentizačním požadavkem* (*Authentication Request*), ve kterém uvede svoje identifikační údaje. Příjemce tuto informaci vyhodnotí a jako součást rámce s *odpovědí* (*Authentication Response*) uvede *stavový kód* (*Status Code*), který indikuje výsledek autentizace. Přestože stanice rozhodující o úspěchu autentizace získá informaci o identitě autentizujícího se klienta, nemá vůbec žádnou možnost, jak ji ověřit. Otevřená autentizace z uvedeného důvodu bývá proto často označována jako *nulová autentizace* (*Null Authentication*). Otevřenou autentizaci lze provádět nezávisle na použití WEP šifrování (tzn. není vyžadováno od komunikujících stran vlastnictví WEP klíče).
- ***Autentizace sdíleným klíčem*** (*Shared Key Authentication*) se řídí protokolem *výzva-odpověď* (*Challenge-Response*) a předpokládá znalost a korektní použití WEP klíče u žadatele i ověřovatele. Stanice A odešle stanici B *požadavek na autentizaci* (*Authentication Request*) se svými identifikačními údaji. Stanice B odpoví rámcem s náhodně vygenerovanou zprávou, tzv. *výzvou* (*Challenge Text*). Stanice A tuto výzvu *zašifruje* vlastním WEP klíčem a odešle ji zpět jako *odpověď* (*Challenge Response*). Stanice B následně přijatou zprávu *dešifruje*, porovná ji s původně vyslanou výzvou a rozhodne, zda stanice A skutečně zná či nezná WEP klíč a bude nebo nebude úspěšně autentizována. Výsledek žadatel obdrží v posledním rámci (*Authentication Response*).

Která z uvedených možností se v daném případě použije, uvádí autentizující se stanice vždy v prvním rámci (*Authentication Request*). Návrh je pak druhou stranou buď přijat, nebo zamítnut. Implicitní volbou je přitom otevřená autentizace.

Zranitelná místa a publikované útoky na WEP

Protokol WEP je velmi známým díky velkému množství nedostatků a zranitelných míst, které v závěru této části shrnuje tab. 3.2. Za hlavní příčinu těchto slabin se považuje skutečnost, že protokol WEP nebyl vyvíjen skutečnými odborníky na kryptografii.

V následujícím přehledu jsou v chronologické posloupnosti předloženy ty nejvýznamnější ***publikované nedostatky a útoky na WEP***:

- ***Září 2000 - Jesse R. Walker*** jako první poukázal na problémy WEP v publikaci "***Unsafe at any key size; An Analysis of the WEP encapsulation***" [20]. V práci vyvrací domněnku o největší slabině WEP v podobě krátkého 40-bitového sdíleného klíče a naopak ukazuje, že *nejzávažnějším problémem je 24-bitový IV bez ohledu na velikost tajného klíče*. Dle Walkera je kromě nedostatečné délky IV problém i v *absenci standardem definovaného algoritmu pro správu IV*, tzn. určitý uzel WLAN může aplikovat IV již použitý jiným zařízením, což zvyšuje pravděpodobnost *kolize inicializačních vektorů* (*IV Collision*). Ukázal, že s 50% pravděpodobností nastane IV kolize už po 4823 (2^{12}) rámcích, na 99% pak po 12 430 rámcích. Walker navrhl několik zdokonalení (např. 128-bitový IV), ty ale nebyly ve své době implementovány.

- ***Leden 2001*** - autoři ***Borisov***, ***Goldberg*** a ***Wagner*** plublikovali článek s názvem "***Intercepting Mobile Communications: The Insecurity of 802.11***" [21], jež pojednává o možnostech pasivních i aktivních útoků na WEP. Za největší nedostatky protokolu WEP označuje *malý stavový prostor 24-bitových inicializačních vektorů* a *statičnost WEP klíče*, kdy při průměrné velikosti rámce 1500 bytů a přenosové rychlosti 11 Mbit/s dojde k opakování IV, tzn. *IV kolizi*, nejpozději po 18 302 vteřinách, což odpovídá přibližně pěti hodinám provozu. Autoři pak upozorňují na potencionálně proveditelné útoky při úspěšném odposlechu paketů zašifrovaných stejným klíčovým proudem. Útočníkovi je tímto umožněno nejen *odhalení obsahu zašifrovaného paketu* (aplikace operace XOR na oba pakety, lze díky předvídatelnosti provozu - statická pole v IP hlavičce), ale i *modifikace provozu* (integrita zajištěna pomocí CRC-32), *přesměrování dešifrovaného provozu do alternativního síťového uzlu* (útočník ve zprávě změní IP adresu, na kterou ji po dešifrování odešle AP) či *dešifrování veškerého přenosu dat* na základě *slovníku* (cca 15 GB) sestaveného ze všech inicializačních vektorů a odpovídajících klíčových proudů.

- ***Červenec 2001*** - prezentace "***An Inductive Chosen Plaintext Attack against WEP/WEP2***" [22], kde ***Arbaugh*** ukazuje útok na WEP *nezávisle na délce IV*.

- ***Srpen 2001*** - "***Weaknesses in the Key Scheduling Algorithm of RC4***" [23] jako publikace pánů se jmény ***Fluhrer***, ***Mantin*** a ***Shamir***. Autoři v práci popisují způsob, jak lze při odchycení přibližně 4 miliónů paketů zcela *odkrýt šifrovací klíč*. Útok, nazývaný ***FMS*** podle počátečních písmen svých tvůrců, je založen na dvou zásadních slabinách algoritmu *KSA* (*Key Scheduling Algorithm*), jenž využívá šifra RC4 pro generování tabulky klíčů. Prvním nedostatkem je, že KSA produkuje velké množství *slabých klíčů*, kdy malá část tajného klíče určuje značnou část počátečního výstupu KSA. Příčina druhé spočívá v *konkatenaci WEP klíče a IV*, kdy tajný klíč může být snadno odvozen z klíčového proudu použitého s několika různými IV. IV se navíc přenáší nezašifrovaný a několik prvních bytů zašifrovaných dat je také předvídatelných - jde o *SNAP* (*SubNetwork Access Protocol*) hlavičku. V srpnu 2001 byly uvolněny i *SW nástroje* ***AirSnort*** a ***WEPCrack*** pro odhalení WEP klíče.

- ***Únor 2002 - David Hulton*** představil ***optimalizovaný FMS útok*** v publikaci "***Practical Exploitation of RC4 Weaknesses in WEP Environments***" [24]. Nový útok *bere v úvahu více výstupních bytů šifry RC4* a redukuje tak potřebný objem dat pro následnou analýzu (postačuje přibližně 0.5 miliónu paketů).

Tabulka 3.2: Klady (+) a zápory (-) protokolu WEP

+ jednoduchý a výpočetně nenáročný bezpečnostní mechanismus podporovaný normou
+ ochrana proti nezkušeným útočníkům a neúmyslnému narušení WLAN
- nevhodné použití šifry RC4 v prostředí WLAN (v šifře samotné hlavní problém není)
- RC4 klíč vzniká konkatenací WEP klíče a IV, tři byty klíče jsou tak vždy známy
- chybí specifikace mananagementu WEP klíčů, problém s jejich distribucí a obnovou
- typicky jeden WEP klíč pro autentizaci i šifrování veškerého přenosu dat ve WLAN
- norma nedefinuje způsob generování a aktualizace inicializačních vektorů
- malý stavový prostor inicializačních vektorů (2^{12}), vznik IV kolizí
- nedostatečné zajištění integrity přenosu dat (CRC-32), možnost útoků MITM
- žádný bezpečnostní mechanismus zabraňující útokům opakovaný přenosem
- jednostranná autentizace (riziko falešných AP), ověření identity STA (ne uživatele)
- slabá autentizace založená na mechanismu výzva-odpověď, riziko MITM útoků

3.7.5 IEEE 802.1X

Norma *IEEE 802.1X*[5] [25] z roku 2001, známá jako *Port-Based Network Access Control*, byla původně vyvinuta pro použití v klasických (drátových) lokálních sítích, kde měla být řešením pro centralizovanou *autentizaci*, *autorizaci a řízení přístupu* a *management klíčů*. Nespecifikuje ale žádné závazné bezpečnostní mechanismy pro dosažení těchto cílů. Proto se na IEEE 802.1X pohlíží spíše jako na *obecný bezpečnostní rámec* (*framework*) než na úplnou specifikaci samu o sobě.

Architektura

IEEE 802.1X definuje tři základní entity, které se účastní autentizačního procesu. Těmi jsou *žadatel* (*Supplicant*), požadující přístup do sítě, *autentizátor* (*Authenticator*), prosazující autentizaci a řízení přístupu, a *autentizační server* (*AS*, *Authentication Server*), jenž provádí vlastní ověření identity žadatele. Rámec IEEE 802.1X je přitom možné použít v takových lokálních sítích, kde spojení (*port*) mezi entitou přistupující k síti a přístupovým bodem lze charakterizovat jako *jednobodové* (*PTP*, *Point-To-Point*) tak, aby byl mezi žadatelem a autentizátorem vztah *1:1* (*One-To-One*). Zařízení pak přistupuje k LAN na základě dvou *logických portů*: *neřízeného* (*Uncontrolled*), propouštějícího pouze autentizační rámce, a *řízeného* (*Controlled*), kterým přistupuje autorizovaný klient k zdrojům sítě. Autentizaci může iniciovat žadatel i autentizátor - oba se označují zkratkou *PAE* (*Port Access Entity*).

Komunikace mezi žadatelem a autentizačním serverem je při probíhající autentizaci řízena protokolem *EAP* (*Extensible Authentication Protocol*) [26, 27], zvyšujícím bezpečnost původního protokolu *PPP* (*Point-To-Point Protocol*). Autentizátor zde plní jen pasivní roli, která spočívá v předávání zpráv. EAP rámce pro přenosy mezi žadatelem a autentizátorem v lokální síti zapouzdřuje protokol *EAPOL* (*EAP Over LAN*). Obdobně také autentizátor komunikuje s autentizačním serverem skrz *AAA* (*Authentication-Authorisation-Accounting*) protokol na vyšší vrstvě. Po ukončení autentizace následuje fáze *distribuce kryptografických klíčů* úspěšným žadatelům. S jejím dovršením každá stanice sdílí s autentizačním serverem unikátní *tajný klíč* (*MK*, *Master Key*).

[5] jde o standard specifikovaný v rámci podvýboru *IEEE 802.1* a nikoliv IEEE 802.11, někdy také bývá vzhledem ke svému uplatnění především v sítích IEEE 802.11 chybně označován jako IEEE 802.11X

IEEE 802.1X v prostředí WLAN IEEE 802.11

Aplikujeme-li obecnou strukturu rámce IEEE 802.1X na architekturu lokálních bezdrátových sítí definovaných normou IEEE 802.11, *žadatele* představuje *STA* a *autentizátora AP*, který řídí logické porty a udržuje spojení na portu bezdrátové stanice. *Autentizačním serverem* bývá nejčastěji *RADIUS*, případně *DIAMETER* (viz část 3.8.2). V případě WLAN se pak užívají pojmy "*EAP Over Wireless*" (*EAPOW*) a "*EAP Over RADIUS*" (*EAPOR*). STA je umožněna asociace k WLAN, avšak do úspěšného ukončení autentizace je veškerá ostatní komunikace blokována. Autentizátor, tzn. přístupový bod, může také dodatečně provádět *filtrování MAC adres* a některým bezdrátovým stanicím tak odmítnout i pouhé zahájení autentizace. Cílem je prevence vůči *DoS* útokům.

IEEE 802.1X odstraňuje některé nedostatky WEP, nikoliv všechny. Hlavním přínosem jsou centralizované *autentizační* a *autorizační* mechanismy a zejména *management klíčů*. Narozdíl od protokolu WEP tak IEEE 802.1X řeší distribuci klíčů a nově přináší jejich dynamičnost, kdy se generují *unikátní klíče* pro každého *uživatele* a *relaci*, a to s časově omezenou dobou platnosti (implicitně 60 minut). V případě používání globálních klíčů ve WLAN (WEP klíče) je relační klíč získaný od autentizačního serveru použit k zašifrování globálního klíče. Je tak zajišťována *autenticita* a *integrita* každého *paketu*. Navíc jsou k dispozici i autentizační metody (hesla, digitální certifikáty, čipové karty, viz dále), které umožňují *vzájemnou autentizaci* žadatele a autenizačního serveru, přičemž je autentizován sám *uživatel* a nikoliv bezdrátová stanice, jako tomu je v případě WEP. Je tak vyloučeno narušení bezpečnosti v případě krádeže bezdrátového zařízení.

Autentizační metody a jejich zranitelná místa

Protokol EAP nabízí několik metod autentizace, z nichž některé představují otevřená řešení, jiná jsou naopak proprietární. V principu lze využívat i několik současně, avšak za cenu dodatečné režie provozu a vyšších nároků na administraci. V každém případě musí ale být zajištěna podpora dané autentizační techniky na straně žadatele i autentizačního serveru. Následující přehled uvádí nejvýznamnější ***metody autentizace protokolem EAP***:

- ***EAP-MD5*** (*EAP - Message Digest 5*) - nejméně bezpečná metoda, jednostranná autentizace na základě přístupového jména a hesla, riziko slovníkových útoků, chybí podpora dynamických WEP klíčů;
- ***LEAP*** (*Lightweight EAP*) - metoda společnosti Cisco, vzájemná autentizace na základě přístupového jména a hesla pomocí serveru RADIUS, dynamické klíče na uživatele a relaci, riziko slovníkových útoků;
- ***EAP-FAST*** (*EAP - Flexible Authentication via Secure Tunneling*) - nástupce LEAP, vzájemná autentizace přístupovým jménem a heslem, metoda odolná vůči slovníkovým útokům (vytvořen bezpečný tunel mezi žadatelem a serverem RADIUS);
- ***EAP-TLS*** (*EAP - Transport Layer Security*) - vzájemná autentizace na základě digitálních cerifikátů, metoda bezpečná a odolná vůči MITM útokům, vyšší nároky na implementaci;
- ***EAP-TTLS*** (*EAP - Tunneled Transport Layer Security*) - vzájemná autentizace založená na TLS, digitální certifikát jen na straně autentizačního serveru, autentizace uživatelů přístupovým jménem a heslem;

- ***PEAP*** (*Protected EAP*) - podobné TTLS, bezpečný tunel vytvořen mezi žadatelem a autentizačním serverem pomocí TLS, digitální certifikát na straně serveru, uživatel se autentizuje některou z jiných EAP metod;
- ***EAP-SIM*** (*EAP - Subscriber Identity Module*) - jde o metodu navrženou společností Nokia pro autentizaci uživatelů a distribuci relačních klíčů v GSM, v bezdrátových lokálních sítích má význam jako podpora vzájemné autentizace při roamingu mezi mobilními sítěmi a veřejnými WLAN (*tzv. hot-spots*), pro zajištění integrity zpráv používá autentizační kód;
- ***EAP-AKA*** (*EAP - Authentication and Key Agreement*) - mechanismus zajišťující autentizaci a distribuci relačních klíčů v prostředí UMTS na základě USIM.

Jak již naznačuje název *Extensible Authentication Protocol*, EAP je protokolem, který umožňuje další dodatečné rozšíření o nově vznikající autentizační metody. Jmenovitě jde např. o metodu *EAP-PAX* (*EAP - Password Authenticated eXchange*) nebo *EAP-SAKE* (*EAP - Shared-secret Authentication and Key Establishment*). Ne všechny v minulosti navrhované metody ale nakonec našly svoje uplatnění. Jako příklady mohou sloužit metody *EAP-SKE* (*EAP - Shared Key Exchange*) a *EAP-GSS* (*EAP - Generic Security Service*), které se nepodařilo udržet ani ve stádiu návrhu. Na závěr této části je ve formě tabulky 3.3 provedeno shrnutí nejdůležitější vlastnosti IEEE 802.1X.

Tabulka 3.3: Klady (+) a zápory (-) IEEE 802.1X

+ *lze použít jako nadstavbu protokolu WEP - odstraňuje některé jeho nedostatky*
+ *umožňuje vzájemnou autentizaci uživatele a bezdrátové sítě*
+ *podpora autentizace založené na identitě uživatele a nikoliv zařízení*
+ *více autentizačních metod s různou úrovní bezpečnosti (hesla, ceritifikáty, ...)*
+ *protokol EAP umožňuje další rozšíření i o nové autentizační metody*
+ *dynamické generování klíčů (na uživatele a pro relaci)*
+ *při implementaci lze využít stávajících prostředků (RADIUS)*
- *je vyžadována nákladnější infrastruktura (autentizační server)*
- *riziko slovníkových, DoS a MITM útoků, únosů relací a krádeží identity (dle metody)*

3.7.6 WPA

Specifikace *WPA* (*Wi-Fi Protected Access*) [28] z roku 2003 měla za cíl odstranit všechny závažné nedostatky protokolu WEP takovým způsobem, aby bylo dosaženo vysoké úrovně bezpečnosti v oblasti *autentizace*, *důvěrnosti* a *integrity* dat, ale současně bez nutnosti výměny stávajícího technického vybavení WLAN. Aktualizace nezbytné pro implementaci WPA by se tedy měly odehrávat pouze na úrovni softwarových a firmwarových změn. Vzhledem k takovému požadavku byly ponechány některé bezpečnostní prvky z protokolu WEP, jiné naopak převzaty z doplňku IEEE 802.11i (viz část 3.7.7), jehož ratifikace proběhla až v roce 2004. Přestože tedy WPA vychází z bezpečnostních mechanismů definovaných normou IEEE 802.11, nejde o standard definovaný přímo organizací IEEE, nýbrž o aktivitu sdružení *Wi-Fi Alliance*, které zamýšlelo WPA jako dočasné, kompromisní řešení právě před oficiálním uvedení bezpečnostní specifikace IEEE 802.11i.

Autentizace

V závislosti na prostředí, ve kterém se bezdrátová lokální síť provozuje, nabízí specifikace WPA dva ***autentizační mechanismy***:

- ***IEEE 802.1X*** představuje autentizační schéma, které je primárně orientováno na *podnikové prostředí* (tzv. *WPA-Enterprise*). Ověření identity probíhá mezi stanicí a *AAA serverem* na základě protokolu *EAP*, jenž nabízí několik autentizačních metod, z nichž sdružení *Wi-Fi Alliance* doporučuje techniku *EAP-TLS* (viz část 3.7.5). Použití jiných metod autentizace je sice také možné, může však přinést problémy s nekompatibilitou bezdrátových zařízení různých výrobců.
- ***Autentizace s přednastaveným klíčem*** (*PSK*, *Pre-Shared Key Authentication*) je zjednodušeným mechanismem autentizace pro *menší sítě* (tzv. *WPA-Personal*), kde není pro distribuci klíčů k dispozici autentizační server. Stejně jako v případě protokolu WEP je nutné sdílené klíče nakonfigurovat manuálně u všech zařízení a často také bývá nastaven jeden shodný klíč pro celou bezdrátovou síť. Specifikace WPA vyžaduje 256-bitový sdílený klíč, ale vzhledem k jeho přílišné složitosti pro zapamatování uživateli se používají *ASCII hesla* (8 až 63 znaků), z nichž je pak vlastní *PSK klíč* o délce 32 bytů vygenerován.

Hierarchie klíčů

Vrcholem *hierarchie WPA klíčů* pro ***unicastový provoz*** je ***PMK*** (*Pair-wise Master Key*) o délce 256 bitů, jenž se v případě použití IEEE 802.1X odvodí na základě autentizačního procesu, při manuální distribuci sdílených klíčů jde pak přímo o přednastavený PSK klíč. Pomocí PMK se dále vyvozuje dočasný 512-bitový klíč ***PTK*** (*Pair-wise Transient Key*) jako výstup pseudonáhodné funkce *PRF-512* (*PseudoRandom Function - 512*), která za vstupní parametry vyžaduje kromě PMK ještě MAC adresu obou komunikujících stran (tzn. STA a AP), pevně zvolený řetězec a dvě náhodná čísla, která si mezi sebou vymění účastnící pomocí *čtyř zpráv* (*4-Way Handshake*). Výsledný PTK klíč pak tvoří čtyři dílčí 128-bitové ***relační klíče***:

- ***KEK*** (*Key Encryption Key*) - pro zajištění důvěrnosti zpráv protokolu EAPOL;
- ***KCK*** (*Key Confirmation Key*) - integrita a autenticita zpráv protokolu EAPOL;
- ***TEK*** (*Temporary Encryption Key*) - pro zajištění důvěrnosti dat protokolem TKIP;
- ***TMK*** (*Temporary MIC Key*) - pro zajištění autenticity a integrity dat protokolem TKIP, pro každý směr jeden ze dvou 64-bitových MIC klíčů - ***TMK1*** a ***TMK2***.

Analogicky pro ***multicastový provoz*** pak existuje klíč ***GMK*** (*Group Master Key*), jehož hodnotu generuje přístupový bod. Odvozený ***GTK*** (*Group Transient Key*, 256 bitů) klíč tvoří dva dílčí 128-bitové ***relační klíče***:

- ***GEK*** (*Group Encryption Key*) - zajištění důvěrnosti dat protokolem TKIP;
- ***GIK*** (*Group Integrity Key*) - zajištění autenticity a integrity dat protokolem TKIP.

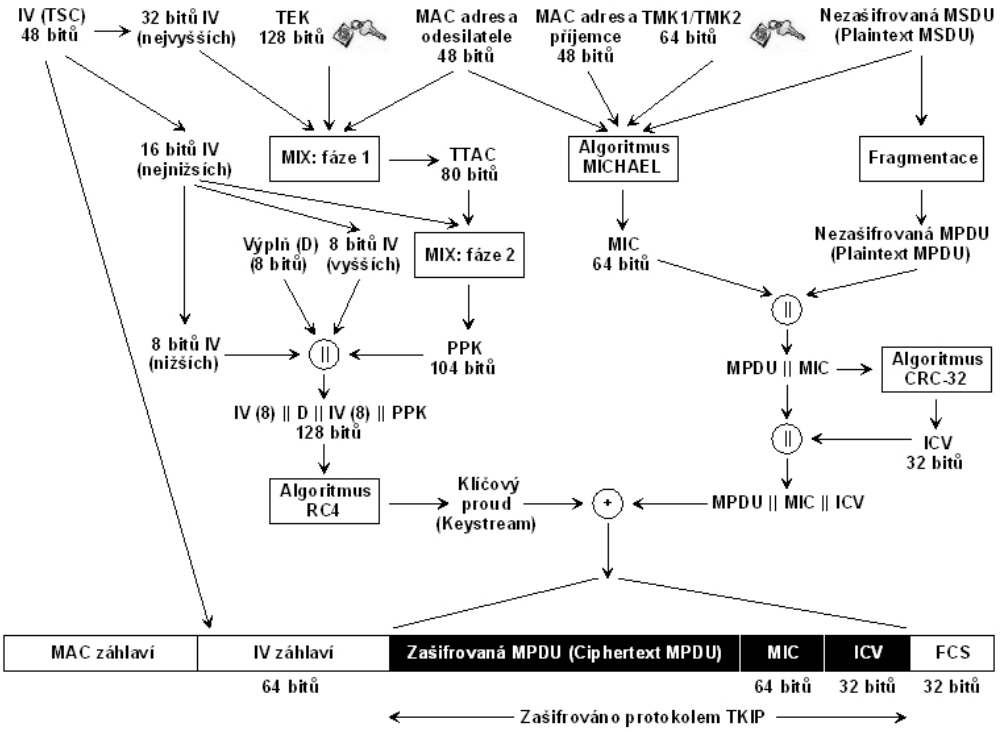
TKIP - důvěrnost a integrita dat

Schéma šifrování protokolem *TKIP* (*Temporal Key Integrity Protocol*) je zachyceno na obr. 3.4. Nejzásadnějším rysem, který jej spojuje s protokolem WEP, je použití šifry *RC4*. Narozdíl od WEP však používá 48-bitové *inicializační vektory* (*IV*), které zamezují IV kolizím a současně plní roli *sekvenčního čítače* (*TSC*, *TKIP Sequence Counter*). Číslování přenášených rámců je v protokolu implementováno jako bezpečnostní opatření vůči útokům opakovaným přenosem. TKIP využívá místo prosté konkatenace sdíleného klíče a IV, kterou implementuje WEP, *dvoufázovou jednocestnou funkci*. *První fáze* směšuje nejvyšších 32 bitů inicializačního vektoru, MAC adresu odesilatele o délce 48 bitů a 128-bitový TEK klíč. Vstupem *druhé fáze* je 80-bitový výstup (*TTAC*, *TKIP-mixed Transmit Address and Key*) fáze předcházející a dále nejnižších 16 bitů IV. Výsledkem je *unikátní klíč* pro každý rámec (tzv. *PPK*, *Per-Packet Key*, správné označení by však mělo být *Per-Frame Key*, případně *Per-MPDU Key*, viz dále) o délce 104-bitů, ke kterému se následně připojí dva nejnižší byty IV a jeden *výplňkový byte* (tzv. *Dummy Byte*) jako prevence vůči vzniku slabých klíčů. Výsledkem je 128-bitový *RC4 šifrovací klíč*.

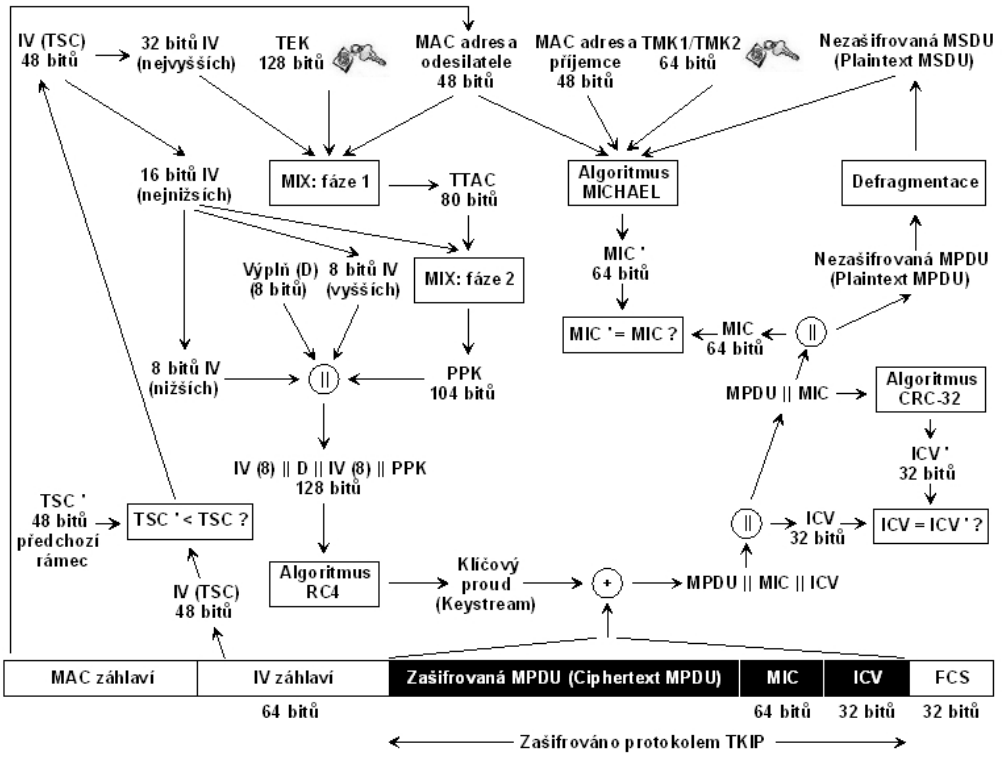
Z vlastní *nezašifrované zprávy* (*Plaintext MSDU*), předané z vyšší vrstvy v podobě *MSDU* (*MAC Service Data Unit*), je nejprve vypočten algoritmem *MIC* (*Message Integrity Check*), často označovaným také jako *MICHAEL*, *kryptografický kontrolní součet*, který má zajistit *integritu* a *autenticitu* přenášených dat. Jeho vstupními parametry jsou kromě MSDU také zdrojová a cílová MAC adresa a 64-bitový TMK klíč (TMK1 nebo TMK2). MSDU následně projde *fragmentací* a ke každé vzniklé *MPDU* (*MAC Protocol Data Unit*) se připojí hodnota MIC. Z výsledné konkatenace je pak algoritmem *CRC-32* spočten druhý kontrolní součet - *ICV* (*Integrity Check Value*). *Zašifrovaná zpráva* (*Cihpertext MPDU*) je stejně jako u protokolu WEP výsledkem operace *XOR*, jejíž první parametr představuje výstup šifry RC4, tzn. *klíčový proud* (*Keystream*), druhý pak *MPDU s připojeným MIC a ICV*. Inicializační vektor se v zapouzdřeném rámci přenáší jako součást 64-bitového *IV záhlaví*, které obsahuje i další položky, mezi něž patří mj. identifikátor použitého klíče.

Dešifrování protokolem TKIP (viz obr. 3.5) je (stejně jako v případě protokolu WEP) vzhledem k aplikaci symetrické kryprografie založeno na stejném algoritmu jako šifrování. Jediný rozdíl spočívá pouze v dodatečných kontrolách TSC, ICV a MIC. Jako první se prověří hodnota inicializačního vektoru, jenž není šifrován a v případě TKIP udává i pořadí příchozího rámce. TKIP narozdíl od protokolu WEP definuje mechanismus generování a aktualizace inicializačních vektorů, kdy jejich počáteční hodnota musí být vždy rovna nule s postupnou inkrementací o jedničku s každou zašifrovanou MPDU. Každá zpráva s TSC nižší, než je hodnota inicializačního vektoru uvedená v předchozím přijatém rámci, bude tedy adresátem odmítnuta. Následuje kontrola ICV, která probíhá stejně jako v případě WEP. Po rekonstrukci původní MSDU z odpovídajícího počtu dešifrovaných MPDU je závěrem provedeno ověření integrity přenesených dat algoritmem MICHAEL, navrženým jako kompromis mezi bezpečnosti a výpočetní efektivností[6]. To si tvůrci uvědomovali a implementovali dodatečný bezpečnostní mechanismus: bude-li zjištěna během jedné vteřiny alespoň v dvou případech neshoda mezi přijatým a explicitně vypočteným MIC, paket bude odmítnut, proběhne disasociace stanice a po uplynutí jedné minuty její opětovná asociace včetně nového ustavení kryptografických klíčů. Při konstrukci MIC příjemce dle směru provozu použije jeden z klíčů TMK1, TMK2. Zde rozhoduje, zda je adresát přístupovým bodem nebo stanicí, tzn. probíhá-li komunikace ve směru od AP k STA či naopak.

[6]té bylo dosaženo použitím bitových posuvů a součtů místo výpočetně náročnějších operací násobení, které se běžně používají v kryptograficky silnějších protokolech (např. MD5, SHA-1 aj.)



Obrázek 3.4: TKIP - šifrování (operace XOR značena jako +, konkatenace symbolem ||)



Obrázek 3.5: TKIP - dešifrování (operace XOR značena jako +, konkatenace symbolem ||)

Zranitelná místa a útoky na WPA

Přestože specifikace WPA úspěšně odstranila mnohé nedostatky protokolu WEP, obsahuje také svoje vlastní specifické slabiny. Mezi nejzávažnější zranitelná místa patří otevřenost vůči *slovníkovým útokům* na hesla, která se v případě použití autentizace s přednastaveným klíčem po jejich zadání následně transformují na vlastní PSK klíče. Vzhledem k tomuto riziku sdružení Wi-Fi Alliance doporučuje generování PSK klíčů z *ASCII hesel* buď vůbec neimplementovat, nebo používat hesla s možná největší délkou (za bezpečné minimum je považováno heslo o délce 20 znaků, maximálně však 63 znaků). Zranitelná místa obsahuje i protokol *EAP*, jenž se využívá v případě autentizace založené na *IEEE 802.1X* (viz 3.7.5), přestože její bezpečnostní úroveň je ve srovnání s autentizací s přednastaveným klíčem nepoměrně vyšší. Bezpečnostní mechanismy zaměřené vůči úmyslnému narušení integrity přenosu dat (tzn. disasociace stanice, časová prodleva a opětovná asociace) pak mohou být předmět *DoS* útoků. Celkové zhodnocení WPA obsahuje tab. 3.4.

Tabulka 3.4: Klady (+) a zápory (-) specifikace WPA

+ *odstraňuje všechny závažné nedostatky protokolu WEP*
+ *pro přechod z protokolu WEP na WPA postačují pouze softwarové/firmwarové změny*
+ *vysoká úroveň zabezpečení při zachování dobré výpočetní efektivity*
+ *dopředná kompatibilita s IEEE 802.11i a zpětná slučitelnost s WEP*
+ *management klíčů a podpora vzájemné autentizace na bázi 802.1X/EAP*
+ *pro menší sítě jednodušší autentizace nevyžadující použití autentizačního serveru*
+ *konstrukce unikátního klíče pro každý rámec na základě dvoufázové hašovací funkce*
+ *rozšířená délka inicializačních vektorů (48 bitů), výrazně sníženo riziko IV kolizí*
+ *výpočetně efektivní kryptografická kontrola integrity zprávy (MIC)*
+ *zabraňuje přesměrování provozu (MIC bere v úvahu MAC adresu zdroje a cíle)*
+ *IV slouží i jako sekvenční čítač - zamezení útokům opakovaným přenosem*
- *použití synchronní proudové šifry RC4, nevhodné pro prostředí bezdrátové komunikace*
- *vyšší složitost TKIP šifrování snižuje výkonnost oproti WEP o 5 až 15 %*
- *bezpečnostní mechanismy zamezující zneužití MIC mohou být předmětem DoS útoků*
- *zranitelná PSK autentizace, 802.1X náročnější na implementaci (autentizační server)*

3.7.7 IEEE 802.11i (WPA2)

Doplněk *IEEE 802.11i* [30] byl ratifikován roku 2004 jako úplná náhrada protokolu WEP. Nová bezpečnostní architektura, kterou specifikace IEEE 802.11i definuje, je označována jako *RSN* (*Robust Security Network*). Přestože mnohé z jejích rysů byly zahrnuty již ve specifikaci WPA, přináší navíc některé významné bezpečnostní mechanismy. Mezi ně patří zejména protokol *CCMP*, jenž využívá šifru *AES* a zajišťuje již dostatečnou úroveň *důvěrnosti*, *integrity* a *autenticity* přenosu dat. Nahrazuje protokol *TKIP* (algoritmus *RC4*), který je již jen volitelný z důvodu *zpětné kompatibility* (*TSN*, *Transient Security Network*). Dalšími novými rysy v IEEE 802.11i jsou podpora *zabezpečení ad-hoc sítí*, *handover* v rámci ESS na základě *předběžná autentizace* a drobné úpravy v *managementu kryptografických klíčů*. Bezdrátovým zařízením, které podporují bezpečnostní mechanismy dle IEEE 802.11i, sdružení *Wi-Fi Alliance* uděluje označení *WPA2*.

Autentizace a hierarchie klíčů

Autentizace v IEEE 802.11i probíhá stejně jako u WPA. Je tedy k dispozici jeden režim založený na *PSK*, druhý využívá rámce *802.1X* s protokolem *EAP* a vyžaduje *autentizační server*. Nově je podporována již zmíněná *předběžná autentizace* (*Preauthentication*), jež má za cíl snížit zpoždění při přechodu STA od jednoho AP k jinému. Stanice v tomto případě pošle autentizační požadavek v předstihu přístupovému bodu, k němuž se v budoucnu předpokládá asociovat. Zpráva se šíří prostřednictvím distribučního systému přes AP, ke kterému je v daném okamžiku stanice autentizována. Zde se uplatňuje další nový prvek IEEE 802.11i: *ukládání klíčů PMK do cache* (*PMK Caching*), které provádí při dokončení úspěšné autentizace STA i AP v BSS buňce, do níž stanice přechází. Po uskutečněném handoveru obě zařízení pracují s PMK klíčem uloženým v cache, čímž je eliminována časově náročná komunikace s autentizačním serverem pomocí zpráv protokolu EAP.

Změny se týkají i *šifrovacích klíčů*. Zatímco TKIP používá klíč PTK o délce 512 bitů a 256-bitový GTK klíč, CCMP vyžaduje jediný klíč pro zajištění důvěrnosti, integrity a autenticity sloučením klíčů TEK s TMK a GEK s GIK. Důsledkem je 384-bitový *PTK* klíč pro unicastový a 128-bitový *GTK* klíč pri multicastový provoz.

CCMP - důvěrnost, integrita a autenticita dat

CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) [31] je protokol využívající šifru *AES* [32, 33] se 128-bitovým klíčem. Pracuje v režimu *CCM*, který kombinuje režim *CTR* (*Counter Mode*), zajišťující šifrováním *důvěrnost* obsahu MPDU, a režim *CBC-MAC* (*Cipher Block Chaining Message Authentication Code*), jenž má zabezpečovat *integritu* a *autenticitu* MPDU na základě *MIC*. *Inicializační vektory* mají délku 48-bitů a stejně jako u TKIP slouží také k *číslování rámců*, v nichž jsou uloženy jako součást *CCMP záhlaví* (u TKIP IV záhlaví). Zapouzdřený rámec má stejnou podobu jako u WPA (viz obr. 3.4), není jen obsažena hodnota ICV, což zkracuje délku rámce o 32 bitů. CCMP je protokolem s celkově velmi vysokou úrovní bezpečnosti a žádné závažnější slabiny, které by byly prakticky využitelné pro provádění útoků, nejsou známé.

Tabulka 3.5: Klady (+) a zápory (-) IEEE 802.11i (WPA2) ve srovnání s WPA a WEP

+ komplexní zabezpečení, všechny bezpečnostní výhody WPA, plně nahrazuje WEP
+ protokol CCMP s šifrou AES zvyšující úroveň důvěrnosti, integrity a autenticity dat
+ nově podpora předběžné autentizace, cachování PMK klíčů a zabezpečení ad-hoc sítí
- nové bezpečnostní prvky (nezahrnuté ve WPA) vyžadují hardwarové změny WLAN
- zranitelná PSK autentizace, 802.1X vyžaduje složitější infrastrukturu

3.8 Zabezpečení WLAN na vyšších vrstvách

Dalšího posílení bezpečnosti WLAN lze docílit za pomoci *protokolů vyšších vrstev*, které však nejsou, jak již bylo několikrát zdůrazněno, specifické pro WLAN IEEE 802.11 a bezdrátové sítě výboru IEEE 802 obecně (což ale samozřejmě nesnižuje jejich přínos pro komplexní zabezpečení WLAN). V této části proto budou v kontextu WLAN stručně popsány jen ty nejvýznamnější a nejpoužívanější bezpečnostní mechanismy. Podrobnější informace nalezne čtenář ve specializovaných publikacích. [34, 35].

3.8.1 Zabezpečení WLAN na síťové vrstvě

Zatímco linková vrstva zabezpečuje přenos dat mezi sousedními uzly, v kompetenci *třetí vrstvy* je zajištění komunikace síťových uzlů, mezi nimiž neexistuje přímé spojení. Její nejdůležitější funkci tak představuje *adresování* a *směrování* na základě znalosti topologie komunikační sítě. Na síťové vrstvě je nutné v případě WLAN implementovat *handover* mezi přístupovými body nacházejícími se v odlišných ESS, příp. i doplňkové mechanismy pro zajištění *QoS* (na linkové vrstvě řeší kvalitu služeb IEEE 802.11e, handover pak specifikace IEEE 802.11F a vyvíjený doplněk IEEE 802.11r, viz 3.9.1).

Statické přidělování IP adres

Počítačové sítě běžně využívají protokol *DHCP* (*Dynamic Host Configuration Protocol*), který mj. umožňuje *dynamické přidělování IP adres*. To sice přináší výhody v podobě výrazného snížení administrativní zátěže a zamezení vzniku IP kolizí, jeho implementace v případě WLAN ale vyvolává vážné bezpečnostní otázky. Umožnění přístupu k DHCP serveru znamená také možnost přistupovat k síti, což v klasických lokálních sítích vzhledem k nutnosti fyzické přípojky nepředstavuje z pohledu bezpečnosti větší problém. Při přístupu k WLAN však žádné fyzické bariéry neexistují a každý, kdo zná SSID bezdrátové sítě, může snadno požádat o přidělení IP adresy a tu také získat. Zde je riziko *neutorizovaného přístupu* do WLAN, poněvadž DHCP server sám o sobě nedokáže odlišit oprávněného uživatele od případného útočníka. Proto použití DHCP v případě WLAN není žádoucí a naopak je doporučováno statické přidělování IP adres.

Filtrování IP adres

Techniku statického přidělování IP adres lze dále zefektivnit filtrováním založeným na *přístupových seznamech IP adres*, které funguje velmi podobně jako v části 3.7.3 popsaný mechanismus filtrování MAC adres na linkové vrstvě. Řízení přístupu na úrovni IP adres je přínosné i při použití DHCP.

Firewall

Firewall je dobře známým bezpečnostním mechanismem, který zajišťuje *řízení přístupu* na základě filtrování vstupního a výstupního provozu dle určitých pravidel, přičemž konkrétní způsob, jakým jsou konfigurovány, se označuje termínem *bezpečnostní politika firewallu*. Firewall typicky provádí kontroly na úrovni protokolu, zdrojové a cílové adresy, zdrojového a cílového portu, stavu spojení apod., ty nejmodernější obsahují i prvky IDS (viz část 3.9.3). Klasické firewally pracují na síťové vrstvě a mají podobu *paketových filtrů*, popř. *stavových paketových filtrů*, vyšší úrovně bezpečnosti lze dosáhnout pomocí firewallů aplikační vrstvy, jde o tzv. *aplikační brány*, známé také jako *proxy firewally*. V prostředí bezdrátových sítí je nutné používat firewally za účelem separace bezdrátové lokální sítě od pevné podnikové sítě a zabránění *neautorizovanému přístupu* k WLAN z Internetu.

VPN/IPSec

Silným a často používaným bezpečnostním opatřením je *VPN* (*Virtual Private Network*). VPN se nasazuje tam, kde vzdálený přístup skrz WLAN jako tranzitní síť je sám o sobě považován za nezabezpečený. Proto *VPN klient* (bezdrátová stanice) a *VPN brána* (může být uvnitř podnikové infrastruktury, ale spíše na jejím okraji vzhledem k použití firewallu)

mezi sebou ustaví *bezpečené tunelové spojení* za účelem zajištění *autentizace*, *důvěrnosti* a *integrity* přenášených dat. VPN spojení se nejčastěji vytváří pomocí protokolů *IPSec* (*IP Security Protocol*), *L2F* (*Layer-2 Forwarding*), *L2TP* (*Layer-2 Tunnelling Protocol*), *PPTP* (*Point-to-Point Tunnelling Protocol*), *GRE* (*Generic Routing Encapsulation*) aj. Přestože použití VPN představovalo největší přínos pro zabezpečení WLAN v dobách, kdy nebyly dostupné dostatečně silné bezpečnostní mechanismy na úrovni linkové vrstvy (tzn. pouze WEP), neztrácí na významu ani při implementaci doplňku IEEE 802.11i. VPN sice neobsahuje žádná závažná zranitelná místa a většina problému souvisí s konkrétní implementací daného výrobce, je ale nutné věnovat pozornost zabezpečení ve fázi *ustavování tunelového spojení*, která je náchylná na útoky typu *MITM* a *DoS*. Mohou také vznikat problémy při *handoveru*.

3.8.2 Zabezpečení WLAN na aplikační vrstvě

Aplikační vrstva je nejvyšší vrstvou RM ISO/OSI a plní funkci *služebního rozhraní pro spouštění aplikační procesů* a jejich vzájemnou *komunikaci* v síti. Mimo dále uvedených bezpečnostních mechanismů pracují na aplikační vrstvě např. protokoly *Kerberos*, *TACACS* a *TACACS+*, dále také běžné *softwarové nástroje* pro detekci a odstraňování *škodlivých programů* (*Malware*).

TLS/SSL

TLS (*Transport Layer Security*) [36] a jeho předchůdce *SSL 3.0* (*Secure Sockets Layer*) [37] jsou protokoly, které zabezpečují síťovou komunikaci některých aplikací (nikoliv všech). TLS/SSL vyžaduje spolehlivý transportní protokol (TCP) a zajišťuje stejné bezpečnostní cíle jako VPN. Pro jejich dosažení využívá asymetrickou (*autentizace*, *distribuce klíčů*) i symetrickou (*důvěrnost* a *integrita* zpráv) kryptografii. Autentizaci lze provádět *hesly*, *tokeny* nebo *digitálními certifikáty*.

RADIUS

Protokol *RADIUS* (*Remote Authentication Dial In User Service*) [38, 39] byl zmíněn již v části 3.7.5. RADIUS se ve WLAN uplatňuje jako velmi často používané řešení pro zajištění *autentizace*, *autorizace* a *účtovatelnosti* (*AAA*, *Authentication-Authorisation-Accounting*). Z protokolů transportní vrstvy využívá UDP. V RADIUS architektuře vystupují *uživatelé* (připojují se na klienty), *klienti* (přístupové servery, NAS servery) a *autentizační servery* (RADIUS servery). Podporováno je několik *autentizačních metod* (PPP PAP, EAP, ...). Komunikace mezi klientem a serverem probíhá na základě *sdíleného hesla*, které se po síti nepřenáší. Uživatel nejprve naváže spojení s klientem, který si od něj vyžádá autentizační údaje a následně je přepošle autentizačními serveru. Ten rozhodne, zda bude či nebude přístup do sítě povolen. RADIUS však obsahuje zranitelná místa, která mohou být využita pro realizaci útoků *hrubou silou*, *opakovaným přenosem*, *slovníkových*, *DoS* a *MITM* útoků.

DIAMETER

DIAMETER [40] je dalším z *AAA protokolů* a jako nástupce protokolu RADIUS přináší několik nových rysů. Mezi nejvýznamnější z nich se řadí použití spolehlivého protokolu transportní vrstvy (TCP nebo SCTP namísto UDP) a zdokonalená podpora roamingu. DIAMATER sice podporuje RADIUS přenosy, nezaručuje ale přímo zpětnou kompatibilitu.

3.9 Další vývoj v oblasti zabezpečení WLAN

Závěr kapitoly o zabezpečení WLAN je věnován aktuálním oblastem výzkumu a vývoje, a to jak vznikajícím bezpečnostním doplňkům normy IEEE 802.11, tak i dalším mechanismům.

3.9.1 IEEE 802.11r - rychlý a bezpečný handover

Vzhledem k stále většímu rozšíření technologie WLAN a rostoucímu počtu bezdrátových zařízení vznikají nové požadavky na podporu mobilních aplikací pracujících v reálném čase. Proto jedním z aktuálních témat výzkumu v oblasti WLAN je *handover*, a to především co se týče *minimalizace zpoždění* a zajištění dostatečné úrovně *bezpečnosti*. Právě tyto cíle se snaží naplnit nový doplněk *IEEE 802.11r* [41], jehož schválení se očekává v měsíci září roku 2007. Přestože handoverem se již zabývá doporučení IEEE 802.11F, doplněk IEEE 802.11i a IEEE 802.11e zavádí do WLAN podporu pro zajištění kvality služeb, běžně dosahované latence se pohybují řádově ve stovkách milisekund. To ale vůbec nepostačuje pro potřeby *bezdrátové telefonie* (*VoWLAN*, *Voice over WLAN*), kde je pro plynulé přechody tolerováno maximální zpoždění do padesáti milisekund.

IEEE 802.11r také obsahuje i významné rysy z hlediska bezpečnosti. Cílem je provádět veškeré autentizační procesy ještě před započetím handoveru. Klíč PMK má být generován již při asociaci stanice k síti a bude distribuován všem AP, které jsou v podsíti autentizované. Při přechodu stanice mezi přístupovými body se tedy předpokládá, že PMK klíč je již k dispozici. IEEE Specifikace 802.11i sice volitelně podporuje ukládání PMK klíčů do cache, doplněk IEEE 802.11r však navíc redukuje zpoždění tím, že provádí další odvozování klíčů již v průběhu reasociace a nikoliv až po jejím dokončení. IEEE 802.11r také specifikuje novou hierarchii klíčů včetně způsobu jejich odvozování.

3.9.2 IEEE 802.11w - zabezpečení management rámců

Činnost pracovní skupiny vyvíjející doplněk *IEEE 802.11w* [42] byla zahájena v roce 2005. Cílem výboru IEEE 802.11w je vytvoření specifikace nových mechanismů pro zabezpečení *management rámců*. Management rámce zodpovídají za asociaci, reasociaci, disasociaci, autentizaci, deautentizaci, synchronizaci a výměnu informací o parametrech jednotlivých stanic (viz část 3.1.2). Původně neobsahovaly citlivá data a nebyla ani vyžadována žádná forma jejich ochrany. S dalším rozvojem normy IEEE 802.11 a přibývajícími návrhy nových doplňků (viz tab. 3.1), které mj. definují správu rádiových prostředků (IEEE 802.11k), rychlý handover mezi přístupovými body (IEEE 802.11r) a mechanismy managementu WLAN (IEEE 802.11v), se ale situace mění a cílem je rozšíření platnosti bezpečnostních mechanismů definovaných doplňkem IEEE 802.11i také na management rámce. Dokončení specifikace IEEE 802.11w se očekává v průběhu roku 2008.

IEEE 802.11w definuje tři různé typy ochrany. Do první kategorie spadají management rámce využívané při komunikaci mezi danou stanicí a přístupovým bodem (tzn. *unicast*). Z těchto rámců může útočník zjistit informace o topologii sítě a umístění jednotlivých síťových zařízení, což jsou poznatky užitečné při provádění *DoS* útoků na WLAN. Proto IEEE 802.11w specifikuje bezpečnostní mechanismy pro zajištění *důvěrnosti* těchto rámců. Jde přitom o stejné algoritmy jako v případě IEEE 802.11i, tzn. šifrování *TKIP* a *CCMP*. Přestože takto může být zabráněno některým *DoS* útokům, pracovní skupina vyvíjející doplněk IEEE 802.11w deklaruje, že toto není cílem, poněvadž útočník může provádět velmi účinné *DoS* útoky na fyzické vrstvě, tj. *jamming*.

V druhém případě jde o obecné *broadcastové management rámce*, které jsou méně obvyklé a typicky neobsahují utajované informace (např. zprávy o nastavení rádiových frekvencí). Proto postačuje zajištění jejich *integrity*. Návrh uvažuje podobný *integritní kód*, jaký používá TKIP, tzn. *MIC* (*Message Integrity Check*). Přístupový bod by pak sdílel kryptografický klíč s každou přidruženou stanicí.

Poslední kategorii představují *deautentizační a disasociační rámce*, kde IEEE 802.11w navrhuje bezpečnostní mechanismus v podobě *dvojice jednorázových klíčů* (jeden pro STA, druhý pro AP), na základě kterých by klient ověřil platnost *deautentizace*. Zde však mohou nastat problémy při nasazování systémů pro prevenci průniku (viz dále část 3.9.3).

3.9.3 Systémy pro detekci a prevenci průniku

Ne všechny útoky mohou být detekovány a odvráceny běžnými bezpečnostními mechanismy. Proto jsou vyvíjeny *systémy pro detekci průniku* (*IDS*, *Intrusion Detection System*), které mají identifikovat narušení a zneužití počítačových systému a sítí na základě shromažďování a analýzy dat o jejich provozu. IDS systémy byly nejprve vyvíjeny pro klasické (drátové) sítě, později se výzkumné aktivity rozšířily i na WLAN. IDS systémy pro použití v bezdrátových sítích sítích se pak označují zkratkou *WIDS* (*Wireless Intrusion Detection System*).

Architekturu IDS tvoří tři komponenty: *senzory*, zachycující události důležité z hlediska bezpečnosti, *konzola*, jež řídí senzory a monitoruje chování systému, a *centrální systém*, který ukládá data generovaná senzory a dle určitých pravidel vydává výstražné signály.

IDS systémy lze klasifikovat mnoha různými způsoby, tradičně se dle *typu* a *umístění senzorů* dělí na tzv. *Host-based IDS* (*HIDS*) a *Network-based IDS* (*NIDS*). Implementace *HIDS* má podobu *softwarového agenta*, jenž identifikuje narušení analýzou systémových volání, aplikačních logů, modifikací v souborovém systému a dalších aktivit probíhajících v systému, na kterém je nainstalován. *NIDS* naopak monitoruje a analyzuje *provoz sítě*. Dalším důležitým kritériem je použitá *detekční metoda*. Na jejím základě se rozlišují tzv. *Signature-based IDS* (*SIDS*), které porovnávají uložené atributy známých útoků se vzory aktuálního chování systému, a tzv. *Anomaly-based IDS* (*AIDS*) systémy, které na základě soustavného monitorování dynamicky vytvářejí a aktualizují statistické vzorky standardního chování a odhalují anomálie v provozu systému či sítě .

WIDS vycházejí ze standardních systémů pro detekci průniku, jsou ale uzpůsobeny pro použití v prostředí WLAN. Dokáží detekovat řadu útoků na WLAN a případně i určit *polohu útočníka* (triangulace). Mohou tak být úspěšně odhaleny nejen *DoS útoky na fyzické vrstvě*, ale i pouhé *skenování bezdrátové sítě* softwarovými nástroji. Mezi další schopnosti WIDS patří mj. *detekce falešných AP*, *DoS útoků na linkové vrstvě*, *krádeže MAC adres*, aktivních *ad-hoc sítí*, použitého *nastavení pro šifrování přenosu dat* a další.

(W)IDS systémy nabízejí pouze omezené možnosti vzhledem ke skutečnosti, že pracují v pasivním režimu. Omezují se tak pouze na detekci a monitorování, aktivní zásahy jsou za hranicí jejich schopností. Proto jejich logickými nástupci jsou *systémy pro prevenci průniku* (*IPS*, *Intrusion Prevention System*), které již mají zabudované aktivní prvky a lze je přirovnat k aplikačním firewallům.

Přes všechny výhody mají IDS a IPS systémy určité *nedostatky*. Ty se definují pomocí *metrik*, které udávají v závislosti na nastavené cítlivosti systému počet *chybně detekovaných* (*FPR*, *False Positive Rate*) a *chybně nedetekovaných* (*FNR*, *False Negative Rate*) útoků. Významným parametrem je také citlivost, při níž nastává *rovnost hodnot FPR a FNR* (*CER*, *Crossover Error Rate*). Navíc IDS/IPS systémy mohou značně snižovat výkonnost a slabiny v nich samých jsou dále zneužitelné.

3.9.4 Reputační systémy

Další a méně tradiční možností zabezpečení WLAN je použití tzv. *reputačních systémů*, které obecně monitorují a zaznamenávají chování entit v určitém prostředí a získávají tím informace o jejich *důvěryhodnosti*. Lze tak sestavit *profily* a *vzory standardního chování* a naopak detekovat *anomálie* a *útoky*. Reputační systémy mohou být doplněny *motivačním systémem*, kdy za žádoucí chování entita získá speciální privilegia a naopak následkem nežádoucího chování bude určitou formou znevýhodněna. Reputační systémy jsou zranitelné tzv. *útokem Sybily* (*Sybil Attack*), kdy útočník vytvoří velké množství *pseudonymních entit* a získá tak v daném prostředí velký vliv.

V [43] autor uvádí zkušenosti s nasazením reputačního systému v prostředí komunitní WLAN IEEE 802.11. Informace o chování uživatelů byly po dobu dvou měsíců získávány ze senzorů umístěných v přístupových bodech. Mezi sledované parametry patřily IP a MAC adresy, síla signálu, úroveň šumu, čas a přístupové body, k nimž se uživatel připojoval, a množství přenesených dat, přičemž legitimnost těchto i jiných metrik je při hodnocení reputace předmětem dalšího výzkumu. Výsledkem byly nové poznatky o chování uživatelů a odhalení několika skutečných útočníků.

Kapitola 4

Zabezpečení WPAN IEEE 802.15

Bezdrátové osobní sítě (***WPAN***, ***Wireless Personal Area Network***) specifikuje podvýbor ***IEEE 802.15***. WPAN umožňuje bezdrátovou komunikaci a interoperabilitu mobilních a přenosných zařízení (PC, PDA, pagery, periferie, mobilní telefony, ...), která se fyzicky nacházejí v tzv. *osobním operačním prostoru* (*POS*, *Personal Operating Space*). POS zaujímá oblast o průměru typicky do 10 m v okolí určitého zařízení nebo jednotlivce. WPAN je tedy bezdrátovou sítí s *krátkým dosahem* (*Short-distance Wireless Network*) jako silný prostředek interpersonální komunikace s možností propojení na vyšší sítě.

WPAN se ve srovnání s WLAN liší nejen svým dosahem, ale i propustností, počtem síťových uzlů, jejich vlastníky a fyzickými rozměry, životností sítě, energetickou náročností i souvisejícími finančními náklady na zřízení, provoz a údržbu sítě. Uvedené charakteristiky pak generují i specifické vlastnosti WPAN z pohledu bezpečnosti.

Mluví-li se o WPAN jako o bezdrátové osobní síti, tak jde v zásadě o označení zaměnitelné s termínem pro *osobní síť* (*PAN*, *Personal Area Network*), neboť téměř vždy je využito *bezdrátové přenosové médium* - typicky *rádiové*, příp. *infračervené*. Určitou podmnožinou WPAN jsou tzv. *bezdrátové tělesné sítě* (*WBAN*, *Wireless Body Area Network*) [44], které používají jako přenosové médium *lidské tělo*. WBAN propojuje senzory, čipy a další zařízení, která jsou k tělu nebo oblečení člověka připojena, příp. do něj přímo implantována. V této souvislosti se lze setkat i s konflikty v terminologii, kdy některé publikace a jejich autoři za WPAN považují výhradně ty sítě, které se jinak běžně označují právě jako WBAN.

Pracovní skupina IEEE 802.15 vytvořila několik samostatných standardů pro WPAN, které se vzájemně liší zejména *rychlostí přenosu dat*, *podporou QoS* a *energetickou náročností*. Základní přehled a charakteristiku norem uvádí tab. 4.1. Vzhledem k odlišným rysům i z bezpečnostního hlediska je jejich další výklad v této kapitol proveden odděleně.

Tabulka 4.1: Standardy pro WPAN vytvořené pracovní skupinou IEEE 802.15

Standard	**Rok**	**Popis**
802.15.1	2002	norma pro WPAN založená na specifikaci Bluetooth 1.1
802.15.2	2003	zabývá se koexistencí WPAN s jinými bezdrátovými sítěmi
802.15.3	2003	standard pro vysokorychlostní WPAN (známé jako WiMedia)
802.15.4	2003	WPAN s nízkou propustností a spotřebou energie (základ ZigBee)
802.15.5	–	doporučení pro využití smyčkové topologie (Mesh) ve WPAN

4.1 IEEE 802.15.1

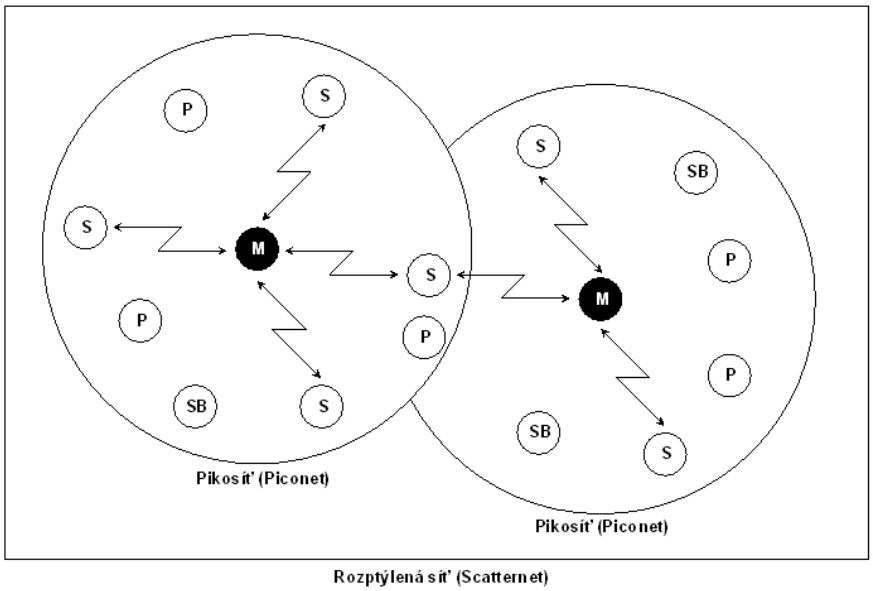
Pracovní skupina ***IEEE 802.15.1*** vznikla roku 1998, aby vytvořila specifikaci pro WPAN založenou na technologii ***Bluetooth***[1], původně vyvinutou v roce 1994 společností Ericsson a od roku 1998 spravovanou konzorciem *Bluetooth Special Interest Group* (*Bluetooth SIG*). První verze normy IEEE 802.15.1 [45], schválená roku 2002, vychází ze specifikace Bluetooth verze 1.1. V současné době je Bluetooth velmi rozšířenou technologií, jež nachází uplatnění při propojování nejrůznějších typů zařízení (osobní počítače, PDA, mobilní telefony, domácí spotřebiče, ...) na krátkou vzdálenost.

4.1.1 Architektura WPAN podle normy IEEE 802.15.1

Standard IEEE 802.15.1 však nelze zcela zaměňovat se specifikací Bluetooth, poněvadž z ní přejímá jen tu část architektury, která se zaměřuje na definici linkové a fyzické vrstvy.

Topologie

IEEE 802.15.1 umožňuje jak topologii *jednobodovou* (*PTP*, *Point-To-Point*), určenou pro přímou komunikaci dvou zařízení, tak i *vícebodovou* (*PTMP*, *Point-To-MultiPoint*), která má podobu tzv. *pikosítě* (*Scatternet*), viz obr. 4.1. Zařízení, které se v dané fyzické oblasti aktivuje jako první, plní roli *hlavní stanice* (*M*, *Master*), jež může simultánně obsloužit až sedm *podřízených stanic* (*S*, *Slave*), přičemž přes hlavní stanici je směrován veškerý provoz v rámci pikosítě. Mnoho dalších zařízení (do 200) může být buď *neaktivních* (*P*, *Parked*), nebo uvedených do *režimu spánku* (*SB*, *Stand-By*). Pikosítě se mohou překrývat a vytvářet tak tzv. *rozptýlené sítě* (*Scatternet*), přičemž každá pikosíť disponuje právě jednou hlavní stanicí, avšak podřízené stanice mohou být začleněny do několika různých pikosítí současně. Navíc jedno zařízení může v jedné pikosítí představovat hlavní stanici a v některé jiné být současně stanicí podřízenou.



Obrázek 4.1: Vícebodová topologie WPAN 802.15.1

[1] přezdívka krále Haralda II - *Blatand* ("*modrý zub*" podle jeho záliby v borůvkách a ostružinách) [46]

MAC podvrstva

Pro přístup k přenosovému médiu IEEE 802.15.1 používá techniku TDMA. MAC podvrstva implicitně nabízí *asynchronní spojení* (*ACL*, *Asynchronous Connection Less*) s *přepínáním paketů* a rychlým potvrzováním při vícebodovém uspořádání. Volitelně lze realizovat také *synchronní přenosy* (*SCO*, *Synchronous Connection Oriented*) založené na *přepínání okruhů*, které předcházejí opakovaným přenosům díky *zvýšení redundance přenášených dat* (*FEC*, *Forward Error Correction*). Jsou využívány při jednobodové topologii pro zajištění *QoS*.

Fyzická vrstva

WPAN IEEE 802.15.1 pracuje stejně jako WLAN IEEE 802.11b/g v pásmu ISM 2.4 GHz a využívá metodu rozprostřeného spektra FHSS (1600 proskoků/s, 79 různých kanálu o šířce 1 MHz v rozmezí 2402 až 2480 MHz), která byla kromě svého bezpečnostního významu vybrána především za účelem snížení pravděpodobnosti vzniku situace, kdy více než jedno ze zařízení vysílá ve stejném fyzickém prostoru na shodné frekvenci. Posloupnost frekvenčních proskoků určuje ten uzel, jenž plní roli hlavní stanice. Podřízené stanice se pak musejí odpovídajícím způsobem synchronizovat. Pro separaci vysílání a příjmu se využívá časového duplexu (TDD).

Přenosové rychlosti na fyzické vrstvě dosahují až 1 Mbit/s, avšak reálně dosažitelná propustnost je u nespojovaných přenosů omezena hodnotou 433.9 kbit/s (symetricky), resp. 732.2 / 57.6 kbit/s (asymetricky), v případě spojovaných přenosů je to 64 kbit/s. Dosah je u sítí WPAN IEEE 802.15.1 závislý na *třídě zařízení*: *třída 1* (100 mW) - do 100 m; *třída 2* (2.5 mW) - do 10 m; *třída 3* (1mW) - 0.1 až 10 m. Není přitom vyžadována přímá viditelnost mezi rádiovým vysílačem a přijímačem.

Revize původní normy

Zatímco původní norma *IEEE 802.15.1-2002* byla založena na specifikaci *Bluetooth 1.1*, o tři roky později organizace IEEE vydala její kompletní revizi, která bývá běžně uváděna pod označením *IEEE 802.15.1-2005* [47] a vychází ze specifikace *Bluetooth 1.2*. Změny se týkají zejména řízení toku dat, detekce chyb, synchronních přenosů dat a rychlosti ustavení spojení. Další významný prvek představuje zdokonalená technika rozprostřeného spektra ve formě *adaptivních frekvenčních proskoků* (*AFH*, *Adaptive Frequency Hopping*), zajišťující vyšší odolnost vůči rádiovým interferencím. Revize ale nepřináší žádné nové rysy ohledně bezpečnosti na linkové vrstvě.

4.1.2 Bezpečnostní model WPAN IEEE 802.15.1

Z bezpečnostních cílů WPAN IEEE 802.15.1 zajišťuje *autentizaci*, *autorizaci* a *důvěrnost*, specifikovány jsou dvě *úrovně důvěryhodnosti zařízení*, tři *bezpečnostní režimy* a tři *úrovně bezpečnosti služeb*.

Úrovně důvěryhodnosti zařízení

Na úrovní *důvěryhodnosti zařízení* norma rozlišuje *zařízení důvěryhodná* (*Trusted Device*) a *zařízení nedůvěryhodná* (*Untrusted Device*). Důvěryhodné zařízení je takové zařízení, které je autentizováno a disponuje neomezeným přístupem ke všem, příp. vybraným službám. Nedůvěryhodným zařízením je naopak přístup ke službám určitým způsobem omezen, přestože jejich identita mohla být již dříve také ověřena.

Bezpečnostní režimy

Každé zařízení může v sítí IEEE 802.15.4 operovat v několika *bezpečnostních režimech*. *Režim 1* (*Security Mode 1*) je *nezabezpečený* a zařízení neiniciuje vůbec žádné bezpečnostní procedury. *Režim 2* (*Security Mode 2*) koresponduje s *bezpečností na úrovni služeb*, kdy zařízení iniciuje bezpečnostní procedury až po ustavení spojení (tzn. na vyšších vrstvách). *Režim 3* (*Security Mode 3*) představuje *bezpečnost na úrovni linkové vrstvy*, tzn. zařízení iniciuje bezpečnostní služby dříve, než je spojení sestaveno.

Bezpečnostní úroveň služeb

Jakmile je ustaveno spojení mezi zařízeními, lze volit tři různé úrovně *bezpečnosti služeb*. První z bezpečnostních úrovní umožňuje přidělení přístupu některému ze zařízení výhradně na základě *autorizační* procedury (*Authorization Required*). V případě druhé úrovně je nutná *autentizace* zařízení před připojením k aplikaci (*Authentication Required*). Třetí úroveň vyžaduje při přístupu k aplikaci zapnuté *šifrování* (*Encryption Required*).

4.1.3 Zabezpečení IEEE 802.15.1 na fyzické vrstvě

WPAN IEEE 802.15.1 využívá na fyzické vrstvě *FHSS*, což je jedna z technik rozprostřeného spektra. Ta samá technika byla použita i v prvním vydání standardu IEEE 802.11 z roku 1997. Přestože princip FHSS byl vysvětlen dříve v části 3.6.2, je nutné poukázat na některé její specifické vlastnosti v IEEE 802.15.1.

Změna kmitočtu zde probíhá každých 625 mikrosekund, což snižuje možnost *odposlechu*, neboť za těchto podmínek je obtížné přítomnost aktivního zařízení vůbec detekovat. Navíc při krátkém dosahu WPAN (nejčastěji do 10 metrů) a možnosti regulovat vysílací výkon lze případné narušitele daleko snadněji identifikovat. Nicméně zkušení útočníci jsou schopni za pomoci antén se silnými směrovými charakteristikami zachytit signál i z větších vzdáleností a synchronizovat se s použitou sekvencí frekvenčních proskoků. Navíc řízení vysílacího výkonu je volitelné a ne každé zařízení tuto možnost nutně podporuje. Proto FHSS má v případě IEEE 802.15.4 primární bezpečnostní význam spíše při obraně vůči úmyslným interferencím (tj. *jammingu*) pro zajištění *dostupnosti* a *integrity* přenosu dat, než jako opatření zamezující odposlechu a narušení *důvěrnosti*.

4.1.4 Zabezpečení IEEE 802.15.1 na linkové vrstvě

Linková vrstva je základní bezpečnostní platformou WPAN IEEE 802.15.1. Na této úrovni norma specifikuje *management klíčů*, *autentizaci* a *šifrování přenosu dat*.

Management klíčů

V standardu IEEE 802.15.1 je definováno schéma *managementu klíčů*, na jehož základě se kryptografické klíče generují, ukládají a distribuují. Proces managementu klíčů ale vyžaduje jednoznačnou identifikaci jednotlivých zařízení ve WPAN. Základním identifikátorem každé stanice je *adresa zařízení* (*BD_ADDR*). Dalším parametrem je *PIN* (*Personal Identification Number*). Adresa zařízení má délku 48 bitů a je veřejná. PIN je číslo s variabilní délkou, která se pohybuje v rozmezí 8 až 128 bitů, přičemž nejčastějším případem je čtyřmístná hodnota. PIN může buďto zadávat vlastník zařízení, nebo přímo výrobce (méně časté, pouze u zařízení s minimálními paměťovými prostředky a uživatelským rozhraním). Každé zařízení má navíc *generátor náhodných čísel*, který se uplatňuje při odvozování klíčů.

IEEE 802.15.1 aplikuje symetrickou kryptografii s bezpečností založenou na sdílení klíčů. Pro účely ***autentizace*** jsou definovány čtyři 128-bitové ***linkové klíče*** (*Link Key*):

- ***Klíč zařízení*** (K_A, *Unit Key*) - vygeneruje se při instalaci zařízení algoritmem E_{21}. Jeho parametry jsou 128-bitové náhodné číslo a BD_ADDR stanice A. Používá se zejména při omezeném paměťovém prostoru.
- ***Kombinační klíč*** (K_{AB}, *Combination Key*) - unikátní klíč pro pár zařízení (A a B). Generuje se stejně jako klíč zařízení algoritmem E_{21} (parametry šifry jsou odvozeny z náhodných čísel a BD_ADDR obou zařízení).
- ***Hlavní klíč*** (K_{master}, *Master Key*) - tento klíč používá hlavní stanice (Master) pro skupinové (broadcastové) vysílání. Hlavní klíč je generován pomocí algoritmu E_{21} (vstupem jsou dvě náhodná čísla o délce 128-bitů).
- ***Inicializační klíč*** (K_{init}, *Initialization Key*) - uplatňuje se v inicializačním procesu při ochraně přenášených parametrů. Vytváří se stejně jako hlavní klíč algoritmem E_{21}, a to na základě náhodného čísla (128 bitů), hodnoty PIN, která musí být stejná u obou zařízení, a BD_ADDR iniciující stanice.

Jednotlivé typy linkových klíčů mají různou *životnost*. Hlavní klíč je *dočasný* a jeho doba platnosti je omezena na jednu relaci, klíč zařízení a kombinační klíč jsou klíči *trvalými* (uloženy v paměti nezávislé na napájení). Inicializační klíč je *jednorázový* a použije se jen jedenkrát při inicializaci daného spojení. Pro zabezpečení vlastního přenosu dat slouží ***šifrovací klíč*** (K_c) s délkou 8 až 128 bitů. Odvozuje se z aktuálně používaného linkového klíče algoritmem E_3.

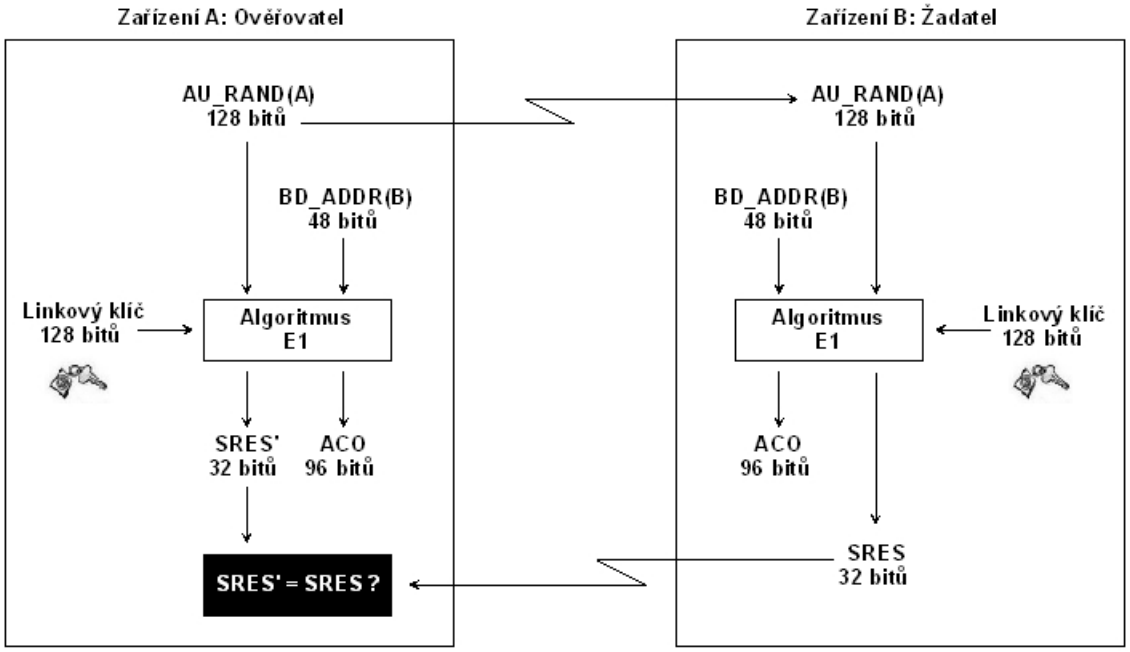
Celý *bezpečnostní proces* IEEE 802.15.1 se skládá z několika fází. Jako první ze všech je vygenerován klíč zařízení (při instalaci), následuje zadání PIN. Dále jsou generovány inicializační klíče, probíhá vygenerování a výměna ostatních linkových klíčů, autentizace, odvození šifrovacího klíče v každém zařízení a vlastní (šifrovaná) komunikace.

Autentizace

Autentizační proceduru IEEE 802.15.1 řídí schéma *výzva-odpověď* (*Challenge-Response*). Zařízení prokazující svoji identitu norma nazývá *žadatelem* (*Claimant*), zařízení provádějící kontrolu identitu je pak označováno jako *ověřovatel* (*Verifier*). Ověřovatelem přitom nemusí být nutně pouze hlavní stanice (Master), což podporuje mechanismus vzájemné autentizace při výměně rolí žadatele a ověřovatele.

Průběh autentizačního procesu zachycuje obr. 4.2. Na straně *ověřovatele* (*zařízení A*) i *žadatele* (*zařízení B*) jsou algoritmem E_1[2] pomocí sdíleného *linkového klíče*, *adresy zařízení žadatele* (*BD_ADDR(B)*) a *náhodného čísla* (*AU_RAND(A)*), které bylo vygenerováno ověřovatelem a následně zasláno žadateli, vytvořeny hodnoty *SRES* (*Signed RESponse*) a *ACO* (*Authenticated Ciphering Offset*), přičemž druhý výstupní parametr se uplatňuje až po skončení autentizace při generování šifrovacího klíče. Žadatel doručí vlastní SRES ověřovateli, který provede porovnání se svým výsledkem výpočtu (*SRES'*), kdy rovnost obou 32-bitových čísel indikuje úspěšnou autentizaci. V opačném případě lze autentizaci opakovaně iniciovat až po určité časové prodlevě, jejíž délka roste exponenciálně s každým dalším neúspěšným pokusem. Při absenci negativních výsledků autentizace se naopak časový interval exponenciálně zkracuje jako preventivní bezpečnostní opatření vůči *DoS* útokům.

[2] šifra E_1 i algoritmy E_{21}, E_{22} a E_3 využívají šifru *SAFER+* (*Secure And Fast Encryption Routine*)



Obrázek 4.2: IEEE 802.15.1 - autentizace

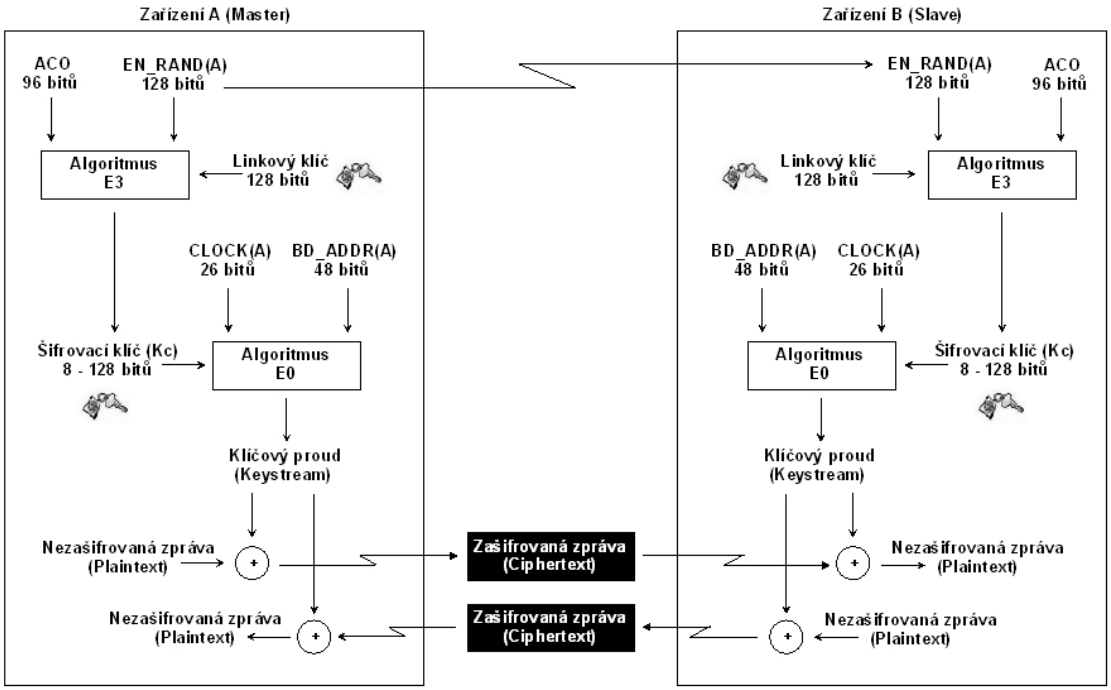
Šifrování přenosu dat

WPAN IEEE 802.15.1 zajišťuje *důvěrnost* přenosu dat proudovou šifrou E_0 (viz obr. 4.3). Algoritmus E_0 pracuje na bázi speciálního *posuvného registru s lineární zpětnou vazbou* (*LFSR*, *Linear Feedback Shift Register*), který patří mezi běžně používaná kryptografická schémata. Pro vygenerování výstupního *klíčového proudu* (*Keystream*) vyžaduje šifra E_0 sdílený *šifrovací klíč* (K_c) o délce 8-128 bitů, 48-bitovou *adresu zařízení hlavní stanice* (*BD_ADDR(A)*) a jako poslední parametr 26 bitů *hodinového signálu* (*BD_ADDR(A)*). Hodinový signál inkrementuje hlavní stanice s každým slotem. Aplikací operace *XOR* na *klíčový proud* a *nezašifrovanou zprávu* (*Plaintext*) vznikne *zašifrovaná zpráva* (*Ciphertext*).

Algoritmus E_0 je symetrickou šifrou a proto proces *dešifrování* na straně příjemce probíhá zcela totožné jako šifrování. Při operaci XOR se vygenerovaný klíčový proud použije na zašifrovanou zprávu. Generování klíčového proudu probíhá stejně jako u odesilatele. Příjemce musí znát adresu odesilatele (*BD_ADDR(A)*), tzn. adresu hlavní stanice, a část hodinového signálu, který hlavní stanice generuje. Vlastní *šifrovací klíč* je vytvořen na obou stranách algoritmem E_3 za použití *náhodného čísla hlavní stanice* (*EN_RAND(A)*), *linkového klíče* a *ACO* (odvozen při autentizaci). Šifrování přenosu dat je v IEEE 802.15.1 implicitně vypnuto, jinak lze zabezpečovat buď veškerou, nebo jen unicastovou komunikaci (tzn. broadcastové rámce nepodléhají šifrování).

4.1.5 Problémy v zabezpečení IEEE 802.15.1

IEEE 802.15.1 v sobě obsahuje značný počet bezpečnostních slabin a nedostatků [15, 48, 49]. Ty nejdůležitější z nich uvádí v závěru této části tab. 4.2. V dalším textu jsou navíc popsány typické útoky na zařízení využívající technologii Bluetooth. Jde o útoky, které jsou relativně snadno uskutečnitelné a vycházejí z praktických zkušeností, nikoliv teoretických analýz. Nejčastější obětí jsou přitom mobilní telefony a jejich uživatelé.



Obrázek 4.3: IEEE 802.15.1 - šifrování přenosu dat

Specifickými útoky na Bluetooth [50, 51, 52] jsou:

- ***Bluejacking*** - zaslání nevyžádané zprávy určitému zařízení (typicky mobilní telefon). Přestože není narušena integrita uložených dat, opakované doručování zpráv může představovat jistou formou *DoS* útoku. Další aspekty spočívají v sociálních dopadech.
- ***Bluebugging*** - vykonávání neautorizovaných činností prostřednictvím napadeného zařízení, kterým je nejčastěji opět mobilní telefon. Mezi akce prováděné útočníky tak patří iniciace telefonních hovorů, odesílání a přijímání textových zpráv, odposlech uskutečněných volání, připojování k Internetu apod.
- ***Bluesnarfing*** - neautorizovaný přístup k datům v zařízení. U mobilního telefonu může být předmětem útoku např. seznam kontaktů, kalendář, ale i identita mobilního účastníka.
- ***Blueprinting*** - cílem útoku je zjistit co nejvíce technických informací o konkrétním zařízení. Unikátní adresa každého zařízení se skládá z šesti bytů, kdy první tři označují výrobce, ostatními byty je specifikována modelová řada, jejíž identifikace však není zcela jednoznačná.
- ***BlueDump*** - útočník provede krádež adresy jednoho z dvojice spárovaných zařízení a připojí se k druhému. Jelikož útočník nezná sdílený linkový klíč, na požadavek o autentizaci odpoví takovým způsobem, že dojde v některých případech k vymazání linkového klíče cílového zařízení a bude vynuceno zahájení inicializační fáze (párování).
- ***BlueChop*** - rozvrácení ustavené pikosítě zařízením, které není součástí WPAN.

Další útoky, jako ***BlueSmack***, ***BlueSnarf++***, ***BlueBump*** a ***Backdoor***, popisuje [53].

Tabulka 4.2: Bezpečnostní slabiny IEEE 802.15.1

- implicitně jen jednostranná autentizace typu výzva-odpověď, prostor pro MITM útoky
- při autentizaci se prověřuje pouze identita zařízení a nikoliv uživatele
- rostoucí časová prodleva při neúspěšných autentizacích může být cílem DoS útoků
- příliš krátký PIN (typicky čtyřmístné číslo), obvykle manuální konfigurace (slabý PIN)
- chybí specifikace generátoru náhodných čísel (riziko statických/periodických hodnot)
- hlavní klíč pro zabezpečení broadcastového provozu je sdílený
- opakované použití klíče zařízení - po prvním použití se stává veřejně dostupným
- inicializační klíč je slabý (odvozen z PIN, náhodného čísla a adresy zařízení)
- slabé zajištění důvěrnosti přenosu dat proudovou šifrou E_0
- šifrování přenosu dat je při implicitním nastavení nepoužito
- délka šifrovacího klíče je variabilní (8 až 128 bitů) a závisí na dohodě komunikujících
- inicializační vektor algoritmu E_0 nezávisí na celém hodinovém signálu (jen 26 bitů)
- nedostatečné zajištění integrity přenášených dat (pouze CRC)
- žádné bezpečnostní mechanismy zabraňující útokům opakovaným přenosem
- omezená úroveň zabezpečení vyžaduje bezpečnostní mechanismy na vyšších vrstvách
- každé zařízení má unikátní a veřejně známou adresu - riziko sledování uživatelů

4.2 IEEE 802.15.2

Norma ***IEEE 802.15.2*** [54] je v této kapitole uvedena jen pro úplnost, neboť nespecifikuje žádný z typů WPAN a nemá žádný bezpečnostní význam. Standard byl schválen v roce 2003 jako doporučený model pro *koexistenci* WPAN IEEE 802.15 a jiných bezdrátových sítí, především WLAN IEEE 802.11, které operují v nelicencovaných frekvenčních pásmech. V současné době nevyvíjí pracovní skupina IEEE 802.15.2 žádnou aktivitu.

4.3 IEEE 802.15.3

Vysokorychlostní WPAN s *nízkou spotřebou* specifikuje norma ***IEEE 802.15.3*** [55], která byla schválena v roce 2003. Ve srovnání s IEEE 802.15.1 mají WPAN IEEE 802.15.3 výrazně vyšší datovou propustnost a jsou optimalizovány na kratší vzdálenosti. Aplikace tak nacházejí především v oblasti multimediálních přenosů. Rozvoj IEEE 802.15.3 podporuje neziskové průmyslové sdružení *WiMedia Alliance* (`www.wimedia.org`). Proto se technologie IEEE 802.15.3 také někdy označuje jako ***WiMedia***.

4.3.1 Architektura WPAN podle normy IEEE 802.15.3

V dalším je stručně popsána topologie a linková a fyzická vrstva WPAN IEEE 802.15.3.

Topologie

IEEE 802.15.3 využívá stejnou topologii jako IEEE 802.15.1, tzn. síť pracuje v *ad-hoc* režimu, kdy základní stavební jednotku tvoří *pikosíť*. Komunikaci *zařízení* (*DEV*, *DEVice*) v pikosíti řídí jedna ze stanic, tzv. *koordinátor* (*PNC*, *PicoNet Coordinator*).

Linková vrstva

Linková vrstva IEEE 802.15.3 zajišťuje QoS, efektivitu přenosů, rychlou inicializaci spojení, podporu ad-hoc režimu, dynamičnost pikosítí a autentizaci a zabezpečení přenosu dat. Stejně jako IEEE 802.15.1 používá pro vícenásobný přístup techniku TDMA.

Fyzická vrstva

Na fyzické vrstvě WPAN IEEE 802.15.3 podle původního standardu z roku 2003 pracuje v pásmu ISM 2.4 GHz, které sdílí mj. se sítěmi IEEE 802.15.1 a IEEE 802.11b/g. Spektrum je rozděleno na pět kanálu po 15 MHz, přičemž tři frekvenční úseky jsou vyhrazeny pro zamezení kolizí s WLAN IEEE 802.11. K dispozici je pět různých přenosových rychlostí s použitím *Trellisova kódování* (*TCM*, *Trellis Coded Modulation*) a pěti typů modulací (11 Mbit/s: QPSK, 22 Mbit/s: DQPSK, 33 Mbit/s: 16QAM, 44 Mbit/s: 32QAM a 55 Mbit/s: 64QAM), přičemž nejvyšší z uvedených rychlostí lze dosáhnout při vzdálenosti až 50 metrů. Při 100 metrech se propustnost snižuje na 22 Mbit/s.

Doplňky normy IEEE 802.15.3

Další zdokonalení přinášejí později vydané doplňky normy (viz tab. 4.3). *IEEE 802.15.3a* zavádí *ultraširokopásmové přenosy* pomocí technologie *UWB* (*Ultra Wide Band*). Využívá pásmo 3.1 až 10.6 GHz s maximální dosažitelnou rychlostí 480 Mbit/s (do 1 m). Ještě výrazně vyšší datovou propustnost (více než 2 Gbit/s) přinese doplněk *IEEE 802.15.3c*.

Tabulka 4.3: Doplňky původní normy IEEE 802.15.3

Standard	Rok	Popis
802.15.3a	2004	UWB 3.1-10.6 GHz, 110 Mbit/s (do 10 m) až 480 Mbit/s (do 1 m)
802.15.3b	2005	revize MAC podvrstvy (optimalizace, vyšší interoperabilita, ...)
802.15.3c	2009?	tzv. Millimeter Wave WPAN, 57-64 GHz, více než 2 Gbit/s

4.3.2 Zabezpečení IEEE 802.15.3

Specifika zabezpečení IEEE 802.15.3 ve srovnání s odlišnými standardy pro WPAN i jinými typy bezdrátových sítí obecně lze pozorovat především na úrovni ***fyzické vrstvy*** v podobě technologie *UWB*, která je využitelná počínaje rokem 2004 díky doplňku IEEE 802.15.3a. *Ultraširokopásmové přenosy* jsou využívány již několik desetiletí pro vojenské účely a jejich princip spočívá v rozložení signálu do velmi širokého spektra takovým způsobem, že jsou vysílány krátké pulsy, které zůstávají pod výkonovou úrovní, jež je v jednotlivých dílčích pásmech definována jako šum. To činní *jamming* a *odposlech* velmi obtížnými, poněvadž takový signál lze jen stěží detekovat a odlišit od šumu.

Nicméně pro zkušené útočníky, kteří disponují potřebnými znalostmi a vybavením, není zcela nemožné UWB signál v blízkosti vysílače zachytit. Proto neztrácejí na významu ani bezpečnostní mechanismy na ***linkové vrstvě***. *Autentizace* se řídí protokolem *výzva-odpověď* (stejný mechanismus jako u IEEE 802.15.1), je však implementována *ochrana vůči útokům opakovaným přenosem* (náhodná čísla). *Důvěrnost* a *integrita* přenosu dat je zajištěna šifrováním pomocí algoritmu *AES* se 128-bitovým klíčem.

4.4 IEEE 802.15.4

IEEE 802.15.4 je standardem zastupujícím tzv. *LR-WPAN* (*Low Rate WPAN*), což jsou bezdrátové osobní sítě charakteristické především *malou přenosovou rychlostí*, *minimální energetickými nároky* a *nízkými náklady*. Mezi další rysy patří vysoká spolehlivost, malá latence, minimální podpora QoS, možnost vytváření statických síťových struktur, vysoká hustota síťových uzlů a schopnost plnit svoji funkci dlouhodobě bez zásahu člověka. Celkově jde o jednoduchou a flexibilní technologii, jež je optimalizována pro přenosy v malém objemu mezi mobilními, přenosnými i pevnými zařízeními.

Z výše uvedených charakteristik vyplývá, že IEEE 802.15.4 splňuje typické požadavky kladené na tzv. *bezdrátové senzorové sítě* (*WSN*, *Wireless Sensor Network*), které svoje uplatnění nacházejí v domácnostech (bezdrátové vypínače, termostaty, alarmy, ...), medicíně (sledování zdravotního stavu pacienta), ekologii (automatizované monitorování a sběr dat o stavu životního prostředí), průmyslu (automatizace), spotřební elektronice (komunikace spotřebičů, dálkové ovládání zařízení), ale i v oblasti vojenských a bezpečnostních aplikací. IEEE 802.15.4 však nepředstavuje konkurenční technologii pro ostatní typy WPAN ani např. pro WLAN, poněvadž tyto sítě nejsou pro realizaci WSN vhodné vzhledem k jejich vysoké složitosti, spotřebě energie a finanční nákladnosti.

4.4.1 Architektura WPAN podle normy IEEE 802.15.4

Norma IEEE 802.15.4 [56, 57], dokončená roku 2003, je základem technologie ***ZigBee***[3], jejíž vývoj a propagaci podporuje průmyslové konsorcium *ZigBee Alliance* (`www.zigbee.org`). Stejně jako v případě IEEE 802.15.1 a Bluetooth ale nejde o dva totožné standardy, neboť IEEE 802.15.4 definuje výhradně fyzickou a linkovou vrstvu (jako všechny ostatní bezdrátové standardy třídy IEEE 802). Specifikace ZigBee pak zahrnuje i vyšší vrstvy.

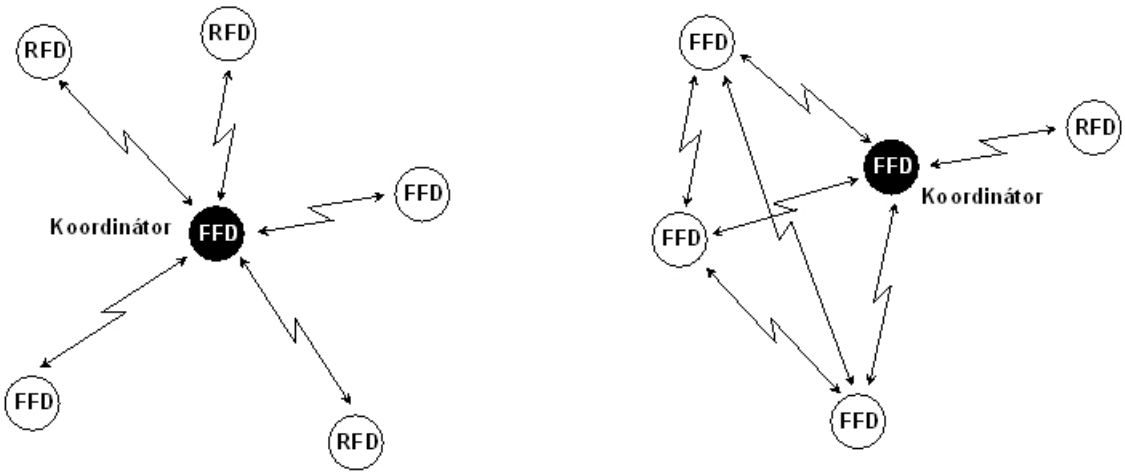
Topologie

V závislosti na požadavcích konkrétní aplikace umožňuje WPAN IEEE 802.15.4 dvě základní topologie (viz obr. 4.4): *hvězdu* (*Star*) a *přímé propojení* (*Peer-To-Peer*). Uzly sítě mohou být přitom zařízení dvou typů: *zařízení s plnou funkčností* (*FFD*, *Full Function Device*), jimž je umožněna vzájemná komunikace se zařízeními obou kategorií, a *zařízení s omezenou funkčností* (*RFD*, *Reduced Function Device*), která mají možnost navazovat spojení pouze se zařízeními s plnou funkčností. Činnost WPAN, příp. její části, řídí vždy jeden *koordinátor* (*PAN Coordinator*), kterým může být pouze zařízení FFD. V hvězdicové topologii mohou zařízení přímo komunikovat pouze s koordinátorem, v druhém případě je dovolena i přímá komunikace mezi jednotlivými uzly s přihlédnutím k výše uvedeným omezením. Topologie s přímým propojením navíc umožňuje vznik dalších, složitějších uspořádání, jako je *strom* (*Cluster Tree*) a síť se *smyčkovou topologií* (*Mesh*).

MAC podvrstva

MAC podvrstva IEEE 802.15.4 je velmi jednoduchá. Zajišťuje přenosy datových rámců (*Data Frame*), potvrzování přijetí (*Acknowledgement Frame*), centralizovanou konfiguraci (*MAC Command Frame*) a synchronizaci (*Beacon Frame*). Pro přístup k fyzickému médiu je implementována metoda CSMA/CA.

[3] název inspirován technikou komunikace včel (*Bee*) ve formě zvláštního, zmateného tance (*Zig-Zag*) [58]



Obrázek 4.4: Topologie IEEE 802.15.4: hvězda (vlevo) a přímé propojení (vpravo)

Fyzická vrstva

Norma specifikuje tři rádiová frekvenční pásma. V globálním měřítku je předpokládáno použití mezinárodního pásma ISM 2.4 GHz s 16 kanály, modulací O-QPSK a maximální kapacitou 250 kbit/s. Pro americký kontinent je určeno spektrum 915 MHz s 10 kanály a přenosovou rychlostí 40 kbit/s. V Evropě je to pásmo 868 MHz s 1 kanálem a datovou propustností 20 kbit/s. Ve všech pásmech se využívá rozprostřeného spektra, konkrétně technika DSSS. Dosah se dle operačního prostředí pohybuje v rozmezí 10 až 75 metrů.

Doplňky standardu IEEE 802.15.4

K prvnímu vydání normy IEEE 802.15.4 z roku 2003 vznikly zatím pouze dva doplňky, které jsou uvedeny v tab. 4.4. První dokončený doplněk, *IEEE 802.15.4b*, byl schválen v roce 2006 jako důkladná revize původní normy. Revize se běžně označuje jako standard *IEEE 802.15.4-2006*. Druhý z doplňků, *IEEE 802.15.4a*, dosud schválen nebyl. Přináší ale zásadní změny na úrovni fyzické vrstvy, což se týká především technologie UWB, která se používá v sítích IEEE 802.15.3.

Tabulka 4.4: Doplňky normy IEEE 802.15.4

Standard	Rok	Popis
802.15.4a	2007	fyzické vrstvy (UWB, CSS) s vyšší kapacitou a menším příkonem
802.15.4b	2006	revize původní normy (oprava chyb, efektivnější, nižší složitost, ...)

4.4.2 Zabezpečení IEEE 802.15.4

Tato část se primárně zaměřuje na bezpečnostní mechanismy definované přímo normou IEEE 802.15.4, tzn. na zabezpečení senzorových sítí na úrovni linkové a fyzické vrstvy. V závěru je však nastíněna i problematika zabezpečení WPAN na vyšších vrstvách síťové architektury, které specifikuje standard ZigBee.

Obecná bezpečnostní specifika senzorových sítí

Senzorové sítě jsou specifické velmi *omezenými výpočetními*, *paměťovými*, *energetickými* a *komunikačními prostředky*. Proto je nezbytné velmi pečlivě volit takové bezpečnostní mechanismy, které budou dostupné zdroje využívat co možná nejefektivnějším způsobem a současně zaručí dostatečnou úroveň zabezpečení. Navíc útočníci mohou soustředit svoje útoky na vyčerpání takto omezených zdrojů s následkem nedostupnosti celé sítě.

Další zásadní aspekt představuje *operační prostředí* senzorové sítě, které silně závisí na aplikační oblasti a funkci, kterou v ní má plnit. Nezřídka jde přitom o velmi obtížně dostupné a nehostinné, příp. přímo nepřátelské prostředí s vysokým rizikem fyzického útoku a selhání zařízení. Extrémním případem jsou špionážní senzorové sítě, po jejichž vytvoření není možný další fyzický kontakt mezi jejími uzly a entitou, které sít slouží.

Bezpečnostní režimy IEEE 802.15.4

Norma definuje několik úrovní zabezpečení, které se liší svými bezpečnostními mechanismy. ***Bezpečnostními režimy IEEE 802.15.4*** jsou:

- ***Nezabezpečený režim*** (*Unsecured Mode*) - implicitní úroveň zabezpečení, která neposkytuje vůbec žádné bezpečnostní služby;
- ***Režim s přístupovými seznamy*** (*ACL Mode*) - tento režim nezajišťuje žádnou kryptografickou ochranu, kdy zařízení přijímají rámce pouze od těch zařízení, které mají uvedeny ve vlastním *přístupovém seznamu* (*ACL*, *Access Control List*);
- ***Zabezpečený režim*** (*Secured Mode*) - nabízí zabezpečení na základě algoritmu AES a v závislosti na operačním režimu šifry (AES-CTR, AES-CCM nebo AES-CBC) zajišťuje podmnožinu následujících bezpečnostních cílů: *řízení přístupu*, *důvěrnost*, *integrita* a *aktuálnost* přenosu dat.

Implementace nastavitelných úrovní zabezpečení v podobě volitelných bezpečnostních módů je zcela běžná i v jiných počítačových sítích, a to i jiných než bezdrátových. Ovšem v případě senzorových sítí, a tedy i WPAN IEEE 802.15.4, mají tyto mechanismy ještě výrazně vyšší přínos vzhledem k omezeným výpočetním, paměťovým, energetickým a komunikačním zdrojům. V závislosti na aplikačních požadavcích a mnoha odlišných fyzických prostředích, v nichž mohou být senzorové sítě nasazeny a které se liší závažností svých hrozeb, a operačním prostředí WPAN lze pak efektivně volit úroveň zabezpečení a optimalizovat čerpání dostupných prostředků.

Zabezpečení IEEE 802.15.4 na fyzické vrstvě

Jediným bezpečnostním mechanismem, který je specifikován přímo normou IEEE 802.15.4 na úrovni fyzické vrstvy, je *DSSS* jako technika *rozprostřeného spektra*. Obranný význam metod rozprostřeného spektra vůči *odposlechu* a *jammingu* byl několikrát zmíněn již v rámci předchozích kapitol, a to především jako součást výkladu zabezpečení WLAN IEEE 802.11 (viz část 3.6.2). Mimoto lze uplatňovat také obecně platná opatření pro zabezpečení rádiové komunikace, jako je regulace vysílacího výkonu a zamezení šíření rádiového signálu do nežádoucích fyzických oblastí. Zde se riziko jak záměrných, tak i neúmyslných rádiových interference navíc dále zvyšuje vzhledem ke skutečnosti, že všechna tři *frekvenční pásma* (868 MHz, 915 MHz a 2.4 GHz) vyhrazená pro IEEE 802.15.4 jsou *nelicencovaná*. Regulační orgány tak nemohou proti narušitelům účinně postupovat.

Specifické útoky na senzorové sítě se zaměřují na *vyčerpání omezených zdrojů* s důsledkem nedostupnosti WPAN. Vzhledem k operačnímu prostředí WPAN, které může být v řadě případů obtížně dostupné a v některých případech i přímo nepřátelské, představují vážnou hrozbu útoky na *fyzickou integritu* jednotlivých komponent WPAN. Jejich cílem bývá opět ohrožení dostupnosti, ale i získání důvěrných dat (včetně kryptografických klíčů apod.) uložených v jednotlivých uzlech, popř. modifikace funkce zařízení. Jedinou obranou vůči uvedeným útokům jsou účinná fyzická bezpečnostní opatření. Přestože význam fyzických bezpečnostních opatření je u senzorových sítí značný, jejich popis přesahuje rámec práce.

Zabezpečení IEEE 802.15.4 na linkové vrstvě

Linková vrstva IEEE 802.15.4 je zabezpečena univerzální symetrickou šifrou *AES*, kterou mj. používají bezdrátové sítě IEEE 802.11 (doplněk IEEE 802.11i), IEEE 802.16 a také IEEE 802.15.3. Management kryptografických klíčů norma nespecifikuje, jelikož ponechává tuto roli procesům vyšších vrstev. Zajištění *integrity* a *důvěrnosti* šifrováním algoritmem AES se vztahuje na *datové*, *řídicí* a *synchronizační* rámce, ale nikoli na informace potvrzující správné přijetí rámců (viz část 4.4.1). Mezi ostatní poskytované bezpečnostní služby patří *autentizace* a *aktuálnost dat*. WPAN IEEE 802.15.4 nabízí na linkové vrstvě několik stupňů zabezpečení, které korespondují s ***režimy šifry AES***:

- ***AES-CTR*** zajišťuje *důvěrnost* a *aktuálnost* přenášených dat. Odesílaná zpráva je rozdělena na *bloky* o velikosti 16 bytů, šifrování se provádí aplikací operace *XOR* na jednotlivé bloky nezašifrované zprávy a výstup algoritmu AES, který je generován na základě sdíleného klíče a *čítače*. Čítač plní roli *inicializačního vektoru* a je složen z *adresy odesilatele* (64 bitů), statické *výplně* (8 bitů) a tří *dílčích čítačů*: *čítače rámce* (32 bitů), *čítače klíče* (8 bitů) a *čítače bloku* (16 bitů). Všechny čítače jsou průběžně aktualizovány, přičemž k inkrementaci čítače klíče dochází tehdy, pokud čítač rámce dosáhne své maximální hodnoty. Dešifrování probíhá zcela analogicky (symetrická kryptografie). Příjemce může navíc volitelně zkontrolovat hodnoty čítačů a detekovat potencionální *útoky opakovaným přenosem* (rámce s hodnotou čítače nižší než uvedenou v záznamu příjemce se zahazují).

- ***AES-CBC-MAC*** je režimem, jenž zajišťuje *autenticitu* a *integritu* přenosu dat. Vstupní zpráva je rozdělena do *bloků* jako v případě AES-CTR s tím rozdílem, že při šifrování daného bloku se jako jeden ze vstupů používá zašifrovaný blok předchozí (u prvního bloku se uplatňuje *inicializační vektor*). Výsledkem ale není zašifrovaná zpráva, nýbrž *kryptografický kontrolní součet* (*MIC*, *Message Integrity Code*) o délce 32, 16 nebo 128 bitů, který se ke zprávě přenášené v otevřené podobě připojí. Příjemce pak provede kontrolu integrity a autenticity příchozí zprávy porovnáním v rámci uvedeného a explicitně vypočteného MIC.

- ***AES-CCM*** - kombinuje oba předchozí režimy, tzn. *AES-CTR* a *AES-CBC-MAC*. Ze vstupní zprávy (bere se v úvahu hlavička i vlastní data) je nejprve vypočtena hodnota MIC, v druhém kroku probíhá její šifrování v režimu AES-CTR. Režim AES-CCM tak zajišťuje současně *autenticitu*, *integritu* a *důvěrnost* dat i *ochranu vůči útokům opakovaným přenosem*.

Zabezpečení WPAN IEEE 802.15.1 na linkové vrstvě obsahuje několik zranitelných míst (viz tab. 4.5). Ty se ale netýkají šifry AES samotné. Hlavní problematické oblasti představují *správa inicializačních vektorů*, *management klíčů* a *zajištění integrity dat* [59, 60].

Tabulka 4.5: Problémy v zabezpečení IEEE 802.15.4 na linkové vrstvě

- riziko opětného použití inicializačního vektoru při výskytu klíče v různých ACL
- výpadek napájení způsobí vymazání seznamů přístupových práv a vynulování čítačů
- chybí podpora pro skupinové klíče, kdy určitá podmnožina uzlů sdílí jeden klíč
- při sdílení jednoho klíče všemi stanicemi nelze zamezit útokům opakovaným přenosem
- slabá podpora sdílení klíčů mezi dvojicí uzlů (není určen min. počet položek ACL)
- DoS útoky generováním explicitního provozu pro umělé zvyšování čítačů u příjemce
- šifrování přenášených dat se nevztahuje na potvrzovací rámce
- při použití režimu AES-CTR není vůbec zajištěna integrita a autenticita dat

Zabezpečení na vyšších vrstvách (ZigBee)

Specifikace *ZigBee* bývá někdy nesprávně zaměňována s normou IEEE 802.15.4 a přestože ZigBee přejímá definici dvou nejnižších vrstev architektury z normy IEEE 802.15.4, ne všechna zařízení implementující standard IEEE 802.15.4 jsou nutně kompatibilní s ZigBee. Nicméně ZigBee je ve své kategorii velmi rozšířenou technologií a má tedy smysl se v této souvislosti zabývat i zabezpečením senzorových sítí na vyšších vrstvách, a to *síťové* (*NWK*) a *aplikační* (*APL*), které specifikace ZigBee zahrnuje [61].

Nejdůležitější úlohou *síťové vrstvy* ZigBee je aplikace bezpečnostních mechanismů na rámce, správa dynamických změn v topologii WPAN (vložení/odebrání uzlu) a především směrování, přičemž jednu z nejzávažnějších hrozeb v senzorových sítích představují právě *útoky na směrovací protokoly*. *Aplikační vrstvu* tvoří *podpůrná aplikační podvrstva* (*APS*), *ZigBee objekty* (*ZDO*) a *uživatelské aplikační objekty*. APS udržuje párovací tabulky (pro párování zařízení dle poskytovaných služeb a požadavků) a také zodpovídá za přeposílání zpráv. ZigBee objekty specifikují roli zařízení (koordinátor/směrovač/koncové zařízení), provádějí vyhledávání zařízení a zajišťují správu poskytovaných služeb. Vlastnosti zařízení a jejich vzájemnou komunikaci charakterizují tzv. *ZigBee profily*, které jsou rozlišeny na základě unikátního 16-bitového identifikátoru. Z bezpečnostních opatření aplikační vrstvy se předpokládají zejména *IDS/IPS systémy*.

ZigBee využívá stejně jako norma IEEE 802.15.4 algoritmus *AES* se 128-bitovým klíčem. Operační režim CCM je však mírně modifikován (zjednodušen) a označuje se jako *CCM**. Narozdíl od IEEE 802.15.4 ale již zahrnuje definici a management kryptografických klíčů. Je zaveden pojem tzv. *důvěryhodného centra* (*Trust Center*), které řídí přístup zařízení do sítě a provádí distribuci klíčů. Je definován *důvěryhodný manažer* (*Trust Manager*) pro autentizaci, *síťový manažer* (*Network Manager*), který spravuje a distribuuje síťové klíče, a *konfigurační manažer* (*Configuration Manager*), jehož úkolem je podpora zabezpečení mezi koncovými body komunikace (*End-to-End*). Důvěryhodné centrum může pracovat ve dvou režimech. V *rezidentálním režimu* (*Residential Mode*) umožňuje zařízením přístup do sítě, ale už neprovádí ustavení a periodickou obnovu klíčů. Cílem je minimalizovat paměťové nároky a zamezit jejich nárůstu s rozšiřováním sítě. V *komerčním režimu* (*Commercial Mode*) je naopak centralizovaná distribuce a aktualizace kryptografických klíčů zajištěna, požadavky na paměť však mohou při expanzi WPAN vzrůstat. ZigBee používá tři základní *typy klíčů*: *hlavní* (*Master Key*), *linkový* (*Link Key*) a *síťový* (*Network Key*). Hlavní klíč se instaluje jako první a je určen pro dlouhodobé zabezpečení komunikace mezi dvěma zařízeními. Linkový klíč má kratší platnost, síťový klíč slouží pro globální zabezpečení sítě.

4.5 IEEE 802.15.5

Vývoj specifikace *IEEE 802.15.5* [62] probíhá od roku 2005. Nejde ale o standard definující další typ WPAN, nýbrž o doporučení pro využití *smyčkové topologie*, označované jako *Mesh*, v již existujících bezdrátových osobních sítích.

Smyčkové uspořádání nabízí jako alternativu také WMAN IEEE 802.16 (viz část 5.1.1). Přínosy smyčkové topologie spočívají v rozšíření pokrytí sítě bez zvýšení vysílacího výkonu a citlivosti přijímače, vyšší spolehlivosti díky redundanci při směrování, snazší konfiguraci a nižší energetické spotřebě a tím i vyšší životnosti sítě vzhledem k nižšímu počtu opakovaných přenosů. Uvedené charakteristiky mají velký význam i z pohledu *bezpečnosti*, poněvadž menší energetické požadavky zvyšují odolnost vůči *DoS* útokům a redundantní síťové cesty představují schopnost čelit dynamickým změnám v topologii WPAN, k nimž může docházet např. následkem *fyzické likvidace* některého zařízení. IEEE 802.15.5 plánuje podporu jak *plné* (každý uzel WPAN je propojen přímo se všemi ostatními uzly v dosahu), tak i *částečné* (některé uzly jsou propojeny jen s těmi uzly, s nimiž nejvíce komunikují) *smyčkové topologie*. Odpovídající anglické termíny jsou *Full Mesh Topology* a *Partial Mesh Topology*.

Kapitola 5

Zabezpečení WMAN IEEE 802.16

Bezdrátové metropolitní sítě (***WMAN***, ***Wireless Metropolitan Area Network***) jsou normalizovány podvýborem ***IEEE 802.16*** a představují efektivní technologii pro poskytování *širokopásmového bezdrátového přístupu* (*BWA*, *Broadband Wireless Access*). IEEE 802.16 se přitom považuje za zástupce již *druhé generace bezdrátového přístupu*, poněvadž vychází z původních telefonních *místních smyček* (*WLL*, *Wireless Local Loop*), které předcházely BWA a byly určeny pro přenos hlasu.

Práce na standardu IEEE 802.16 byla zahájena v roce 1999. První verze normy prošla ratifikací roku 2001, ale vzhledem k určitým jejím charakteristikám (viz část 5.1.3) se dočkala spíše kritického přijetí. Teprve po vydání několika dalších doplňků (viz část 5.1.4), které původní specifikaci výrazně revidují a obohacují o nové funkce, mezi něž mj. patří podpora mobility, norma dospěla do stavu, kdy mohly začít vznikat použitelné aplikace. Přestože rozšíření WMAN IEEE 802.16 není v současnosti ještě příliš výrazné a například s WLAN IEEE 802.11 zcela nesrovnatelné, představuje do budoucna velmi perspektivní řešení tzv. *poslední míle* jako alternativa k současným kabelovým a xDSL přípojkám.

Pro přístup k Internetu jsou v dnešní době často využívány i lokální bezdrátové sítě, ty ale nebyly původně navrženy a zamýšleny pro použití ve venkovním prostředí ani jako přístupová síť. WMAN pak WLAN výrazně technologicky překonává, především co se týká dosahu, přenosových rychlostí, mobility, zabudované podpory pro QoS, efektivity využívání kmitočtového spektra a v neposlední řadě také z hlediska bezpečnosti, přestože důkladnou bezpečnostní prověrkou těchto sítí bude teprve až jejich širší praktické nasazení. Ve svých cílech se však oba typy sítí výrazně neliší. V obou případech jsou charakteristické svou škálovatelností, flexibilitou, rychlou, snadnou a nenákladnou instalací i provozem. WMAN se ještě více zaměřuje na přenosy v reálném čase. Bezdrátové metropolitní sítě ale nepředstavují přímou náhradu WLAN, jak bývá někdy uváděno. Jejich role bude spočívat spíše v propojování místních lokálních sítí, mj. i tzv. *hotspots*, což jsou WLAN poskytující veřejný přístup k Internetu.

Podobně jako sítě IEEE 802.11 mají označení Wi-Fi a sdružení Wi-Fi Alliance, v případě IEEE 802.16 jde o zkratku ***WiMAX*** (*Worldwide Interoperability for Microwave Access*) a neziskovou organizaci *WiMAX Forum* (`www.wimaxforum.org`), jež byla založena v roce 2001 současně s ratifikací standardu IEEE 802.16. Provádí testování a certifikaci produktů podle normy, čímž zaručuje jejich vzájemnou interoperabilitu. Bezdrátovým zařízením splňujícím požadovaná kritéria uděluje označení "*WiMAX Forum Certified*".

Alternativou k IEEE 802.16 jsou normy *HIPERMAN* a *HIPERACCESS* institutu ETSI. Jejich význam lze ale přirovnat ke vztahu sítí HIPERLAN k WLAN IEEE 802.11, tzn. jsou technologicky, ale nikoli tržně srovnatelné. Mezi další patří např. technologie *WiBro*.

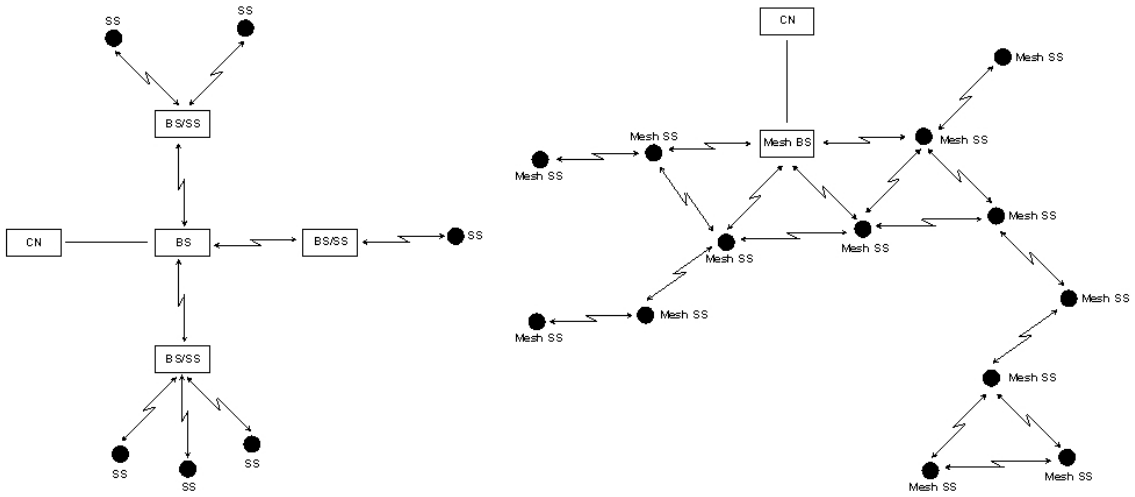
5.1 Architektura WMAN podle normy IEEE 802.16

Architektura sítí IEEE 802.16 je vzhledem k orientaci práce na bezpečnostní problematiku popsána jen velmi stručně, podrobné informace lze dohledat v normě [63, 64] a [65, 66].

5.1.1 Topologie

Základní topologií IEEE 802.16 je *vícebodové spojení* (*PTMP*, *Point-To-MultiPoint*), kdy *základnová stanice* (*BS*, *Base Station*) představuje centralizovaný prvek, který zabezpečuje komunikaci s několika podřízenými *účastnickými stanicemi* (*SS*, *Subscriber Station*) současně. Celý komplex je některou z BS připojen k *páteřní sítí* (*CN*, *Core Network*), viz obr. 5.1.

Volitelnou možností je *smyčková topologe* (*Mesh*) - tu specifikuje doplněk IEEE 802.16a z roku 2003 (viz část 5.1.4). *Účastnické stanice* (*Mesh SS*) mohou komunikovat i přímo mezi sebou, čímž je řešen také problém omezeného dosahu *základnové stanice* (*Mesh BS*) při daném vysílacím výkonu. Ostatní účastnické stanice pak plní roli bezdrátových směrovačů, replikujících signál na trase mezi vysílačem a přijímačem. Data tak putují k cíli nepřímo.



Obrázek 5.1: IEEE 802.16 - vícebodová (vlevo) a smyčková (vpravo) topologie

5.1.2 MAC podvrstva

MAC podvrstva IEEE 802.16 se ve srovnání s IEEE 802.11 výrazně liší. Je *spojovaná* a pro přístup k médiu používá protokol TDMA s centrálním plánováním, pomocí kterého BS přiděluje přenosovou kapacitu jednotlivým SS, což má velký význam pro zajištění kvality služeb jako podpora aplikací citlivých z hlediska času (hlas, video).

IEEE 802.16 dělí MAC podvrstvu na další tři *logické podvrstvy*. Nejvyšší podvrstvu představuje *MAC SSCS* (*MAC Service Specific Convergence Sublayer*), jež přijímá datové jednotky protokolů vyšších vrstev, provádí jejich klasifikaci, zpracování a následné předání na vstup nižší podvrstvy. Tou je *MAC CPS* (*MAC Common Part Sublayer*), vykonávající hlavní funkce MAC podvrstvy, jako je ustavení a udržování spojení, alokace šířky pásma, opakování přenosů, QoS, podpora handoveru, multicastové a broadcastové komunikace, přenosů v reálném čase, ale i služeb bez požadavků na čas a upřednostňování dat a další. Bezpečnost IEEE 802.16 na MAC podvrstvě (management klíčů, autentizace a šifrování) zajišťuje speciální bezpečnostní podvrstva *MAC SS* (*MAC Security Sublayer*).

5.1.3 Fyzická vrstva

První vydání normy IEEE 802.16 (2001) nařizovalo využití frekvencí v pásmu 10 až 66 GHz. Komunikace na uvedených kmitočtech ale vyžaduje přímou viditelnost mezi SS a BS, což byl jeden z hlavních problémů, proč takto specifikovaná WMAN nebyla příliš vhodná pro poskytování BWA. Standard navíc také neumožňoval mobilitu SS a jednalo se tedy jen o *pevný širokopásmový bezdrátový přístup* (*FBWA*, *Fixed Broadband Wireless Access*). IEEE 802.16-2001 pro modulaci signálu využívá pouze *jednu nosnou* (*SC*, *Single Carrier*), propustnost se pohybuje v rozmezí 32 až 134 Mbit/s.

První revize původního standardu, doplněk *IEEE 802.16a*, byla schválena v roce 2003 a nevyžaduje přímou viditelnost mezi vysílačem a přijímačem. Odstranění tohoto požadavku bylo dosaženo rozšířením specifikace fyzické vrstvy o techniku OFDM (1 nebo 256 kanálů), používanou i v jiných typech bezdrátových sítí, a její variantu *OFDMA* (*OFDM Advanced*) s 2048 kanály, dále také rozšířením kmitočtového rozsahu o licencované i nelicencované frekvence v pásmu 2 až 11 GHz. I nadále lze pracovat s *jedinou nosnou* (*SCa*), nově je zavedena technika *HUMAN* (*High-speed Unlicensed Metropolitan Area Network*) s dynam. výběrem kanálu. Maximální udávaná propustnost činní 75 Mbit/s, dosah pak 2 až 5 km při přímé a 30 až 50 km při nepřímé viditelnosti (některé zdroje uvádějí až 70 km).

Celá norma IEEE 802.16 prošla revizí v roce 2004 jako doplněk *IEEE 802.16d* a typicky se označuje jako *IEEE 802.16-2004*. Na fyzické vrstvě však nepřináší žádné zásadní změny.

Posledním významným z doposud schválených doplňků je *IEEE 802.16e*, jehož hlavním rysem je podpora *mobility* účastnických stanic (*MBWA*, *Mobile Broadband Wireless Access*) v pásmu 2 až 6 GHz do 120 km/h (literatura ale uvádí hodnotu až 150 km/h). Další inovací je zdokonalená technika OFDMA, označovaná jako *SOFDMA* (*Scalable OFDMA*).

5.1.4 Doplňky standardu IEEE 802.16

Tab. 5.1 uvádí seznam aktuálních doplňků[1] původní normy IEEE 802.16. K dokončeným specifikacím[2] je připsán rok ratifikace, u rozpracovaných doplňků očekávaný termín schválení.

Tabulka 5.1: Doplňky původní normy IEEE 802.16

Doplněk	**Rok**	**Popis**
802.16a	2003	(ne)licencované frekvence 2 až 11 GHz, 75 Mbit/s, OFDM(A)
802.16b	2003	rozšíření spektra o kmitočty 5 až 6 GHz, podpora QoS
802.16c	2002	systémové profily a testování zařízení pro pásmo 10 až 66 GHz
802.16d	2004	revize 802.16a, profily pro testování slučitelnosti zařízení s 802.16a
802.16e	2005	mobilita SS (do 120 km/h), 2 až 6 GHz, 75 Mbit/s, SOFDMA
802.16f	2005	MIB (Management Information Base) a doprovodné procedury
802.16g	2007?	vytváří standardizované procedury a rozhraní pro management
802.16h	2008?	řeší koexistenci systémů operujících v bezlicenčním pásmu
802.16i	2009?	MIB (Management Information Base) s podporou mobility
802.16j	2010?	relay stanice pro vyšší pokrytí, kapacitu a propustnost WMAN
802.16k	2010?	802.1D (definice propojovacích mostů) pro použití v 802.16
802.16m	2010?	podpora IMT-Advanced, až 100/1000 Mbit/s (mobilní/pevná SS)

[1] přehled dostupný na URL: `http://grouper.ieee.org/groups/802/16/tgs.html (květen 2007)`
[2] obsahy přístupné na URL: `http://standards.ieee.org/getieee802/802.16.html` (květen 2007)

5.2 Bezpečnostní otázky IEEE 802.16

Požadavky na zabezpečení WMAN specifikované ve formě *bezpečnostních cílů* odpovídají těm, které byly uvedeny v kapitole věnované zabezpečení WLAN (viz kap. 3). Stejně tak WMAN čelí stejným obecným *hrozbám* a základním typům *útoků* (viz část 3.4.2) a vzhledem k použití bezdrátové technologie má v principu i podobná *zranitelná místa* (viz část 3.3).

Podobnost s WLAN končí na úrovni bezpečnostních mechanismů *fyzické* a *linkové* vrstvy, ačkoli standardy IEEE 802.11 a IEEE 802.16 používají některé totožné kryptografické algoritmy. Norma IEEE 802.16, zejména její první verze, je již známá řadou zranitelných míst, jejichž odhalování je však zatím spíše předmětem teoretických rozborů, poněvadž praktické nasazování těchto sítí je v současnosti teprve v počátcích. Na *vyšších vrstvách* se u WMAN předpokládá použití stejného typu bezpečnostních opatření jako ve WLAN, tzn. VPN/IPSec, IDS/IPS atd. (viz část 3.8).

Následující části se proto věnují specifickým bezpečnostním mechanismům, zranitelným místům a útokům na WMAN IEEE 802.16 na fyzické (viz část 5.3) a linkové (viz část 5.4) vrstvě. Specifické téma představuje bezpečnost WMAN se smyčkovou topologii (Mesh), avšak vzhledem ke skutečnosti, že jde o velmi podobnou problematiku jako bezpečnost WPAN, jíž se zabývala již předchozí kapitola (viz kap. 4), není tomuto věnována zvláštní pozornost, nicméně důkladnou analýzu provádí [67].

5.2.1 Vývoj podpory zabezpečení IEEE 802.16

Nejdůležitější ***milníky v oblasti zabezpečení WMAN podle normy IEEE 802.16***:

- ***2001*** - první vydání normy IEEE 802.16 specifikuje protokol ***PKM*** pro *autentizaci*, *autorizaci* a *management klíčů*, šifrování ***DES-CBC*** - pouze *důvěrnost* přenosu dat;
- ***2004*** - v revizi normy ***AES-CCM*** - *důvěrnost*, *integrita* a *autenticita* přenosu dat;
- ***2005*** - IEEE 802.16e definuje ***druhou verzi protokolu PKM*** (***PKMv2***), silnější *autentizace*, *autorizace* a *management klíčů*, nově ***AES-CBC*** a ***AES-CTR***.

5.3 Zabezpečení IEEE 802.16 na fyzické vrstvě

Stejně jako u WLAN je i pro WMAN největší hrozbou na fyzické vrstvě záměrné rušení rádiového signálu, tj. *jamming*. Určitou modifikaci jammingu představuje tzv. *scrambling*, kdy útočník provádí rušení po krátké časové intervaly a zaměřuje se jen na určitý typ dat.

Bezpečnostní opatření definovaná přímo v normě, která dokáží částečně čelit oběma útokům, jsou dvě. Tím prvním je *OFDM* (*Orthogonal Frequency Division Multiplexing*), příp. zdokonalené varianty *OFDMA* a *SOFDMA*. Jejich význam je obdobný jako v případě metod rozprostřeného spektra FHSS a DSSS (viz část 3.6.2). OFDM paralelně přenáší data pomocí několika ortogonálních subnosných o nižší přenosové rychlosti bez nutnosti ochranných intervalů. Výhodou je vysoká spektrální efektivita a z bezpečnostního hlediska zejména *odolnost proti šumu* a *vícecestným interferencím*, neboť úzkopásmové rušení na určité frekvenci zasáhne pouze jednu subnosnou. Druhou skutečností je to, že narozdíl od bezdrátových LAN IEEE 802.11, které pracují výhradně v bezlicenčním kmitočtovém pásmu, standard IEEE 802.16 umožňuje využití také *licencovaných frekvencí*, které jsou pod dohledem regulačních orgánů, což by mělo případné útočníky odrazovat.

Proti jammingu a scramblingu se lze také bránit *zvýšením výkonu signálu a zisku* přijímače/vysílače. Detekci lze provádět *monitorováním rádiového spektra* (viz část 3.9.3).

5.4 Zabezpečení IEEE 802.16 na linkové vrstvě

Bezpečnost bezdrátových metropolitních sítí IEEE 802.16 se zajišťuje především na linkové vrstvě. Bezpečnostní mechanismy na úrovni fyzické vrstvy a naopak na vrstvách vyšších mají samozřejmě také svůj význam, ale jejich charakter je spíše doplňkový.

5.4.1 Bezpečnostní model podvrstvy MAC SS

Jak již bylo uvedeno v části 5.1.2, standard IEEE 802.16 vyčleňuje pro implementaci bezpečnostních mechanismů na úrovni linkové vrstvy speciální *bezpečnostní podvrstvu*, která je v normě označována jako *Security Sublayer* (*MAC SS*). V literatuře se lze ale běžně setkat i s jinými termíny, a to nejčastěji s pojmenováním *Privacy Sublayer*.

Identifikace síťových uzlů a spojení

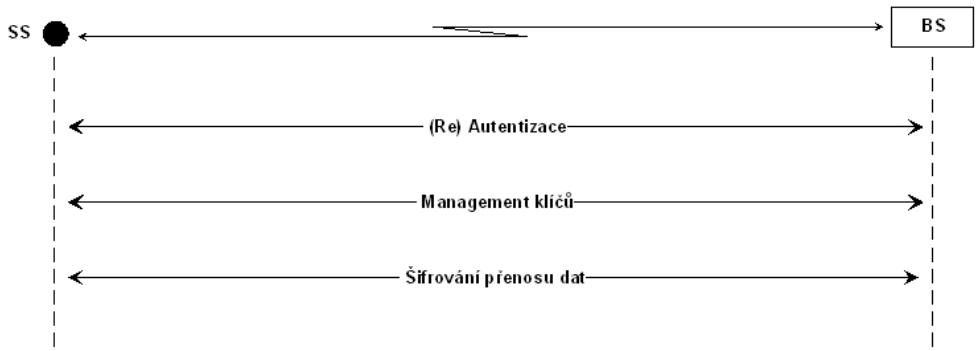
MAC podvrstva standardu IEEE 802.16 poskytuje *služby orientované na spojení*. Každý slot je součástí určitého *spojení* s unikátním identikátorem *CID* (*Connection IDentifier*). Spojení mohou být zaměřena buďto na *přenos rámců s informacemi pro management* (*Management Connection*), nebo jde o *transportní spojení* (*Transport Connection*), jímž se realizují všechny ostatní datové přenosy.

Norma dále zavádí pojem tzv. *bezpečné asociace* (*SA*, *Security Association*), což je souhrnné označení pro kryptografické algoritmy a klíče použité při zabezpečení komunikace mezi danou účastnickou a základnovou stanicí. Odlišení jednotlivých SA je provedeno na základě identifikátoru *SAID* (*Security Association IDentifier*). IEEE 802.16 používá dva typy bezpečné asosiace, a to *datovou SA* (*Data SA*) a *autorizační SA* (*Authorization SA*). Norma však obsahuje explicitní definici pouze první z uvedených. Datové SA dále dělí na *primární* (*Primary SA*), *statické* (*Static SA*) a *dynamické* (*Dynamic SA*). Primární SA se ustavuje během inicializačního procesu jako unikátní spojení mezi SA a BS a v tomto případě jsou si oba identifikátory CID a SAID rovny. Statická SA má význam pouze pro interní účely BS, dynamická SA vzniká i zaniká dle potřeb specifických služeb.

Komunikující strany jsou identifikovány na základě *certifikátu*. Jeho držiteli jsou přitom pouze účastnické stanice, certifikáty určené pro základnové stanice norma nedefinuje. Každé účastnické stanici implicitně přísluší dva digitální certifikáty *X.509* [68, 69], a to jeden *certifikát identifikující SS* (nastavený již přímo během výroby) a jeden *certifikát výrobce*, jenž slouží pro identifikaci výrobce bezdrátového zařízení.

Bezpečnostní proces

Celý *bezpečnostní proces* IEEE 802.16 znázorňuje obr. 5.2. Při vstupu do WMAN účastnická stanice prohledává rádiové spektrum za účelem nalezení vhodného downlinkového signálu, jenž použije pro ustavení spojení. Poté jsou nastaveny parametry fyzické vrstvy a sestaven *primární management kanál*, určený pro *autentizaci*, *autorizaci* a *management klíčů*, což jsou bezpečnostní mechanismy, které v IEEE 802.16 zajišťuje protokol *PKM* (viz části 5.4.2 a 5.4.3). Účastnická stanice se registruje na základě požadavku, který zašle základnové stanici. Základnová stanice v odpovědi přiřadí CID *sekundárnímu management spojení*. SS a BS vytvoří transportní spojení, volitelně lze nastavit *šifrování přenášených dat*, které je implementováno *zapouzdřovacím protokolem* (viz část 5.4.4). Zapouzdřovací protokol je realizován univerzálními kryptografickými algoritmy (norma IEEE 802.16 v tomto ohledu nedefinuje žádná vlastní, specifická šifrovací schemata).



Obrázek 5.2: Bezpečnostní proces IEEE 802.16

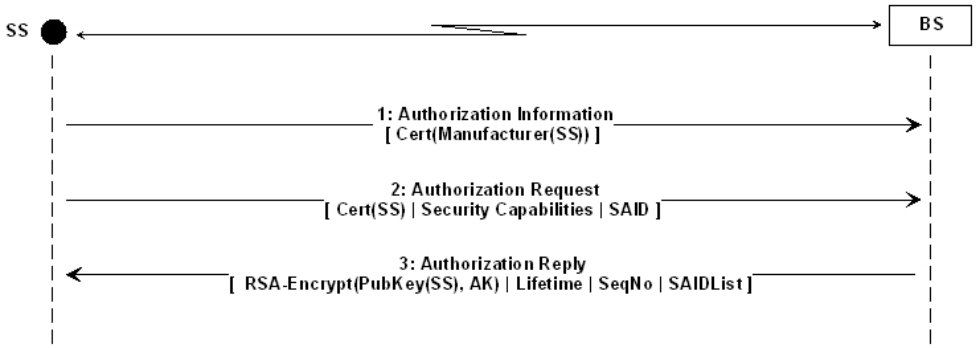
5.4.2 PKMv1

PKM (*Privacy Key Management*) je *autentizačním* a *autorizačním protokolem*, který navíc zajišťuje *distribuci kryptografických klíčů* mezi účastnickou (klient) a základnovou (server) stanicí. Specifikace protokolu PKM byla ale ve značném rozsahu převzata ze standardu *DOCSIS* (*Data Over Cable Service Interface Specifications*) [70], jenž vyvinula společnost *CableLabs* jako průmyslové řešení v oblasti kabelové komunikace. Specifikace DOCSIS bývá často také uváděna pod zkratkou *BPI+* (*Baseline Privacy Interface Plus Specification*). Vzhledem k odlišnosti bezpečnostních modelů drátových a bezdrátových sítí vyvolává použití normy DOCSIS v prostředí WMAN již samo o sobě vážné bezpečnostní pochybnosti.

První verze protokolu PKM (*PKMv1*), definovaná původním standardem IEEE 802.16 z roku 2001, obsahovala řadu zranitelných míst, které jsou analyzovány v závěru této části. Většinu slabin odstranila až *druhá verze protokolu PKM* (*PKMv2*, viz část 5.4.3), zavedená doplňkem IEEE 802.16e z roku 2001. Původní bezpečnostní platforma založená na PKMv1 se pak nazývá *základní bezpečnostní podvrstva* (*Basic Security Sublayer*). Zdokonalené šifrovací mechanismy (algoritmus AES) společně s protokolem PKMv2 naopak představují tzv. *rozšířenou bezpečnostní podvrstvu* (*Extended Security Sublayer*).

Autentizace a autorizace

Autentizační a autorizační proces protokolu PKM se uskutečňuje pomocí výměny tří zpráv mezi účastnickou a základnovou stanicí (viz obr. 5.3). Celou proceduru iniciuje SS, jež zašle BS zprávu *Authorization Information* s *certifikátem X.509 identifikujícím výrobce* (*Cert(Manufacturer(SS))*). Tato zpráva je nepovinná a BS ji může ignorovat, jde však o důležitou informací při rozhodování, zda se jedná o důvěryhodné zařízení, tj. pochází-li od důvěryhodného výrobce či nikoli. Následující zprávu, *Authorization Request*, vyšle bez prodlevy opět účastnická stanice a uvede v ní *certifikát X.509 identifikující SS* (*Cert(SS)*) s *veřejným klíčem*, *podporované autentizační/šifrovací algoritmy* (*Security Capabilities*) a identifikátor primárního SA, tj. *SAID*. BS certifikát účastnické stanice následně ověří a rozhodne, zdali je SS autorizovaným zařízením. Veřejný klíč SS základnová stanice použije při úspěšné autentizaci pro konstrukci odpovědi. Tou je zpráva *Authentication Reply*, která ustavuje *autorizační SA* mezi SS a BS. V odpovědi je obsažen 128-bitový *autorizační klíč* (*AK*, *Authorization Key*) *zašifrovaný* veřejným klíčem (algoritmus *RSA*) účastnické stanice (*RSA-Encrypt(PubKey(SS),AK)*), jeho *doba platnosti* (*Lifetime*), *sekvenční číslo* (*SeqNo*) a také *seznam SA deskriptorů* (*SAIDList*). Vlastnictví AK umožňuje účastnické stanici autorizovaný přístup do WMAN, přičemž daný AK sdílí výhradně jediný pár SS a BS.

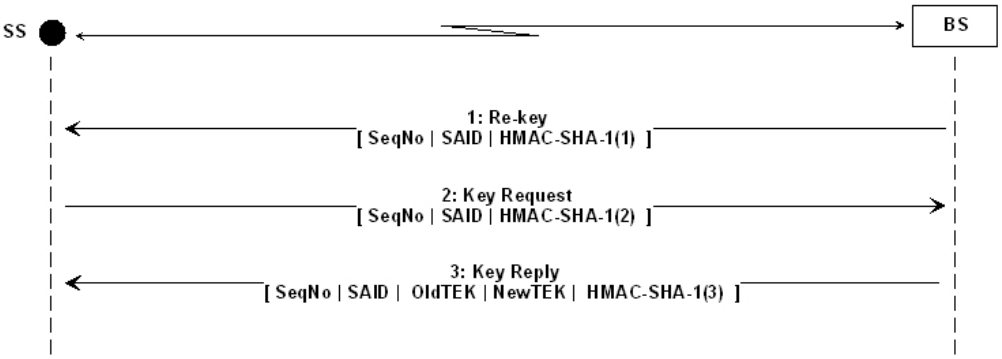


Obrázek 5.3: IEEE 802.16: autentizace a autorizace protokolem PKMv1

Management klíčů

Po ukončení autentizace a autorizace dochází k odvozování *sekundárních klíčů* (na obou stranách). Těmi jsou dva 160-bitové *HMAC* (*Hashed Message Authentication Code*) [71] klíče a jeden šifrovací klíč *KEK* (*Key Encryption Key*) o délce 128 bitů. Všechny tři klíče se odvozují z AK na základě hašovací funkce *SHA-1* (*Secure Hash Algorithm 1*) [72].

Proceduru ustavení *datové SA* znázorňuje obr. 5.4. Zpráva *Re-key* je volitelná a BS ji posílá tehdy, chce-li vynutit obnovu klíčů v již existující datové SA. *SeqNo* identifikuje použitý AK, *SAID* slouží jako identifikátor datové SA. Ze všech položek první zprávy je vypočten *haš* (*SHA-HMAC-1(1)*) na základě klíče HMAC určeného pro komunikaci ve směru od BS k SS (tzv. pro *downlinkové* spojení). Celý proces ale ve většině případů iniciuje SS zprávou *Key Request*, kterou žádá BS o zaslání parametrů SA. SS v ní uvede *SAID* ze seznamu SAIDList, *SeqNo* a *haš* (*SHA-HMAC-1(2)*). Základnová stanice ověří haš příchozí zprávy a také to, zda SAID skutečně odpovídá některé SA příslušející SS. V případě úspěchu zašle BS účastnické stanici v *odpovědi* (*Key Reply*) *původní* (*OldTEK*) a *nový* (*NewTEK*) šifrovací klíč *TEK* (*Traffic Encryption Key*). Oba jsou *zašifrovány* algoritmem *3DES* (*Triple Data Encryption Standard*) [73] v režimu *ECB* (*Electronic Code Book*) za použití klíče KEK. Ke každému z obou TEK klíčů jsou zaslány také *inicializační vektor*, *doba platnosti* a *sekvenční číslo*, přičemž doba platnosti původního a nově vygenerovaného TEK klíče je stanovena tak, aby došlo k dostatečnému časovému překryvu. Parametry *SeqNo*, *SAID* a *SHA-HMAC-1(3)* mají analogický význam jako v předchozích zprávách. SS může následně dešifrovaný TEK klíč použít pro šifrování přenosu dat (viz část 5.4.4).



Obrázek 5.4: IEEE 802.16: management klíčů protokolem PKMv1

Bezpečnostní analýza protokolu PKMv1

Bezpečnostní analýzou protokolu PKM se podrobně zabývá [74, 75], [76] navrhuje i vlastní řešení zjištěných nedostatků, které se týkají autentizace. autorizace i managementu klíčů.

Nejzřejmějším problémem *autentizace* podle protokolu PKMv1 je její *jednostrannost*, kdy se autentizuje SS vůči BS, ale účastnická stanice již nemá možnost ověřit identitu základnová stanice. Otvírá se tak prostor pro útoky *MITM* a *falešné BS* (*Rogue BS*), které představují podobný problém jako falešné přístupové body v sítích IEEE 802.11. Identifikace SS je založena na vlastnictví dvou digitálních certifikátů *X.509*, certifikát pro BS není v souvislosti s podporou pouze jednostranné autentizace definován. V normě také chybí přesná specifikace distribuce certifikátu *certifikační autoritou* (*CA*, *Certification Authority*). Riziko zde představují možné *krádeže identity*, pokud by byl jeden certifikát s unikátními kryptografickými klíči přiřazen více než jedné SS.

Autentizační a autorizační protokol je navíc náchylný na *útoky opakovaným přenosem*. Zprávám *Authentication Information* a *Authentication Request* chybí *časové razítko* (nebo případně jiný, ekvivalentní mechanismus, jako např. náhodná čísla) a *digitální podpis SS*, jenž by zaručil jejich *autenticitu* a *nepopiratelnost*. V případě zprávy *Authentication Reply* se navíc projevuje již zmíněný problém jednostranné autentizace. Potencionální útočník může zachycovat požadavky vyslané SS, konstruovat vlastní odpovědi na základě podvrženého autorizačního klíče a snadno získat kontrolu nad komunikací účastnické stanice. Jedná se tedy o typický útok typu *MITM*. S generováním autentizačního klíče jsou ale spojeny i další problémy. BS musí vytvářet AK zcela nezávisle na ostatních klíčích. To vyžaduje kvalitní *generátor náhodných čísel*. Norma ale žádné explicitní požadavky v tomto ohledu vůbec nespecifikuje. Generování AK by také mělo být za účelem dosažení co nejvyšší úrovně bezpečnosti prováděno za přispění obou stran. V případě protokolu PKMv1 je však tato procedura ponechána zcela v pravomoci BS.

Podobné nedostatky obsahuje i proces ustavování datové SA, tj. ta část protokolu PKMv1, která zajišťuje *management klíčů*. Nejzávažnější problém zde představuje malý *stavový prostor* 2-bitových *sekvenčních čísel* TEK klíčů. Po každém čtvrtém klíči dojde vynulování sekvenčního čítače, čímž je umožněn úspěch útokům opakovaným přenosem. Vzhledem k tomu, že minimální životnost TEK klíče je 30 minut a současně maximální doba platnosti AK až 70 dnů, datová SA může použít až 3360 různých TEK klíčů. Proto je nezbytné rozšířit stavový prostor identifikátoru SAID, a to alespoň na 12 bitů ($2^{12} = 4096$). *Autenticita* a *integrita* zpráv je sice při managementu klíčů zajišťována klíčovaným hašem (HMAC), ale generující funkce *SHA-1* byla oficiálně kompromitována roku 2005.

5.4.3 PKMv2

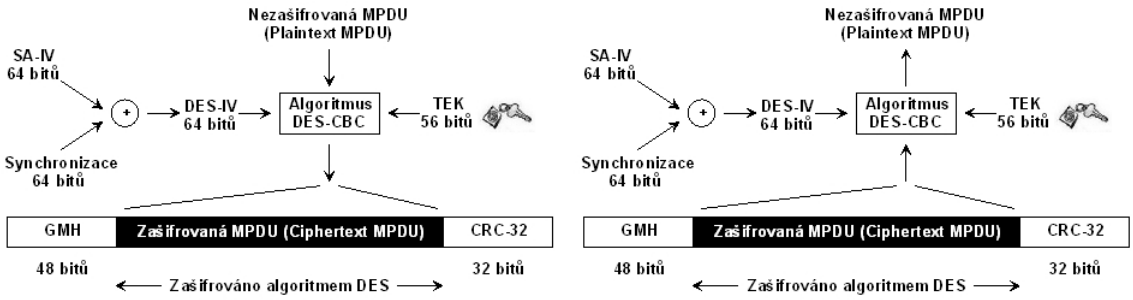
Druhá verze protokolu PKM (*PKMv2*) z roku 2005 je součástí doplňku *IEEE 802.16e* jako klíčový prvek pro podporu zabezpečení MBWA a řešení všech zásadních nedostatků PKMv1. Je zahrnuta *oboustranná autentizace* ověřující identitu *zařízení* i *uživatele* dle *IEEE 802.1X/EAP* (viz část 3.7.5). Zůstala i možnost autentizace pomocí algoritmu *RSA*, držitelem certifikátu *X.509* je však již i *BS*. Při ustavování autorizačního klíče jsou použita *náhodná čísla* pro zajištění *aktuálnosti všech zpráv*, stejně tak i mechanismy pro zabezpečení jejich *integrity* a *autenticity*. Jako alternativa k HMAC slouží *CMAC* (*Cipher-based Message Authentication Code*) [77], založený na šifře AES. PKMv2 prodlužuje délku *sekvenčních čísel* na 64 bitů a vzhledem k podpoře mobility je implementována *nová hierarchie klíčů*, *předběžná autentizace* a *optimalizované reautentizační mechanismy*.

5.4.4 Šifrování přenosu dat

Druhou komponentou bezpečnostního procesu IEEE 802.16 je *zapouzdřovací protokol* pro zabezpečení datových přenosů ve WMAN, které se ale plně vztahuje jen na transportní spojení, jelikož management rámce šifrování nepodléhají.

DES

Původní norma *IEEE 802.16-2001* využívá šifru *DES* (*Data Encryption Standard*) [78] v blokovém režimu *CBC* (*Cipher Block Chaining*). Šifrování (viz obr. 5.5) *otevřené MPDU* (*Plaintext MPDU*) se provádí na základě sdíleného 56-bitového *TEK klíče*, ustaveného dříve ve fázi managementu klíčů. *Inicializační vektor šifry DES* (*DES-IV*) o délce 64 bitů se získá aplikací operace *XOR* na *inicializační vektor SA* (*SA-IV*), přidružený ke klíči TEK, a *synchronizační pole* ze záhlaví rámce. Vznikne *zašifrovaná MPDU* (*Ciphertext MPDU*). *MAC záhlaví* (*GMH*, *Generic MAC Header*) a také *kontrolní součet* (*CRC-32*) se přenášejí v otevřené podobě. Dešifrování probíhá analogicky. Vstupem algoritmu DES-CBC je zašifrovaná MPDU, výsledkem je původní zpráva, příjemce použije vlastní kopii TEK a SA-IV, kterou sdílí s odesilatelem. Šifra DES samotná i způsob, jakým je v IEEE 802.16 pro šifrování dat použita, má několik nedostatků, které uvádí tab. 5.2.



Obrázek 5.5: IEEE 802.16: šifrování (vlevo) a dešifrování (vpravo) algoritmem DES-CBC

Tabulka 5.2: Slabiny algoritmu DES a jeho použití v IEEE 802.16

- algoritmus DES v režimu CBC vůbec nezajišťuje integritu ani autenticitu zpráv
- šifra DES s 56-bitovým klíčem poskytuje jen slabou důvěrnost přenosu dat
- nejsou implementovány žádné mechanismy zabraňující útokům opakovaným přenosem
- DES-IV zkonstruovaný na základě SA-IV a synchronizační informace je předvídatelný
- šifra DES má řadu vlastních chyb (komplementární a slabé klíče, návrh S-boxů, ...)

AES

Jako náhradu šifry DES nařizuje revidovaná norma *IEEE 802.16-2004* použití algoritmu *AES-CCM*, který využívá i doplněk IEEE 802.11i (viz část 3.7.7). Zajišťuje již dostatečnou úroveň *důvěrnosti*, *integrity* a *autentičnosti* přenášených dat, stejně tak i *ochranu proti útokům opakovaným přenosem*. Doplněk *IEEE 802.16e* pak přidává možnost provozovat algoritmus AES i v režimech *CBC* a *CTR*.

Kapitola 6

Zabezpečení MBWA IEEE 802.20

Bezdrátový standard ***IEEE 802.20***[1], uváděný někdy také pod označením ***Mobile-Fi***, je jednou z nejnovějších specifikací pro ***mobilní širokopásmový bezdrátový přístup*** (***MBWA***, ***Mobile Broadband Wireless Access***). Stejnou technologii používá např. také WMAN IEEE 802.16 v podobě svého doplňku IEEE 802.16e.

Vývoj normy započal v březnu 2002 a původně probíhal pod dohledem malé komise, jež byla součástí podvýboru IEEE 802.16. V závěru roku 2002 však vznikla samostatná pracovní skupina IEEE 802.20, jelikož podpora mobility uživatelů nepředstavovala původní záměr IEEE 802.16. Ačkoli existují určité rozdíly v architektuře i službách poskytovaných doplňkem IEEE 802.16e a normou IEEE 802.20, jde přitom především o rozdílná frekvenční pásma a maximální rychlosti pohybu zařízení/uživatele, obě specifikace definují stejný typ bezdrátové sítě a jsou postaveny na stejném technologickém základu. Zaměřují se na stejnou aplikační oblast a mají i velmi podobné cíle. V případě IEEE 802.16e jde sice o doplněk, který je navíc zatížen původním standardem a jeho pozdějšími dodatky IEEE 802.16a a IEEE 802.16d, avšak právě to, že jde o modifikaci již existující a postupně se rozšiřující technologie, může sítím WMAN IEEE 802.16 s podporou mobility velmi usnadnit jejich prosazení (narozdíl od IEEE 802.20). Další otázkou zůstává, jak se v budoucnu s nástupem IEEE 802.20 vyrovnají klasické mobilní sítě a jejich provozovatelé.

Uvedené skutečnosti již od samého vzniku pracovní skupiny IEEE 802.20 vyvolávají četné konflikty přímo v organizaci IEEE samotné a v roce 2006 dokonce vyústily v dočasné pozastavení prací na několik měsíců. Kritická situace byla ještě dále vyhrocena lobbistickými tlaky některých společností, které se snažily prosazovat začlenění vlastních technologií do specifikace. I přes značné komplikace ale vývoj standardu IEEE 802.20 nadále pokračuje a jako očekávaný termín dokončení se uvádí rok 2008. Neexistují tedy zatím žádné praktické zkušenosti s provozem MBWA IEEE 802.20 a ani návrh normy není veřejně přístupný. Informace vztahující se k tématu jsou proto dostupné jen ve velmi omezené míře a tato kapitola práce tak vychází z dosud publikovaných odborných článků [79, 80, 81, 82] a oficiálních materiálů IEEE [83, 84].

6.1 Architektura MBWA podle návrhu normy IEEE 802.20

V architektuře IEEE 802.20 lze nalézt mnoho rysů, které jsou specifické pro odlišné typy bezdrátových sítí. Jde především o podobnost s klasickými mobilními sítěmi (celulární architektura) a bezdrátovými metropolitními sítěmi (specifikace fyzické a linkové vrstvy).

[1] aktuality ohledně IEEE 802.20 jsou dostupné na URL: `http://www.ieee802.org/20/` (květen 2007)

6.1.1 Topologie

Topologie IEEE 802.20 se inspiruje *buňkovými systémy* klasických mobilních sítí s pokrytím rozsáhlých oblastí a členěním na makro/mikro/piko buňky. Budou podporovány rychlé přechody mezi jednotlivými buňkami/kanály (tzn. *handover*), ale také mobilita napříč MBWA různých poskytovatelů (tj. *roaming*). O možnosti alternativních uspořádání, jako je např. ad-hoc režim a smyčková topologie (Mesh), není zatím rozhodnuto.

6.1.2 MAC podvrstva

MAC podvrstva MBWA IEEE 802.20 vychází z technologií vyvinutých pracovní skupinou IEEE 802.16 a je taktéž rozdělena na další podvrstvy, jmenovitě *MAC SSCS*, *MAC CPS* a *MAC SS* (viz část 5.1.2). Navíc i techniky pro podporu mobility byly převzaty z doplňku IEEE 802.16e. Mechanismy provádějící ustavení spojení nejsou dosud plně definovány, zcela jistě ale bude zabudována podpora pro *QoS*, neboť obrazové a hlasové přenosy v reálném čase jsou jednou z klíčových služeb IEEE 802.20. Pro potvrzování správného přijetí rámců má být využito tzv. *hybridní ARQ* (*HARQ*, *Hybrid ARQ*). Na MAC podvrstvě budou také implementovány pokročilé kryptografické mechanismy jako významný základ komplexního zabezpečení MBWA IEEE 802.20 (viz dále část 6.2).

6.1.3 Fyzická vrstva

Fyzická vrstva IEEE 802.20 podobně jako její MAC podvrstva využívá technologických prvků normy IEEE 802.16, je však daleko více primárně orientována na mobilitu. Zatímco doplněk IEEE 802.16e umožňuje mobilitu do rychlosti 120 km/h, v případě IEEE 802.20 je to až 250 km/h (tzn. bude možné využívat MBWA i v rychle jedoucích vlacích). Dalším zásadním rozdílem je pracovní frekvenční pásmo, kdy IEEE 802.16e zavádí mobilitu na kmitočtech 2 až 6 GHz a IEEE 802.20 bude pracovat na licencovaných frekvencích ve spektru do 3.5 GHz, jejichž využití odstraňuje nutnost přímé viditelnosti. Pro zajištění duplexního provozu se předpokládá využití technik FDD i TDD. Jednotlivé kanály by měly mít šířku pásma do 5 MHz, přičemž přenosová rychlost na uživatele bude přibližně 1 Mbit/s pro downlinkové spojení (tzn. ve směru od základnové stanice směrem k mobilnímu zařízení) a 300 kbit/s pro uplink (tzn. ve směru od mobilního zařízení směrem k základnové stanici). Agregovaná rychlost v jedné buňce (velikost do 15 km) by se měla blížit hodnotám 4 Mbit/s (downlink) a 800 kbit/s (uplink). Pro sdílení spektra jsou navrhovány techniky CDMA a OFDMA. Použitá modulace a kódování odpovídá IEEE 802.16a/d (BPSK až 64QAM).

6.2 Návrhy na zabezpečení IEEE 802.20

Přestože standard IEEE 802.20 zatím dokončen nebyl, oficiální materiály organizace IEEE již naznačují některé rysy v oblasti budoucího zabezpečení MBWA. Mnohé bezpečnostní otázky (viz část 6.2.1) však zůstávají stále nezodpovězeny (viz část 6.2.2).

6.2.1 Poskytované bezpečnostní služby

Mezi uvažované bezpečnostní služby poskytované MBWA IEEE 802.20 patří *důvěrnost* a *integrita* přenosu dat, *oboustranná autentizace*, *autorizace* a *anonymita uživatelů*. Dále budou implementovány mechanismy zajišťující obranu vůči *DoS útokům*, *krádežím identity* a *útokům opakovaným přenosem*. Norma má zahrnovat i specifikaci *managementu klíčů*.

Šifrování přenosu dat

Pro šifrování přenosu dat by měl být povinně použit algoritmus *AES* se 128-bitovým klíčem, přičemž bude možné volit všechny čtyři kombinace zajišťující důvěrnost/integritu (současně důvěrnost i integrita, pouze důvěrnost, pouze integrita, bez zajištění důvěrnosti a integrity). Podle vyjádření organizace IEEE je v případě standardu IEEE 802.20 cílem co nejvyšší úroveň zabezpečení, která bude schopná odolat všem známým typům útoků. Proto hodlá podrobit bezpečnostní mechanismy IEEE 802.20 extenzivní analýze za pomoci zkušených kryptologů, aby se neopakovala podobná situace jako v případě WLAN IEEE 802.11 a jejího protokolu WEP. Použité kryptografické algoritmy by měly být veřejně dostupné bez jakýchkoliv omezení. Bezpečnostní opatření definovaná standardem na úrovni linkové vrstvy mají sice zásadní význam, nicméně i pracovní skupina IEEE 802.20 připouští, že toto řešení je zamýšleno pouze jako částečné s předpokladem dodatečného zabezpečení za pomoci protokolů vyšších vrstev (EAP, TLS, SSL, IPSec, ...).

6.2.2 Otevřené bezpečnostní otázky

Otevřenými bezpečnostními otázkami zůstávají *cílová architektura* (buďto ad-hoc, nebo infrastrukturní síť), *míra flexibility* (podpora různých bezpečnostních režimů/šifer/verzí), očekávaný *výkon kryptografických algoritmů* (latence, propustnost, výpočetní náročnost, implementační složitost), *logické umístění bezpečnostní podvrstvy* a souvisejících rozhraní v rámci architektury IEEE 802.20 (tři varianty: mezi fyzickou vrstvou a MAC podvrstvou, mezi LLC a MAC podvrstvou, příp. integrace do MAC podvrstvy), *rozsah zabezpečení rámců* (datové/řídicí/managementu), *bezpečnost broadcastového a multicastového provozu* (požadavky na zdroje, šířku pásma, synchronizace, ...), *dopad zabezpečení na handover* (latence), *míra komplexnosti řešení* (v jakém rozsahu je zabezpečení na linkové vrstvě dostatečné a do jaké míry bude nutné využívat protokolů vyšších vrstev), zajištění *ochrany vůči útokům opakovaným přenosem* (mechanismy využívající náhodná čísla/časová razítka), *režie zabezpečení* (jak velká část rámce má být vyhrazena pro bezpečnostní informace), specifikace *managementu klíčů* (je vyžadována přesná definice požadavků) a otázky ohledně *ochrany identity uživatelů* (definice identity uživatele, do jaké míry má být chráněna).

Kapitola 7

Zabezpečení MIH IEEE 802.21

Norma ***IEEE 802.21***[1] se od ostatních standardů výrazně liší. Není schématem pro výstavbu určité bezdrátové sítě, nýbrž zavádí podporu pro mobilitu uživatelů napříč heterogenními typy drátových i bezdrátových sítí definovaných výborem IEEE 802, ale také mezi sítěmi IEEE 802 a externími sítěmi. Podporovány jsou např. technologie UMTS, GSM či GPRS. Tuto techniku označuje organizace IEEE jako ***MIH*** (***Media Independent Handover***), podstatně častěji se lze ale v odborné literatuře setkat s termínem ***vertikální handover*** (*Vertical Handoff*). *Horizontální handover* (*Horizontal Handoff*), tj. mobilitu na úrovni základnových stanic využívajících stejnou přístupovou technologii (např. přesuny uživatele mezi jednotlivými AP ve WLAN), IEEE 802.21 také umožňuje, nicméně prioritou zůstává podpora mobility mezi sítěmi heterogenních typů.

Pracovní skupina IEEE 802.21 byla založena v roce 2004, schválení vyvíjeného standardu se neočekává dříve než v druhé polovině roku 2007. Situace je tedy obdobná jako v případě normy IEEE 802.20, tzn. návrh specifikace ani praktické zkušenosti s MIH nejsou zatím známé. Předběžné oficiální informace lze získat z tutoriálu IEEE [85], dodatečné poznatky jsou dostupné z několika dalších dokumentů [86, 87, 88, 89].

7.1 Architektura WRAN podle návrhu normy IEEE 802.21

Architekturu MIH tvoří abstraktní vrstva *MIHF* (*Media Independent Handover Function*), jež představuje jednotné služební rozhraní pro vyšší vrstvy. Navíc ale zajišťuje komunikaci i se specifickými komponentami linkové a fyzické vrstvy. MIHF definuje tři typy služeb: *MIES* (*Media Independent Event Service*), *MICS* (*Media Independent Command Service*) a *MIIS* (*Media Independent Information Service*).

7.1.1 MIES

MIES poskytuje služby vyšším vrstvám hlášením místních (klient) i vzdálených (síť) *událostí* linkové vrstvy. Události mohou být jednak *lokální* (týkají se klienta), jednak *vzdálené* (odehrávají se v síti). Tok informací skrz síťovou architekturu je orientován od nižších vrstev k vrstvě MIHF a odtud směrem k vyšším vrstvám. Ačkoliv vrstva MIHF operuje nad médii různých typů a je v tomto ohledu považována za nezávislou, ne všechny typy médií podporují stejný typ událostí. Události tak musejí být registrovány na nižších vrstvách. Typickými událostmi jsou navázání/ukončení spojení, změna parametrů spojení aj.

[1] oficiální webová stránka podvýboru IEEE 802.21 viz URL: `http://www.ieee802.org/21/` (květen 2007)

7.1.2 MICS

Prostřednictvím MICS řídí vyšší vrstvy činnost vrstev nižších, což zahrnuje shromažďování informací o stavu linek a předávání *příkazů* nižším vrstvám. Příkazy mohou být (podobně jako události u MIES) jak *lokální* (ty jsou zadávány z vyšších vrstev), tak i *vzdálené* (původcem je entita přístupové sítě). Mezi typické příkazy patří zjišťování stavu spojení, vyhledávání nově vzniklých spojení, konfigurace nového spojení, přepínání mezi dostupnými spojeními a další.

7.1.3 MIIS

MIIS rozšiřuje služby MIHF o mechanismy určené pro vyhledávání a distribuci statických i dynamických *informací* o okolních sítích. Mezi statické informace patří např. název sousední sítě a jejího poskytovatele, příklady dynamických údajů jsou informace o stavu kanálů, bezpečnosti a MAC adresách. Pro reprezentaci informací MIIS využívá standardní formáty, kterými jsou *XML* (*eXtensible Markup Language*) a *TLV* (*Type-Length-Value*).

MIHF tedy podporuje pouze první dvě z typických fází handoveru, tzn. jeho iniciaci (vyhledávání nového spojení) a přípravu (ustavení nového spojení), ale nikoliv už vlastní předání spojení, které je mimo rozsah normy IEEE 802.21.

7.2 Návrhy na zabezpečení IEEE 802.21

Bezpečnost je jednou z hlavních služeb IEEE 802.21, mezi ty další patří QoS, kontinuita služeb (minimalizace zpoždění a ztráty dat), podpora aplikací s různými tolerančními charakteristikami, vyhledání a výběr sítě a řízení výkonu. Vzhledem k tomu, že standard IEEE 802.21 je teprve ve fázi vývoje, nejsou zatím příliš známé informace dotýkající se bezpečnosti. Signalizaci při handoveru je ale nutné obecně zabezpečit na všech vrstvách. Zde největší hrozby představují *odposlech*, *DoS* a *MITM* útoky.

V rámci IEEE 802.21 se žádné definice bezpečnostních mechanismů nepředpokládají, bude ale podporována *autentizace* a *autorizace* za pomoci pokročilých technik, jako je *předběžná autentizace* (*MPA*, *Media-independent Pre-Authentication*), kterou ve WLAN zavádí již doplňky IEEE 802.11i/r (viz části 3.7.7 a 3.9.1).

MPA je optimalizace zabezpečení handoveru za asistence mobilní stanice, která je schopná nejenom získat síťovou adresu a ostatní konfigurační parametry z *kandidátní cílové sítě* (*CTN*, *Candidate Target Network*), ale také vysílat/přijímat pakety do/z této sítě na základě získané adresy ještě dříve, než se k CTN skutečně připojí. Schopnost komunikace na úrovni síťové vrstvy ještě před ustavením linkového spojení má zásadní význam při snižování latence handoveru a podpoře aplikací citlivých z hlediska času.

Kapitola 8

Zabezpečení WRAN IEEE 802.22

IEEE 802.22[1] [90, 91, 92, 93, 94, 95] je dosud nedokončenou a současně nejnovější specifikací ze všech bezdrátových standardů v rámci výboru IEEE 802. Pracovní skupina IEEE 802.22 vyvíjí od roku 2004 normu pro tzv. ***bezdrátové regionální sítě*** (***WRAN***, ***Wireless Regional Area Network***), jejíž ratifikaci lze očekávat nejdříve v roce 2008. Funkce bezdrátových regionálních sítí je založena na tzv. *kognitivní rádiové technologii* (*Cognitive Radio Technology*). Technologie WRAN bude pracovat ve frekvenčním pásmu lokálně nevyužívaných *televizních kanálů*. Uplatnění IEEE 802.20 se předpokládá primárně v odlehlých, řídce osídlených (venkovských) regionech, kde by měla nabízet datové, hlasové i audiovizuální přenosy. Hlavním cílem WRAN je poskytnout pevný bezdrátový přístup k Internetu s parametry xDSL a kabelových přípojek dalším skupinám obyvatelstva a přispět tak ke snížení tzv. *digitálních rozdílů* (*Digital Divide*).

8.1 Architektura WRAN podle návrhu normy IEEE 802.22

Specifikace IEEE 802.22 stejně jako všechny ostatní standardy výboru IEEE 802 zahrnuje pouze MAC podvrstvu a fyzickou vrstvu. V následujícím textu jsou předloženy základní údaje o navrhované architektuře WRAN, k uvedeným informacím je však nutné přistupovat s tím, že finální verze normy se může ještě značně změnit.

8.1.1 Topologie

Podle návrhu normy IEEE 802.22 má mít topologie bezdrátové regionální sítě výhradně podobu *vícebodového spojení* (*PTMP*, *Point-To-MultiPoint*). Celý systém budou tvořit dvě základní komponenty, a to *základnová stanice* (*BS*, *Base Station*) a *zákaznické zařízení* (*CPE*, *Customer Premise Equipment* nebo také *Consumer Premises Equipment*). Zatímco u základnové stanice se předpokládá instalace pověřenou entitou, zákaznické zařízení bude moci naopak instalovat sám uživatel. Základnová stanice má v rámci své buňky plnit nejen tradiční roli spočívající v řízení provozu a řízení přístupu jednotlivých stanic do sítě, ale také přijímat zpětnovazební signály od jednotlivých účastnických stanic. BS zpětnovazební informace od CPE průběžně zaznamenává a dále vyhodnocuje a provádí na jejich základě důležitá rozhodování, jejichž cílem je zajistit využívání jen neobsazených kanálů a zamezit tak interferencím s jinými zařízeními. Jde o metodu známou jako *Distributed Sensing*.

[1] aktivity podvýboru IEEE 802.22 lze sledovat na URL: `http://www.ieee802.org/22/` (květen 2007)

8.1.2 MAC podvrstva

MAC podvrstva IEEE 802.22 bude ve značném rozsahu inspirována doplňkem IEEE 802.16e, zejména co se týká zajišťování kvality služeb. Přesto však její implementace vyžaduje některé nové rysy vzhledem k nutnosti pružné reagovat na dynamické změny nastávající v operačním prostředí sdílených televizních pásem. Kromě klasických rámců má MAC podvrstva pracovat také se *superrámci* (*Superframe*), které jsou složeny z několika dílčích rámců. Pro zajištění vícenásobného přístupu k přenosovému médiu budou sítě IEEE 802.22 používat techniku časového sdílení (TDMA).

8.1.3 Fyzická vrstva

Fyzická vrstva IEEE 802.22 se podobně jako MAC podvrstva bude v mnohém podobat fyzické vrstvě WMAN, společné rysy lze nalézt především s doplňky IEEE 802.16a/d. Hlavní rozdíly spočívají ve využívaných frekvenčních pásmech a kapacitách kanálů.

IEEE 802.22 má pracovat v pásmu UHF/VHF vyhrazeném pro televizní vysílání, které v mezinárodním měřítku zahrnuje frekvence 47 až 910 MHz, v případě USA je však omezeno na spektrum 54 až 862 MHz. Mezi uvažované šířky kanálu patří 6, 7 a 8 MHz, v USA však jedinou možnou hodnotu bude 6 MHz. Nezávisle na konfiguraci kanálu se předpokládá využití obou základních duplexních technik, tzn. TDD i FDD. Sdílení spektra bude zajištěno metodou OFDMA s 1024/2048 subnosnými a dle kvality kanálu IEEE 802.22 adaptivně využije modulace BPSK až 64QAM. Uváděný maximální dosah WRAN je až 100 km, propustnost 18 až 24 Mbit/s na jeden kanál. Ve frekvenčním pásmu, které má IEEE 802.22 využívat, pracují v současnosti i další zařízení, jako např. bezdrátové mikrofóny. Existuje tak riziko vzájemného rušení. Tyto problémy řeší skupina *IEEE 802.22.1*, další skupina, *IEEE 802.22.2*, vznikla za účelem vývoje doporučení pro instalaci a nasazení WRAN.

8.2 Návrhy na zabezpečení IEEE 802.22

Jak již bylo uvedeno v úvodu této kapitoly, vývoj standardu IEEE 802.22 teprve probíhá a není veřejně znám ani její předběžný návrh. Způsob zabezpečení WRAN tak není zatím přesně definován. Oficiální materiály organizace IEEE přisuzují zabezpečení IEEE 802.22 nejvyšší prioritu, konkrétní bezpečnostní mechanismy pro zajištění *autentizace*, *autorizace*, *důvěrnosti* a *integrity* dat ale budou zřejmě známé až po dokončení normy. Vzhledem k těmto skutečnostem zatím neexistují a ani nemohou existovat žádné praktické zkušenosti s provozem bezdrátových regionálních sítí a s tím spojené informace o zranitelných místech, proveditelných útocích a dalších bezpečnostních problémech této technologie.

Kapitola 9

Bezpečnostní srovnání standardů

Zatímco každá z šesti předchozích kapitol byla zaměřena na zabezpečení jedné konkrétní bezdrátové technologie, tato kapitola naopak provádí bezpečnostní srovnání standardů a nabízí ucelený náhled na celou problematiku. Kritérii porovnání jsou používané bezpečnostní mechanismy fyzické a linkové vrstvy a jejich schopnost zajišťovat deklarované bezpečnostní cíle. Vyzdvižena jsou bezpečnostní specifika jednotlivých typů sítí včetně charakteristických hrozeb, které narušují poskytování bezpečnostních služeb. V závěru je stručně provedeno i srovnání z pohledu dalšího vývoje zabezpečení.

9.1 Srovnání zabezpečení na fyzické vrstvě

Na fyzické vrstvě mají z bezpečnostního hlediska zásadní význam použitá *frekvenční pásma*, způsob *šíření rádiového signálu* a *techniky přenosu dat* specifikované v jednotlivých normách.

Licencovaná a nelicencovaná frekvenční pásma

Jako důležité preventivní bezpečnostní opatření lze na úrovni fyzické vrstvy chápat využívání *licencovaných frekvenčních pásmech*, která jsou pod dohledem regulačních orgánů. Zvyšuje se tak pravděpodobnost odhalení narušitelů i důsledky (sankce), kterým budou muset při uskutečnění útoku čelit. Na druhou stranu provoz bezdrátových zařízení v licencovaných pásmech představuje pro provozovatele i uživatele dodatečnou administrativní a finanční zátěž. Proto bezdrátové sítě často využívají *nelicencovaná frekvenční pásma*.

Nejpoužívanějším nelicencovaným pásmem je v mezinárodním měřítku ISM 2.4 GHz. Využívají je sítě IEEE 802.11b/g, IEEE 802.15.1, IEEE 802.15.3, IEEE 802.15.4 (jedno z pásem, které je určeno pro globální použití) a IEEE 802.16a/e (více frekvencí). Další bezlicenční pásma využívají IEEE 802.11a (5 GHz), IEEE 802.15.4 (868 MHz, 915 MHz), IEEE 802.16a (některé kmitočty ve spektru 2 až 11 GHz). V licencovaných pásmech naopak pracují sítě IEEE 802.16 (některé frekvence v pásmu 10 až 66 GHz), IEEE 802.16a/b/e (některé frekvence v pásmu 2 až 11 GHz), do budoucna i IEEE 802.20 (do 3.5 GHz) a IEEE 802.22 (54 až 862 MHz / 47 až 910 MHz).

Technologie WLAN a WPAN tedy operují výhradně v nelicencovaných pásmech a pravděpodobnost *jammingu* je v těchto sítích teoreticky výrazně vyšší než u připravovaných technologií MBWA a WRAN, kde by k úmyslnému i neúmyslnému rušení vůbec docházet nemělo. Méně přehledná situace je u WMAN, které využívají licencovaná i nelicencovaná pásma. Zvláštním případem je technologie IEEE 802.15.3a, která sice pracuje v pásmu 3.1 až 10 GHz, avšak vzhledem k použití UWB nevyžaduje povolení od regulačních úřadů.

Šíření rádiového signálu

Potencionální útočník představuje hrozbu pro fyzickou vrstvu bezdrátové sítě pouze tehdy, má-li možnost zachytit rádiový signál, příp. získat fyzický přístup k technickému vybavení. Zde je důležitým kritériem *vysílací výkon* a *dosah* sítě. Stejně tak fyzické *operační prostředí*, které šíření rádiového signálu výrazně ovlivňuje. Dalším parametrem, jenž přímo souvisí s již zmíněným dosahem, je použité *frekvenční pásmo*. S vyššími frekvencemi roste nutnost přímé viditelnosti mezi přijímačem a vysílačem a reálně se snižuje dosah bezdrátové sítě.

Zdánlivě nejbezpečnějšími jsou v tomto ohledu *WPAN*. Osobní operační prostor nemá v průměru obvykle více než 10 m a útočník by se tak musel nacházet v bezprostřední blízkosti komunikujícího zařízení. Na druhou stranu např. zařízení IEEE 802.15.1 spadající do třídy 1 s vysílacím výkonem 100 mW mohou disponovat dosahem až 100 m. Vzdálenost několika desítek metrů je reálná i u sítí IEEE 802.15.3 a IEEE 802.15.4. Senzorové sítě svou funkci navíc často plní v odlehlých či přímo nepřátelských oblastech, kde fyzická přítomnost v blízkosti jejich síťových uzlů nepředstavuje pro útočníka zvýšené riziko. Nelze také opomenout fakt, že WPAN usiluje především o propojení mobilních a přenosných zařízení. Mobilita uživatele pak znamená časté změny operačního prostředí, jehož vlastnosti a tím i hrozby se dynamicky a nepředvídatelně mění.

WLAN dosahuje na volném prostranství stovky metrů, při použití speciálních antén může jít i o několik kilometrů. Signál WLAN je tak možné ve srovnání s WPAN snadněji zachytit. Pomineme-li ad-hoc sítě, které IEEE 802.11 sice umožňuje, ale nejsou jejím hlavním cílem, má WLAN oproti osobním sítím výhodu ve statické infrastruktuře. Fyzický operační prostor WLAN je tak pevně vymezen, což usnadňuje používání nástrojů pro monitorování rádiového spektra a tím i odhalení případných útočníků. Vzhledem k relativně neměnnému prostředí lze také přesněji definovat hrozby (např. školní, podnikové nebo WLAN s veřejným přístupem mají svoje specifické hrozby). Navíc plní-li WLAN svůj původní účel, tzn. není-li použita jako přístupová síť, nýbrž jako náhrada klasické (drátové) LAN, pak lze vzhledem k jejímu typickému provozu v uzavřených prostorách šíření signálu dále účinně regulovat fyzickými překážkami (speciální stavební materiály a nátěry, zástěny, okenní fólie apod.). V této souvislosti lze zmínit optické bezdrátové sítě. Rozptyl optického paprsku je velmi malý a jeho zachycení není snadné. Ačkoliv bezdrátové sítě třídy IEEE 802 jsou založeny výhradně na rádiové technologii, původní standard IEEE 802.11 z roku 1997 umožňoval i optické přenosy infračerveným paprskem (viz část 3.6.3).

Bezpečnostní situace *WMAN* se z hlediska zachytitelnosti rádiového signálu příliš neliší od těch bezdrátových lokálních sítí, které jsou provozovány ve venkovním prostředí a poskytují přístup k Internetu. Infrastruktura IEEE 802.16 byla také původně navržena jako statická, anologii k ad-hoc sítím ve WLAN představují ve WMAN sítě se smyčkovou topologií (Mesh). Nicméně dosah WMAN je vyšší, typicky v kilometrech, maximálně několik desítek kilometrů. Situace se ale mění s doplňkem IEEE 802.16e, který z WMAN činní širokopásmovou mobilní bezdrátovou síť.

Sítě *MBWA* IEEE 802.20 a WMAN s podporou mobility jsou pak nejzranitelnější. Spojuje se zde dynamičnost operačního prostředí a proměnnost hrozeb charakteristických pro WPAN s pokrytím rozsáhlých oblastí u *WRAN* IEEE 802.22. Signál bezdrátových regionálních sítí sice bude zachytitelný až na vzdálenost 100 km, technologie WRAN je ale vyvíjena výhradně pro pevný bezdrátový přístup.

Ale i tehdy, pokud se útočníkovi signál zachytit podaří, mohou odposlechu a narušení integrity přenášených dat zabránit speciální přenosové techniky, jejichž význam a použití v různých typech bezdrátových sítí IEEE 802 srovnává následující část.

Modulační schémata a techniky rozprostřeného spektra

Základem zabezpečení na úrovni fyzické vrstvy jsou u bezdrátových technologií metody *rozprostřeného spektra*. Jsou založeny na vysílání rádiového signálu a přenosu dat pomocí výrazně širšího frekvenčního pásma, než je nezbytně nutné. Mají zamezit *odposlechu* a úmyslným i neúmyslným *interferencím*. Fungují tedy jako bezpečnostní mechanismy pro zajištění *důvěrnosti* a *integrity* přenosu dat a *dostupnosti* prostředků sítě. Nevýhodou je vyšší složitost přijímače a náročnější řízení výkonu, což ale nesnižuje úroveň zabezpečení.

Každý z bezdrátových standardů výboru IEEE 802 implementuje některou z technik rozprostřeného spektra. Jde především o metody *FHSS* a *DSSS*. Techniku FHSS používá původní norma IEEE 802.11 z roku 1997 a také standard IEEE 802.15.1. DSSS implementují doplňky IEEE 802.11b/g a norma IEEE 802.15.4. Další velmi používanou technikou je *OFDM*, přestože se obvykle nepovažuje přímo za variantu rozprostřeného spektra. Nicméně např. [13] OFDM jako jednu z metod rozprostřeného spektra uvádí. OFDM uplatňují sítě IEEE 802.11a/g a IEEE 802.16a/d/e. Zdokonalenou variantu, *OFDMA*, specifikují doplňky IEEE 802.16d/e a jejich využití se předpokládá i u vyvíjených standardů IEEE 802.20 a IEEE 802.22. Ve specifikaci IEEE 802.16e lze pak najít další variantu OFDM, označovanou jako *SOFDMA*. Velmi unikátní technologií jsou *ultraširokopásmové přenosy* (*UWB*), které však v současnosti využívají v rámci IEEE 802 pouze sítě IEEE 802.15.3a.

Srovnáme-li výše uvedené techniky, největší předností varianty FHSS je odolnost vůči *úzkopásmovému jammingu*. Snáze se implementuje a dosahuje i vysoké spektrální efektivity. FHSS ale není tak robustní metodou jako DSSS. Zatímco FHSS odolává jammingu tím, že mění frekvence podle pseudonáhodného schématu skoků a při zarušení dílčího kanálu se pokouší data přenést na jiné frekvenci, DSSS obsahuje statistické algoritmy, které dokáží původní (nezarušený) signál díky určité redundanci přenášených dat obnovit. Obě techniky jsou vůči úzkopásmovému rušení účinné a mají svůj bezpečnostní význam.

V případě prevence vůči *odposlechu* je rozhodující, zda útočník zná schéma frekvenčních proskoků u FHSS a čipovací sekvenci při použití DSSS. Tyto informace ale bývají často přímo součástí specifikace. Standardy vypracované výborem IEEE 802 jsou po určité době od jejich ratifikace veřejně a bezplatně dostupné a případným útočníkům nejsou při získávání potřebných parametrů kladeny žádné překážky. Příkladem může být *Barkerův kód* v normě IEEE 802.11. Konstrukce přijímače schopného odposlechu rozprostřeného signálu vyžaduje pokročilé znalosti, ty však mohou útočníci získat z publikací, které na toto téma vznikají. Proto nelze považovat techniky rozprostřeného spektra za mechanismy spolehlivě zaručující důvěrnost. Ta musí být zajištěna na linkové vrstvě, příp. i na vrstvách vyšších.

Z bezpečnostního hlediska dokonalejší metodu než FHSS a DSSS představuje UWB. Rádiový signál je při ultraširokopásmovém přenosu značně obtížné nejen *odposlouchávat* a *rušit*, ale i *detekovat*, protože jej lze jen velmi nesnadno odlišit od šumu. Technologie UWB je použitelná jen na krátké vzdálenosti (řádově desítky metrů) a není proto možné uvažovat o její implementaci např. v metropolitních a regionálních sítích. Velký přínos ale znamená pro osobní bezdrátové sítě, kde může výrazně zvýšit úroveň *důvěrnosti* a *integrity* přenášených dat a zamezít útokům na *dostupnost*.

U sítí s dlouhým a středně dlouhým dosahem je nejčastější volbou OFDM. Přenos dat probíhá paralelně na několika ortogonálních subnosných a zarušení jedné frekvence znamená zasažení jen jedné subnosné. Bezpečnostní přínos OFDM lze tedy přirovnat k FHSS.

Pro úspěšný odposlech je nezbytná i znalost *modulačních technik*. Ty ale nemají pro bezdrátové sítě IEEE 802 z pohledu bezpečnosti žádný význam, neboť použitý typ modulace i její princip nepodléhají utajení. Demodulace signálu je tak vždy možná.

9.2 Srovnání zabezpečení na linkové vrstvě

Linková vrstva má pro zabezpečení bezdrátových sítí zásadní význam. Na její úrovni normy specifikují bezpečnostní mechanismy zajišťující *autentizaci*, *autorizaci* a *důvěrnost*, *integritu* a *autenticitu* přenášených dat na základě šifrování. Některé bezdrátové standardy přitom *bezpečnostní architekturu* linkové vrstvy velmi důkladně specifikují.

9.2.1 Bezpečnostní architektury linkové vrstvy

Před započetím samotného srovnání bezpečnostních mechanismů, které jednotlivé normy implementují, je zajímavé porovnat i celkovou *koncepci* zabezpečení na linkové vrstvě. V tomto ohledu je nejvýraznější normou IEEE 802.16, jež zavádí *bezpečnostní podvrstvu* jako jednu ze tří podvrstev linkové vrstvy. Stejným způsobem bude vystavěno i zabezpečení linkové vrstvy vyvíjeného standardu IEEE 802.20. WPAN bezpečnostní podvrstvu přímo nezahrnují, ale např. IEEE 802.15.1 definuje několik *úrovní důvěryhodnosti* zařízení a služeb a také *bezpečnostní režimy*, které lze nalézt i v normě IEEE 802.15.4. Standard IEEE 802.21 pak specifikuje abstraktní podvrstvu *MIHF*. O bezpečnostní architektuře sítí IEEE 802.22 informace zatím dostupné nejsou. Architektura linkové vrstvy WLAN IEEE 802.11 ve smyslu existence jisté bezpečnostní podvrstvy explicitně vymezena není.

9.2.2 Autentizace

Autentizaci jako proces ověření identity zařízení/uživatele přistupujícího do bezdrátové sítě specifikuje v určité podobě každý z bezdrátových standardů IEEE 802.

Častým autentizačním mechanismem je v bezdrátových sítích protokol *výzva-odpověď*. Implementují jej standardy IEEE 802.11, IEEE 802.15.1 a IEEE 802.15.3. Dále se používá *IEEE 802.1X* s protokolem *EAP*. Tento způsob autentizace uplatňují doplňky IEEE 802.11i a IEEE 802.16e a také specifikace WPA. Ostatní bezpečnostní mechanismy jsou specifické pro jednotlivé typy sítí. IEEE 802.11 umožňuje jednoduchou autentizaci na základě *SSID*, příp. *ESSID*, mimo specifikaci normy lze provádět *filtrování MAC adres*. Autentizaci na základě *přístupových seznamů* definuje také IEEE 802.15.4. Jako součást protokol WEP byla specifikována i tzv. *otevřená autentizace*. WPA a IEEE 802.11i definují *PSK* autentizaci, jež pracuje s přednastavenými klíči. IEEE 802.16 používá vlastní autentizační a autorizační protokol *PKMv1*, příp. *PKMv2* v doplňku IEEE 802.16e. U vyvíjených norem IEEE 802.20 a IEEE 802.22 nejsou konkrétní autentizační mechanismy dosud známé. IEEE 802.21 jako řešení vertikálního handoveru bude poskytovat *předběžnou autentizaci*.

Nejnižší úrovně zabezpečení dosahuje *otevřená autentizace* a autentizace založená na *SSID*, což jsou mechanismy specifické pro WLAN. Při otevřené autentizaci ověřovatel nemá žádnou možnost prověření identity žadatele a její bezpečnostní význam je tak nulový (jako nulová autentizace se často i označuje). SSID implicitně vysílá přístupový bod v pravidelných intervalech a jeho hodnota není utajována. Proto je nutné vysílání SSID buď zamezit, nebo přejít na autentizaci pomocí identikátoru *ESSID*, jehož hodnota je pevně naprogramována do každého přístupového bodu. Avšak u SSID i ESSID zásadním problémem zůstává sdílení stejné přístupové hodnoty (hesla) všemi uživateli WLAN.

Další možností je *filtrace MAC adres*, které se nejčastěji používá ve WLAN, není však principiálně omezena pouze na tento typ sítí. Přestože představuje silnější autentizační mechanismus, než je nulová autentizace a autentizace pomocí SSID a ESSID, jelikož je již zajištěna diferencicace jednotlivých uživatelů, je tato metoda náchylná na *krádeže identity*.

P1rotokol *výzva-odpověď* představuje již sofistikovanější autentizační techniku vzhledem k požadavku na znalost sdíleného tajného klíče. Nevýhodou je otevřenost vůči útokům typu *MITM*. Dalším problémem je management klíčů. Pro každý pár různých zařízení by měl existovat unikátní sdílený klíč. Vzhledem k administrativní náročnosti však často dochází ke sdílení autentizačního klíče všemi stanicemi v sítí. Typickým příkladem je v tomto ohledu WLAN IEEE 802.11, kde se stejné kryptografické klíče používají současně pro autentizaci i šifrování přenášených dat. Stejným problém postihuje *autentizaci s přednastaveným klíčem* (*PSK*), kde je navíc zvýšené riziko *slovníkových útoků*, poněvadž se sdílené klíče generují na základě ASCII hesel. I přes uvedené nedostatky je úroveň autentizace výzva-odpověď, příp. autentizace s přednastavenými klíči, při správném používání výrazně vyšší než mechanismy založené na SSID, ESSID či filtrování MAC adres.

Vyššího stupně zabezpečení dosahuje autentizace založená na *digitálních certikátech*. Tu uplatňují protokoly *PKMv1* a *PKMv2*, které využívají asymetrické kryptografie v podobě algoritmu *RSA*. Autentizace s veřejným klíčem je principiálně méně problematická než autentizační mechanismy vyžadující znalost sdíleného klíče, poněvadž neexistují takové problémy s distribucí a obnovou kryptografických klíčů. Případné slabiny, které obsahuje i protokol PKMv1, nesouvisejí přímo s principem autentizace na základě veřejného klíče, nýbrž v zabezpečení výměny zpráv mezi žadatelem a ověřovatelem a způsobem generování náhodných čísel. Všechny nedostatky protokolu PKMv1 navíc odstranila jeho druhá verze.

Nejvyšší bezpečnostní úrovně dosahuje autentizace na základě *IEEE 802.1X/EAP*. Při autentizaci probíhá komunikace mezi klientem a autentizačním serverem, volit lze z několika metod autentizace. Podporovány jsou např. přístupová jména a hesla, digitální certifikáty, čipové karty aj. Ačkoli byly při bezpečnostní analýze IEEE 802.X/EAP nalezeny určité slabiny, které mohou být využity pro provádění *únosů relací*, *krádeží identity*, *DoS*, *slovníkových* a *MITM* útoků, riziko lze ovlivnit výběrem autentizační metody. Protokol EAP je navíc rozšiřitelný, takže lze do budoucna předpokládat vznik dalších, pokročilejších metod. Ve srovnání s dříve popsanými technikami autentizace má však IEEE 802.1X/EAP zásadní nevýhodu díky požadavku na složitější infrastrukturu (autentizační server).

Jedním ze zásadních aspektů autentizace je, zda se ověřuje identita *zařízení* či *uživatele* a probíhá-li autentizace *vzájemně*, nebo pouze *jednostranně*. Oboustrannou autentizaci, která je současně založena na identifikaci/verifikaci uživatele, poskytují v bezdrátových sítích IEEE 802 pouze protokoly IEEE 802.1X/EAP a PKMv2. Použití oboustranné autentizace je deklarováno i v případě IEEE 802.20. Všechny ostatní autentizační mechanismy nabízejí implicitně pouze jednostrannou autentizaci s ověřením identity zařízení.

9.2.3 Autorizace

Autorizace logicky následuje autentizační proces, kdy po ověření identity je nutné uživateli přiřadit přístupová práva, na jejichž základě bude využívat prostředky bezdrátové sítě. Narozdíl od autentizačních schémat, která jsou součástí každého z bezdrátových standardů třídy IEEE 802, není autorizace ve všech specifikacích nativně podporována.

Např. norma IEEE 802.11 pro WLAN ani žádný z jejích pozdějších doplňků definici autorizačních mechanismů přímo neobsahuje. Stejný stav platí i pro WPAN IEEE 802.15. Standard IEEE 802.16 naopak autorizaci podporuje v podobě protokolů *PKMv1* a *PKMv2*. Autorizační mechanismy by měly být také součástí vyvíjených norem MBWA IEEE 802.20 a WRAN IEEE 802.22. Pro upřesnění je nutné dodat, že doplňky IEEE 802.11i a IEEE 802.16e uvádějí možnost autorizace protokolem *IEEE 802.1X/EAP*. Jde ale o externí mechanismus, který specifikuje norma IEEE 802.1 (byť v rámci výboru IEEE 802).

9.2.4 Zabezpečení přenosu dat

Přenos dat je na linkové vrstvě zabezpečen šifrováním. Je však nutné rozlišovat, jak jsou zajištěny jednotlivé bezpečnostní cíle - *důvěrnost*, *integrita*, *autenticita* a také *aktuálnost* přenosu dat jako *obrana vůči útokům opakovaným přenosem*.

Důvěrnost

Pro bezdrátové standardy IEEE 802 je charakteristické, že zajišťují *důvěrnost* přenosu dat pomocí externích, univerzálních kryptografických algoritmů. Velmi rozšířená je šifra *AES*, kterou používají standardy IEEE 802.11i, IEEE 802.15.3, IEEE 802.15.4 a IEEE 802.16d/e. Implementace algoritmu AES pro zajištění důvěrnosti dat je deklarována i u vznikajícího standardu IEEE 802.20. Použití jiných šifer je pak specifikem jednotlivých sítí. Ve WLAN jde o protokoly *WEP* a *TKIP*, které využívají šifru *RC4*, IEEE 802.15.1 zabezpečuje důvěrnost algoritmem E_0 a IEEE 802.16 používá *DES*. Téměř ve všech případech šifry používají 128-bitový klíč, částečnou výjimkou je pouze *WEP*, kde jsou možné i 64-bitové klíče, a také DES s 56-bitovým klíčem. IEEE 802.15.1 pracuje s variabilní délkou klíče od 8 do 128 bitů. U všech norem s šifrou AES je využit režim *CTR*, ať už přímo či jako součást režimu *CCM*. Operačním režimem šifry DES je *CBC* (IEEE 802.16).

Nejnižší úroveň důvěrnosti zajišťuje protokol WEP se synchronní šifrou RC4, která není vhodná pro prostředí bezdrátové komunikace. Největší problém však spočívá ve způsobu, jakým je v IEEE 802.11 implementována. Protokol TKIP také používá algoritmus RC4, avšak oproti WEP dosahuje výrazně vyšší bezpečnosti díky sofistikovanější konstrukci šifrovacích klíčů včetně prodloužení inicializačních vektorů ze 24 na 48 bitů. Šifry E_0 a DES-CBC jsou pak slabé samy o sobě. V IEEE 802.15.1 jsou navíc problémy s vytvářením inicializačních vektorů, které se odvíjejí od části hodinového signálu. Podobný problém má i IEEE 802.16, kde je inicializační vektor konstruován na základě synchronizační informace, což způsobuje jeho předvídatelnost.

Šifra AES již poskytuje dostatečnou úroveň důvěrnosti přenášených dat a sama žádné závažné nedostatky nemá. Nevýhodou jsou ale např. ve srovnání s algoritmem RC4 vyšší nároky na výpočetní výkon. Otázky implementační, paměťové a výpočetní náročnosti mají přitom zásadní význam v senzorových sítích, kde se AES také používá. Ale i např. ve WLAN vyšší náročnost algoritmu AES znamená nutnost výměny stávajícího technického vybavení. Důsledkem pak je, že se reálně používají méně bezpečné, ale se stávajícím technickým vybavením slučitelné bezpečnostní mechanismy (WEP, WPA).

Integrita

Integritu datových přenosů ve WLAN zajišťují algoritmy *CRC-32* (WEP), *MIC* (TKIP ve WPA a IEEE 802.11i) a *AES* v režimu *CBC-MAC* (IEEE 802.11i). CRC-32 je dále použito u IEEE 802.15.1. AES se objevuje v IEEE 802.15.3, IEEE 802.15.4, IEEE 802.16d/e a podle současného návrhu bude využit pro zajištění integrity i u IEEE 802.20.

Nejnižší úroveň bezpečnosti z hlediska integrity přenosu dat je v sítích založených na původní normě IEEE 802.16 z roku 2001, jež používá DES-CBC, který integritu vůbec nezajišťuje. Za kryptografický kontrolní součet, jenž by zaručoval integritu přenášených dat, v žádném případě nemůže být považován lineární kód CRC-32. Ten je do jisté míry dostatečně účinný je vůči neúmyslným chybám. MIC je výrazně kryptograficky dokonalejší než CRC-32, vznikl však jako kompromisní řešení mezi úrovní zabezpečení a výpočetní efektivitou. Nejsilnějším mechanismem pro zajištění integrity je AES v režimu CBC-MAC.

Autenticita

Autenticita přenášených dat je většinou zajišťována stejnými mechanismy jako integrita. Ve WLAN je to *MIC* (WPA) a *AES* v režimu *CBC-MAC* (IEEE 802.11i). IEEE 802.15.1 (E_0) a první vydání norem IEEE 802.11 (WEP) a IEEE 802.16 (DES-CBC) autenticitu vůbec nezajišťují. AES-CBC-MAC je pak použit kromě IEEE 802.11i v IEEE 802.15.3, IEEE 802.15.4 s IEEE 802.16d/e.

Obrana vůči útokům opakovaným přenosem

Aktuálnost dat jako *ochranu vůči útokům opakovaným přenosem* vůbec nezajišťují protokol WEP v IEEE 802.11, IEEE 802.15.1 a původní norma IEEE 802.16. Ve WLAN *TKIP* (WPA a IEEE 802.11i) zavádí *sekvenční čísla*, které současně plní funkci inicializačních vektorů. Specifikace IEEE 802.11i, IEEE 802.15.3, IEEE 802.15.4 a doplňky IEEE 802.16d/e implementují šifru *AES* v režimu *CTR*, která zajišťuje ochranu vůči útokům opakovaným přenosem formou *čítače*. Při doručení jsou pak odmítnuty všechny zprávy, u nichž velikost čítače/sekvenčního čísla je nižší než poslední adresátem zaznamenaná hodnota.

9.3 Srovnání z pohledu dalšího vývoje zabezpečení

Bezpečnost bezdrátových sítí IEEE 802 prochází dalším vývojem, přestože nejzásadnější etapu mají již zřejmě za sebou. Nové bezpečnostní mechanismy vznikají buď v rámci doplňků současných standardů, nebo jako externí specifikace mimo rozsah norem IEEE.

Bezpečnost na úrovni *fyzické vrstvy* další vývojem už téměř neprochází. Výjimkou jsou sítě IEEE 802.15.4, kde má být v roce 2007 schválen nový doplněk IEEE 802.15.4a. Zavádí technologii *UWB* pro realizaci širokopásmových přenosů i v senzorových sítích a také novou metodu rozprostřeného spektra, označovanou jako *CSS*.

Na *linkové vrstvě* jsou pro zvýšení úrovně zabezpečení WLAN v současnosti vyvíjeny doplňky *IEEE 802.11r* a *IEEE 802.11w*. První z uvedených má zavést podporu pro rychlý a současně *bezpečný handover* mezi AP v rámci ESS. Dokončení IEEE 802.11r se očekává v září roku 2007. IEEE 802.11w má pak zajišťovat *zabezpečení management rámců*. Zde je nutné zdůraznit, že význam zabezpečení management rámců v současné době ve srovnání s minulostí výrazně narůstá. IEEE 802.11w je přitom prvním doplňkem, který se tento problém pokouší komplexně řešit. Částečné zabezpečení rámců obsahujících informace pro management poskytuje i doplněk IEEE 802.16e. Všechny ostatní bezdrátové normy/doplňky výboru IEEE 802 v současné době zabezpečují pouze datové rámce. U WPAN a WMAN žádné bezpečnostní doplňky vyvíjeny nejsou. Bezpečnostní mechanismy vznikajících norem pro MBWA, MIH a WRAN zatím přesně specifikovány také nejsou.

Další úroveň bezpečnosti přinášejí *protokoly vyšších vrstev*, jejichž specifikace přesahuje rámec standardů IEEE 802. Navíc nejsou pro jednotlivé kategorie bezdrátových sítí příliš specifické a nebyly proto ani v této kapitole předmětem vlastního srovnání. I nadále budou uplatňovány klasické bezpečnostní mechanismy, jako jsou firewall, VPN/IPSec, TLS/SSL atd. Za velmi progresivní technologie lze označit *IDS/IPS systémy* a *reputační systémy*, které mohou nalézt uplatnění ve všech typech bezdrátových sítí IEEE 802, ačkoli budou zpočátku využívány pravděpodobně především ve WLAN.

Kapitola 10

Praktická část

Jako praktická část diplomové práce vznikl *elektronický dokument*, který je tematicky zaměřen stejně jako vlastní technická zpráva, problematiku však dále prohlubuje. Celá diplomová práce má charakter přehledové studie zabezpečení bezdrátových standardů třídy IEEE 802. Některé části však vyžadují důkladnější popis a hlubší analýzu, což však přesahuje rámec vlastní písemné zprávy především z hlediska rozsahu. Proto cílem elektronického dokumentu bylo právě obsáhnout a dále prohloubit ta témata a ty problémy, které nemohly být z uvedeného důvodu zařazeny do tohoto textu diplomové práce.

10.1 Použité technologie

Jedním ze základních kritérií při výběru formy elektronického dokumentu byla možnost vhodné prezentace práce v celosvětové sítí jako případný základ webu zaměřeného na problematiku zabezpečení bezdrátových technologií organizace IEEE, jenž by sloužil pro studijní/výukové účely. Dalším požadavkem bylo provázání elektronického dokumentu na významné informační, zejména internetové, zdroje.

Jako technologie pro realizaci praktické části diplomové práce byl proto vybrán jazyk *XHTML* s použitím *kaskádových stylů* (*CSS*). XHTML je progresivní technologií, která vychází z XML a současně zachovává sémantiku HTML. Výhodou XML je jednodušší implementace (jazyk je zjednodušen a lépe se zpracovává), možnost ukládání, indexace a vyhledávání (nativní XML databáze), existuje mnoho nástrojů pro zpracování (DOM a SAX parsery pro čtení dokumentů, XSLT pro transformaci, ...) a značné množství aplikací je také již na XML založeno. V kombinaci s CSS pak XHTML dokument dosahuje nižší datové velikosti, vzhled je definován nezávisle na jeho obsahu a je tak možné snadno oddělit obsah od formy a vzhled dokumentu flexibilně udržovat a měnit. Jeden externí stylový předpis může navíc zajistit konzistentní vzhled celé množiny webových stránek. Výsledkem je jednoznačná a přehledná struktura elektronického dokumentu.

Jazyk XHTML byl použit v nejnovější dostupné verzi 1.1, která vychází z XHTML verze 1.0 Strict. XHTML 2.0 je teprve ve fázi návrhu a navíc nezachovává kompatibilitu s verzemi předcházejícími. Aplikované stylové předpisy odpovídají CSS verze 2.0 s dobrou podporou v současných webových prohlížečích. Všechny XHTML dokumenty, které tvoří jednotlivé části celého elektronického dokumentu, byly úspěšně prověřeny validátorem a jsou plně slučitelné se specifikacemi uvedených verzí. Plná funkčnost byla dále potvrzena v nejnovějších webových prohlížečích, tj. Internet Explorer 7.0, Mozilla Firefox 2.0.0.3 a Opera 9.20. Zdrojové soubory jsou přiloženy na datovém nosiči (Příloha 1).

10.2 Struktura dokumentu

Struktura elektronického dokumentu odpovídá struktuře vlastní technické zprávy. Úvodní strana celého elektronického dokumentu je koncipována jako strukturovaný obsah s přímými odkazy na jednotlivé kapitoly a podkapitoly různých úrovní. Každá kapitola písemné práce je v elektronickém dokumentu implementována jako jeden soubor s kódem XHTML/CSS.

S využitím intuitivních navigačních prvků se lze sekvenčně pohybovat mezi jednotlivými kapitolami, přes logo v záhlaví je pak možný návrat na titulní stránku s obsahem. V rámci každé kapitoly jsou pro snazší orientaci podkapitoly strukturovány, číslovány a pojmenovány totožně s odpovídajícími částmi této písemné práce. Závěrem je uveden seznam zkratek.

10.3 Použité informační zdroje

Jako podklady pro zpracování elektronického dokumentu sloužily normy a další oficiální materiály organizace IEEE, RFC, články, příspěvky a knihy dostupné v elektronické podobě a také tištěné knihy. Převážná většina použitých publikací byla napsána v anglickém jazyce, ostatní literární prameny jsou v češtině.

Pro zpracování úvodní kapitoly elektronického dokumentu byly užity prameny [1] - [5]. Kapitola věnovaná přehledu bezdrátových standardů je založena na zdrojích [6] - [8], [96]. Problematika bezdrátových lokálních sítí byla zpracována za pomoci [9] - [43], [97] - [111]. Kapitola o bezpečnosti bezdrátových osobních sítí čerpá z [44] - [62], [112] - [130]. Při zpracování kapitoly zaměřené na zabezpečení bezdrátových metropolitních sítí autor využil [63] - [78], [131] - [150]. Uvedené informace o zabezpečení mobilních širokopásmových sítích vycházejí z [79] - [84], [151] - [154]. Kapitola popisující problematiku vertikálního handoveru je založena na [85] - [89], [155] - [156]. Téma zabezbečení bezdrátových regionálních sítí bylo vypracováno s použitím [90] - [95], [157] - [161]. Všechny použité zdroje vztahující se k danému tématu jsou v elektronickém dokumentu uvedeny vždy na konci každé kapitoly.

10.4 Obsah dokumentu

Jak již bylo uvedeno, elektronický dokument přejímá strukturu vlastní technické zprávy, rozšířen je obsah s doplněním odkazů na významné informační zdroje. Úvodní kapitola, která stručně popisuje historii bezdrátové komunikace a uvádí motivaci a cíle práce, byla s drobnými úpravami převzata z písemné zprávy. Druhá kapitola, věnovaná bezdrátovým standardům, je v elektronickém dokumentu více rozšířena o charakteristiku mezinárodních normalizačních institucí a průmyslových sdružení. Obsahuje navíc dodatečné informace o architektuře bezdrátových sítí IEEE 802 a přehled jednotlivých standardů zpracovává detailněji. Kapitoly věnované zabezpečení WLAN IEEE 802.11, WPAN IEEE 802.15 a WMAN IEEE 802.16 obsahují ve srovnání s textem této písemné práce především hlubší analýzu jednotlivých bezpečnostních mechanismů s důkladnějším popisem zranitelných míst. V menší míře byly rozšířeny informace o architektuře. Normy MBWA IEEE 802.20, MIH IEEE 802.21 a WRAN IEEE 802.22 dosud schváleny nebyly a proto není příliš velký prostor pro hlubší analýzu bezpečnostních mechanismů. Elektronický dokument zde spíše uvádí rozšiřující informace o celkové koncepci a architektuře těchto sítí. Kapitola srovnávající jednotlivé normy příliš rozšířena nebyla. Tato kapitola, věnující se praktické části diplomové práce, v elektronickém dokumentu pochopitelně chybí. Závěrečná kapitola i seznam zkratek se shodují s odpovídajícími částmi vlastní technické zprávy.

Kapitola 11

Závěr

Cílem diplomové práce bylo provést přehled v oblasti zabezpečení bezdrátových standardů organizace IEEE, které jsou normalizovány výborem 802. V současnosti existuje celkem šest norem, které specifikují různé typy bezdrátových sítí. Těmi jsou IEEE 802.11 pro bezdrátové lokální sítě, IEEE 802.15 pro bezdrátové osobní sítě, IEEE 802.16 pro bezdrátové metropolitní sítě, IEEE 802.20 pro mobilní širokopásmový bezdrátový přístup, IEEE 802.21 pro vertikální handover a IEEE 802.22 pro bezdrátové regionální sítě.

V úvodní části byl naznačen historický i současný technologický vývoj bezdrátových technologií, definována nutnost dodatečného zabezpečení bezdrátových rádiových sítí a uvedena motivace a vymezení cílů studie zabezpečení bezdrátových standardů. Následující kapitola představila společnou architekturu počítačových sítí založených na normách výboru IEEE 802 se stručnou charakteristikou vyvíjených bezdrátových specifikací. Navazující kapitoly byly věnovány zabezpečení vždy jednomu typu bezdrátové technologie, která je vyvíjena v rámci příslušné pracovní skupiny. Pro každý ze standardů byly uvedeny aktuální bezpečnostní mechanismy, zranitelná místa a také potencionální hrozby, které narušují poskytování bezpečnostních cílů bezdrátových sítí a ohrožují tak jejich bezpečností cíle. Práce se zaměřila především na bezpečnostní mechanismy linkové a fyzické vrstvy, které jsou pro jednotlivé typy bezdrátových sítí specifické a na této úrovni se vzájemně odlišují. Určitý prostor byl ale také věnován bezpečnostním protokolům vyšších vrstev. Součástí práce bylo vzájemné srovnání jednotlivých standardů z bezpečnostního hlediska s vyzdvižením jejich specifických vlastností i společných charakteristických rysů.

Jako praktická část diplomové práce byl vytvořen elektronický dokument realizovaný technologiemi XHTML 1.1 a CSS, jenž obsahuje důkladnější popis a hlubší analýzu celé bezpečnostní problematiky. Jedním z hlavních cílů byla také snadná prezentace vytvořené práce v celosvětové sítí s provázáním na významné informační zdroje.

Diplomová práce může sloužit jako studijní materiál a cenný zdroj aktuálních informací z oblasti bezpečnosti bezdrátové komunikace. Bezdrátové technologie procházejí v současné době dynamickým vývojem a existuje tak značný prostor pro navazující studie. Práce měla přehledový charakter s cílem napomoci čtenáři při orientaci v dané oblasti. Další práce proto mohou být zaměřeny výhradně na zabezpečení některé z prezentovaných technologií a dále prohlubovat získané znalosti. To platí především v případě vyvíjených a dosud neschválených standardů IEEE 802.20, IEEE 802.21 a IEEE 802.22. Další možností je např. vytvoření důkladné srovnávací studie, která by brala v úvahu aktuálně používané bezpečnostní mechanismy, aktiva, zranitelná místa, hrozby a kalkulovala rizika pro dané typy sítí. Existuje však i mnoho jiných kategorií bezdrátových sítí, jejichž zabezpečení může být náplní samostatných studií. Jde např. o a klasické mobilní a satelitní sítě.

Literatura

[1] Goldsmith, A.: Wireless Communications, Standford University, 2004.

[2] Dubendorf, V.: A History of Wireless Technologies, 2003.
Dokument dostupný na URL:
http://media.wiley.com/product_data/excerpt/95/04708494/0470849495.pdf
(květen 2007).

[3] Tapan, S., Mailloux, R., Oliner, A.: History of Wireless, Wiley, 2006.

[4] Riva, G., Vatalaro, F., Davide, F.: Ambient Intelligence, 2005.
Dokument dostupný na URL:
http://www.emergingcommunication.com/volume6.html (květen 2007).

[5] Friedewald, M., Da Costa, O.: Ambient Intelligence in Everyday Life, 2003.
Dokument dostupný na URL:
http://www.cybertherapy.info/pages/AmIReportFinal.pdf (květen 2007).

[6] McCabe, C.: Standards Development at the IEEE Standards Association, IEEE-SA, 2005. Dokument dostupný na URL:
http://standards.ieee.org/announcements/bkgnd_stdsprocess.html
(květen 2007).

[7] IEEE Std 802-2001, IEEE, 2002. Dokument dostupný na URL:
http://standards.ieee.org/getieee802/download/802-2001.pdf (květen 2007).

[8] IEEE Std 802.2, 1998 Edition (R2003), IEEE, 1998. Dokument dostupný na URL:
http://standards.ieee.org/getieee802/download/802.2-1998.pdf
(květen 2007).

[9] IEEE Std 802.11, 1999 Edition (R2003), IEEE, 1999. Dokument dostupný na URL:
http://standards.ieee.org/getieee802/download/802.11-1999.pdf
(květen 2007).

[10] Geier, J.: Wireless LANs, Second Edition, Sams Publishing, 2002.

[11] Gast, M.: 802.11 Wireless Networks: The Definitive Guide, O'Reilly, 2002.

[12] Gilbert, H.: Securing Wireless LANs, Wiley, 2003.

[13] Zandl, P.: Wifi - praktický průvodce, Computer Press , 2003.

[14] Thomas, T.: Zabezpečení počítačových sítí bez předchozích znalostí, CPress, 2004.

[15] Karygiannis, T., Owens, L.: Wireless Network Security, 2002.
Dokument dostupný na URL:
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
(květen 2007).

[16] Potter, B., Fleck, B.: 802.11 Security, O'Reilly, 2002.

[17] Rawat, J.: Wi-Fi Security: Best Practices, 2006. Dokument dostupný na URL:
http://www.trisc.org/documents/9_20_Rawat_WLAN.pdf (květen 2007).

[18] Pužmanová, R.: Infračervené sítě, 2004. Dokument dostupný na URL:
http://www.lupa.cz/clanky/infracervene-site/ (květen 2007).

[19] IEEE Std 802.11Q, 2003 Edition, Virtual Bridged Local Area Network, IEEE, 2003.
Dokument dostupný na URL:
http://standards.ieee.org/getieee802/download/802.1Q-2003.pdf
(květen 2007).

[20] Walker, J.: Unsafe at any key size; An analysis of the WEP encapsulation, 2000.
Dokument dostupný na URL:
http://www.dis.org/wl/pdf/unsafe.pdf (květen 2007).

[21] Borisov, N., Goldberg, I., Wagner, D.: Intercepting Mobile Communications: The Insecurity of 802.11, 2001. Dokument dostupný na URL:
http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf (květen 2007).

[22] Argaugh, W. A.: An Inductive Chosen Plaintext Attack against WEP/WEP2, 2001.
Dokument dostupný na URL:
http://www.cs.umd.edu/~waa/attack/frame.htm (květen 2007).

[23] Fluhrer, S., Mantin, I., Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4, 2001. Dokument dostupný na URL:
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf (květen 2007).

[24] Hulton, D.: Practical Exploitation of RC4 Weaknesses in WEP Environments, 2002.
Dokument dostupný na URL:
http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt (květen 2007).

[25] IEEE Std 802.1X-2004, Port-Based Network Access Control, IEEE, 2004.
Dokument dostupný na URL:
http://standards.ieee.org/getieee802/download/802.1X-2004.pdf
(květen 2007).

[26] Blunk, L., Vollbrecht, J.: PPP Extensible Authentication Protocol, RFC 2284, 1998.
Dokument dostupný na URL:
http://www.ietf.org/rfc/rfc2284.txt (leden 2007).

[27] Aboba, B., Blunk, L.: Extensible Authentication Protocol (EAP), RFC 3748, 2004.
Dokument dostupný na URL:
http://www.faqs.org/rfcs/rfc3748.html (květen 2007).

[28] WPA (Wi-Fi Protected Access), Wi-Fi Alliance, 2003. Dokument dostupný na URL:
http://www.wi-fi.org/knowledge_center/wpa (květen 2007).

[29] Blunk, L., Vollbrecht, J.: PPP Extensible Authentication Protocol, RFC 2284, 1998. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc2284.txt (květen 2007).

[30] IEEE Std 802.11i-2004, Amendment to IEEE Std 802.11, IEEE, 2004. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.11i-2004.pdf (květen 2007).

[31] Housley, R.: Counter with CBC-MAC (CCM), RFC 3610, 2003. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc3610.txt (květen 2007).

[32] Chown, P.: Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), RFC 3268, 2002. Dokument dostupný na URL: ftp://ftp.isi.edu/in-notes/rfc3268.txt (květen 2007).

[33] Schaad, J.: Advanced Encryption Standard Key Wrap Algorithm, RFC 3394, 2002. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc3394.txt (květen 2007).

[34] Dostálek, L.: Velký průvodce protokoly TCP/IP: Bezpečnost, Computer Press, 2003.

[35] Northcut, S., Zeltser, L: Bezpečnost počítačových sítí, Computer Press, 2005.

[36] Dierks, T., Rescorla, E.: The Transport Layer Security (TLS) Protocol, RFC4346, 2006. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc4346.txt (květen 2007).

[37] Freier, A. O., Karlton, P., Kocher, P. C.: The SSL Protocol, 1996. Dokument dostupný na URL: http://wp.netscape.com/eng/ssl3/draft302.txt (květen 2007).

[38] Rigney, C., Willens, S., Simpson, W.: Remote Authentication Dial In User Service (RADIUS), RFC2865, 2000. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc2865.txt (květen 2007).

[39] Rigney, C.: RADIUS Accounting, RFC2866, 2000. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc2866.txt (květen 2007).

[40] Calhoun, P., Loughney, J., Guttman, E.: Diameter Base Protocol, RFC3588, 2003. Dokument dostupný na URL: http://www.rfc-editor.org/rfc/rfc3588.txt (květen 2007).

[41] Chaplin, C., Kerry, S. J.: Status of Project IEEE 802.11r, IEEE, 2007. Dokument dostupný na URL: http://grouper.ieee.org/groups/802/11/Reports/tgr_update.htm (květen 2007).

[42] Walker, J., Kerry, S. J.: Status of Project IEEE 802.11 Task Group w, IEEE, 2007. Dokument dostupný na URL: http://grouper.ieee.org/groups/802/11/Reports/tgw_update.htm (květen 2007).

[43] Cvrček, D.: Bezpečnost WiFi sítí jinak, BUSLab, 2007. Dokument dostupný na URL: http://swordfish.buslab.org/?p=78 (květen 2007).

[44] Warren, S., Lebak, J., Yao, J.: Interoperability and Security in Wireless Body Area Network Infrastructures, 2005. Dokument dostupný na URL: http://www.ece.uah.edu/~jovanov/papers/embs05_security.pdf (květen 2007).

[45] IEEE Std 802.15.1-2002, IEEE, 2002. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.15.1-2002.pdf (květen 2007).

[46] Pužmanová, R.: Osobní sítě - Bluetooth a IEEE 802.15, 2002. Dokument dostupný na URL: http://www.lupa.cz/clanky/osobni-site-bluetooth-a-ieee-802-15/ (květen 2007).

[47] IEEE Std 802.15.1-2005, IEEE, 2005. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.15.1-2005.pdf (květen 2007).

[48] Khalifa, O.: Security in Bluetooth Technology, 2005. Dokument dostupný na URL: http://www.aims.ac.za/resources/archive/2004/omnia.ps (květen 2007).

[49] Singelée, D.: Security Overview of Bluetooth, 2004. Dokument dostupný na URL: http://www.cosic.esat.kuleuven.be/publications/article-565.pdf (květen 2007).

[50] Walsch, S., Wan, J., Sadlier, A.: Bluetooth Security, 2006. Dokument dostupný na URL: http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group15/index.html (květen 2007).

[51] Laurie, A., Laurie, B.: Bluetooth, 2004. Dokument dostupný na URL: http://www.thebunker.net/resources/bluetooth (květen 2007).

[52] Rhodes, C.: Bluetooth Security, 2006. Dokument dostupný na URL: http://www.infosecwriters.com/text_resources/pdf/Bluetooth_CRhodes.pdf (květen 2007).

[53] Sapronov, K.: Bluetooth, Bluetooth Security and New Year War-nibbling, 2006. Dokument dostupný na URL: http://www.viruslist.com/en/analysis?pubid=181198286 (květen 2007).

[54] IEEE Std 802.15.2-2003, IEEE, 2003. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.15.2-2003.pdf (květen 2007).

[55] IEEE Std 802.15.3-2003, IEEE, 2003. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.15.3-2003.pdf (květen 2007).

[56] IEEE Std 802.15.4-2003, IEEE, 2003. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf (květen 2007).

[57] IEEE Std 802.15.4-2006, IEEE, 2006. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf (květen 2007).

[58] Kysilka, R.: Zigbee, 2003. Dokument dostupný na URL: http://www.lupa.cz/clanky/zigbee (květen 2007).

[59] Sastry, N., Wagner, D.: Security Considerations for IEEE 802.15.4 Networks, 2004. Dokument dostupný na URL: http://www.cs.berkeley.edu/~nks/papers/15.4-wise04.pdf (květen 2007).

[60] Xiao, Y., Chen, H., Sun, B.: MAC Security and Security Overhead Analysis in the IEEE 802.15.4 Wireless Sensor Networks, 2006. Dokument dostupný na URL: http://www.hindawi.com/GetArticle.aspx?doi=10.1155/WCN/2006/93830 (květen 2007).

[61] Reddy, J.: ZigBee Security Specification Overview, Zigbee Alliance, 2005.

[62] IEEE 802.15 WPAN Task Group 5, IEEE, 2007. Dokument dostupný na URL: http://www.ieee802.org/15/pub/TG5.html (květen 2007).

[63] IEEE Std 802.16-2001, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, 2001. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.16-2001.pdf (květen 2007).

[64] IEEE Std 802.16-2004, Part 16: Air Interface for Fixed Broadband Wireless Access Systems, IEEE, 2004. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.16-2004.pdf (květen 2007).

[65] Pužmanová, R.: Širokopásmový Internet aneb Přístupové a domácí sítě, Computer Press, 2004.

[66] Eklund, C., Marks, R. B., Stanwood, K. L.: IEEE Standard 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access, IEEE Communications Magazine, str. 98 - 107, 2002. Dokument dostupný na URL: http://www.ieee802.org/16/docs/02/C80216-02_05.pdf (květen 2007).

[67] Zhou, Y.: Security of IEEE 802.16 in Mesh Mode, 2006. Dokument dostupný na URL: http://winet.ece.ufl.edu/ yzhou/paper/milcom200680216.pdf (květen 2007).

[68] Housley, R., Ford, W., Polk, W.: Internet X.509 Public Key Infrastructure: Certificate and CRL Profile, RFC 2459, 1999. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc2459.txt (květen 2007).

[69] Adams, C., Farrell, S.: Internet X.509 Public Key Infrastructure: Certificate Management Protocols, RFC 2510, 1999. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc2510.txt (květen 2007).

[70] Data Over Cable Service Interface Specifications (DOCSIS), CableLabs, 2007. Dokument dostupný na URL: http://www.cablemodem.com (květen 2007).

[71] Krawczyk, H., Bellare, M., Canetti, R.: HMAC: Keyed-Hashing for Message Authentication, RFC 2104, 1997. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc2104.txt (květen 2007).

[72] Eastlake, D., Jones, P.: US Secure Hash Algorithm 1 (SHA1), RFC 3174, 2001. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc3174.txt (květen 2007).

[73] Rogaway, P.: The Security of DESX, 1996. Dokument dostupný na URL: http://www.cs.ucdavis.edu/~rogaway/papers/cryptobytes.ps (květen 2007).

[74] Barbeau, M.: WiMax/802.16 Threat Analysis, 2005. Dokument dostupný na URL: http://www.scs.carleton.ca/~barbeau/Publications/2005/iq2-barbeau.pdf (květen 2007).

[75] Johnston, D., Walker, J.: Overview of IEEE 802.16 Security, 2004. Dokument dostupný na URL: http://mia.ece.uic.edu/~papers/WWW/Bubbles/segment/WiMax_Security.pdf (květen 2007).

[76] Xu, S., Matthews, M., Huang, Ch.: Security Issues in Privacy and Key Management Protocols of IEEE 802.16, 2006. Dokument dostupný na URL: http://www.cse.sc.edu/~huangct/acmse06cr.pdf (květen 2007).

[77] Poovendran, R., Lee, J., Iwata, T.: The AES-CMAC Algorithm, RFC 4493, 2006. Dokument dostupný na URL: http://www.ietf.org/rfc/rfc4493.txt (květen 2007).

[78] Daley, M., Kammer, R. G.: Data Encryption Standard (DES), NIST, 1999. Dokument dostupný na URL: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (květen 2007).

[79] Pužmanová, R.: Co nového v sítích, nejen bezdrátových?, 2007. Dokument dostupný na URL: http://www.lupa.cz/clanky/co-noveho-v-sitich-nejen-bezdratovych/ (květen 2007).

[80] Aarnikoivu, S., Winter, J.: Mobile Broadband Wireless Access, 2006. Dokument dostupný na URL: http://www.tml.tkk.fi/Opinnot/T-109.7510/2006/reports/MBWA.pdf (květen 2007).

[81] Introduction of the IEEE 802.20 Standard for Mobile Broadband Wireless Access Systems, OFTA, 2004. Dokument dostupný na URL: http://www.ofta.gov.hk/en/ad-comm/rsac/paper/rsac2-2004.pdf (květen 2007).

[82] Lipset, V.: 802.16e vs. 802.20, 2003. Dokument dostupný na URL: http://www.wi-fiplanet.com/columns/article.php/3072471/ (květen 2007).

[83] IEEE P802.20 PAR, IEEE, 2006. Dokument dostupný na URL: http://standards.ieee.org/board/nes/projects/802-20.pdf (květen 2007).

[84] Klerer, M.: Introduction to IEEE 802.20, IEEE, 2003. Dokument dostupný na URL: http://www.ieee802.org/20/P_Docs/IEEE%20802.20%20PD-04.pdf (květen 2007).

[85] Gupta, V.: IEEE P802.21 Tutorial, IEEE, 2006. Dokument dostupný na URL: http://www.ieee802.org/21/Tutorials/802%2021-IEEE-Tutorial.ppt (květen 2007).

[86] IEEE P802.21 PAR, IEEE, 2004. Dokument dostupný na URL: http://www.ieee802.org/21/802_21_PAR.doc (květen 2007).

[87] Kiernan, B.: Completing the Convergence Puzzle: Media Independent Handover, 2006. Dokument dostupný na URL: http://www.ieeevtc.org/vtc2006fall/plenary/kiernan.pdf (květen 2007).

[88] O'Shera, D.: 802.21 ties it all together, 2005. Dokument dostupný na URL: http://telephonyonline.com/mag/telecom_future_seen_technology_65/ (květen 2007).

[89] Stein, J.: Survey of IEEE 802.21 Media Independent Handover Services, 2006. Dokument dostupný na URL: http://www.rajjain.com/cse574-06/ftp/handover/index.html (květen 2007).

[90] IEEE P802.22 PAR, IEEE, 2004. Dokument dostupný na URL: http://www.ieee802.org/22/P802-22_PAR.pdf (květen 2007).

[91] Cordeiro, C., Challapali, K., Birru, D.: IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios, 2006. Dokument dostupný na URL: http://www.academypublisher.com/jcm/vol01/no01/jcm01013847.pdf (květen 2007).

[92] Cordeiro, C., Challapali, K., Ghosh, M.: Cognitive PHY and MAC Layers for Dynamic Spectrum Access and Sharing of TV Bands, 2006. Dokument dostupný na URL: http://www.wtapas.org/final-papers/Cordeiro-TAPAS06-Session-II-1.pdf (květen 2007).

[93] Chouinard, G.: Wireless Regional Area Network, 2004. Dokument dostupný na URL: http://www.rabc.ottawa.on.ca/e/Files/ACF4DD.ppt (květen 2007).

[94] Notor, J.: The Evolution of Spectrum Sharing in the IEEE 802.22 WRAN Standards Process, Rev 2, 2006. Dokument dostupný na URL: http://www.eecs.berkeley.edu/~dtse/3r_notor.ppt (květen 2007).

[95] Weissberger, A. J.: IEEE 802.22 Wireless Regional Area Network (WRAN), 2005. Dokument dostupný na URL: http://www.viodi.com/newsletter/050302/article1.htm (květen 2007).

[96] Lewis, B., Davis, P.: Wireless Networks for Dummies, Wiley, 2004.

[97] Arbaugh, W. A., Shankar, N.: Your 802.11 Wireless Network has No Clothes, 2001. Dokument dostupný na URL: http://www.cs.umd.edu/~waa/wireless.pdf (květen 2007).

[98] Bangolae, S., Bell, C., Qi, E.: Performance study of fast BSS transition using IEEE 802.11r, 2006. Dokument dostupný na URL: http://portal.acm.org/citation.cfm?id=1143696 (květen 2007).

[99] Barken, L., aj.: Wireless Hacking, Syngress, 2004.

[100] Casole, M.: WLAN security - Status, Problems and Perspective, 2002. Dokument dostupný na URL: http://www2.ing.unipi.it/ew2002/proceedings/sec002.pdf (květen 2007).

[101] Chandra, P.: Bulletproof Wireless Security, Elsevier, 2005.

[102] Earle, A. E.: Wireless Security Handbook, Auerbach Publications, 2006.

[103] Farshchi, J.: Wireless Intrusion Detection Systems, 2003. Dokument dostupný na URL: http://www.securityfocus.com/infocus/1742 (květen 2007).

[104] Lehembre, G.: Wi-Fi security - WEP, WPA and WPA2, 2005. Dokument dostupný na URL: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf (květen 2007).

[105] Maxim, M., Pollino, D.: Wireless Security, McGraw-Hill, 2002.

[106] Nichols, R., Lekkas, P.: Wireless Security - Models, Threats, and Solutions, 2002.

[107] Pužmanová, R.: Bezpečnost bezdrátové komunikace, Computer Press, 2005.

[108] Randal, N., Sosinsky, B.: Wireless Solutions, PC Magazine, 2005.

[109] Schauer, H.: Wireless LAN Security, 2003. Dokument dostupný na URL: http://hsc.fr/ressources/presentations/ecmwf-wireless/ecmwf-wireless.pdf (květen 2007).

[110] Tafazolli, R.: Technologies for the Wireless Future, Wiley, 2006.

[111] Vines, R. D.: Wireless Security Essentials, Wiley, 2002.

[112] Higgins, K. J.: Bluetooth Security Worse Than WiFi, 2007. Dokument dostupný na URL: http://www.darkreading.com/document.asp?doc_id=114424 (květen 2007).

[113] Lemos, R.: Expert: Gaps still pain Bluetooth security, 2004. Dokument dostupný na URL: http://http://news.com.com/2100-1009-5197200.html (květen 2007).

[114] Mavrogiannopoulos, N.: On Bluetooth security, 2005. Dokument dostupný na URL: http://members.hellug.gr/nmav/papers/other/Bluetooth%20security.pdf (květen 2007).

[115] Mikkola, L.: Bluetooth Security, 2004. Dokument dostupný na URL: http://www.netlab.tkk.fi/opetus/s38153/k2004/Lectures/1 (květen 2007).

[116] Sun, J., aj.: Desing, Implementation, and Evaluation of Bluetooth Security, 2001. Dokument dostupný na URL: http://www.mediateam.oulu.fi/publications/pdf/87.pdf (květen 2007).

[117] Traskback, M.: Security of Bluetooth: An overview of Bluetooth Security, 2001. Dokument dostupný na URL: http://www.cs.hut.fi/Opinnot/Tik-86.174/Bluetooth_Security.pdf (květen 2007).

[118] Zetter, K.: Security Cavities Ail Bluetooth, 2004. Dokument dostupný na URL: http://www.wired.com/politics/security/news/2004/08/64463 (květen 2007).

[119] Decuir, J.: Introduction to Ultra Wide Band, 2005. Dokument dostupný na URL: http://www.pcca.org/standards/architecture/mcci_uwb.pdf (květen 2007).

[120] Hunt, P.: Understanding WiMedia Association models and security, 2006. Dokument dostupný na URL: http://rfdesign.com/mag/611RFDE8AssocModelsv2.pdf (květen 2007).

[121] Jin, J.: Ultra-Wideband (UWB), 2006. Dokument dostupný na URL: http://www.tml.tkk.fi/Opinnot/T-109.7510/2006/reports/UWB.doc (květen 2007).

[122] Pužmanová, R.: UltraWideBand, 2004. Dokument dostupný na URL: http://www.lupa.cz/clanky/ultrawideband/ (květen 2007).

[123] Singer, A.: Introduction to the IEEE 802.15.3 Security Architecture, 2002. Dokument dostupný na URL: http://www.securemulticast.org/GSEC/gsec3_ietf53_Singer.pdf (květen 2007).

[124] Bhavsar, V.: ZigBee, 2005. Dokument dostupný na URL: http://www.isi.edu/ weiye/teaching/cs558sp05/presentations/Zigbee.pdf (květen 2007).

[125] Ergen, S. C.: ZigBee/IEEE 802.15.4 Summary, 2004. Dokument dostupný na URL: http://www.cs.wisc.edu/ suman/courses/838/papers/zigbee.pdf (květen 2007).

[126] Koubaa, A., Alves, M., Tovar, E.: IEEE 802.15.4: a wireless communication technology for large-scale ubiquitous computing applications, 2005. Dokument dostupný na URL: http://ubicomp.algoritmi.uminho.pt/csmu/proc/koubaa-129.pdf (květen 2007).

[127] Myers, S.: ZigBee/IEEE 802.15.4, 2006. Dokument dostupný na URL: http://www.cs.wisc.edu/~suman/courses/838/f06/zigbee-myers-talk.pdf (květen 2007).

[128] Walters, J. P., aj.: Wireless Sensor Network Security: A Survey, 2006. Dokument dostupný na URL: http://www.cs.wayne.edu/~weisong/papers/walters05-wsn-security-survey.pdf (květen 2007).

[129] Yuyiang, Y.: ZigBee IEEE 802.15.4, 2005. Dokument dostupný na URL: http://www.sasase.ics.keio.ac.jp/jugyo/2005/print/zigbee_p.pdf (květen 2007).

[130] Zheng, J., Lee, M. J.: A Comprehensive Performance Study of IEEE 802.15.4. Dokument dostupný na URL: http://ees2cy.engr.ccny.cuny.edu/zheng/pub/file/wpan_press.pdf (květen 2007).

[131] IEEE Std 802.16e-2005, IEEE, 2005. Dokument dostupný na URL: http://standards.ieee.org/getieee802/download/802.16e-2005.pdf (květen 2007).

[132] Technical Tutorial Articles on IEEE 802.16, IEEE, 2007. Dokument dostupný na URL: http://www.ieee802.org/16/tutorial/index.html (květen 2007).

[133] Ansari, N.: WiMAX Security: Privacy Key Management, 2007. Dokument dostupný na URL: http://www.it.ecei.tohoku.ac.jp/~kato/workshop2007/01.pdf (květen 2007).

[134] Cordova, H., Boets, P., Biesen, L. V.: Insight Analysis into WI-MAX Standard and its trends, 2007. Dokument dostupný na URL: http://www.ctr.kcl.ac.uk/iwwan2005/papers/72.pdf (květen 2007).

[135] Johnston, D., Walker, J.: 802.16 Security Enhancements, 2003. Dokument dostupný na URL: http://www.ieee802.org/16/tgd/contrib/C80216d-03_60.pdf (květen 2007).

[136] Kaki, J.: 802.16 Security, 2005. Dokument dostupný na URL: http://www.cs.tut.fi/~83180/83180_05_S10c.ppt (květen 2007).

[137] Laskar, J. J.: Concept of Secure Wireless Metropolitan Area Network (SWMAN) in a Mobile Computing Environment, 2004. Dokument dostupný na URL: http://www.scs.org/getDoc.cfm?id=1640 (květen 2007).

[138] Mylavarapu, R.: Security considerations for WiMAX-based converged network, 2005. Dokument dostupný na URL: http://rfdesign.com/mag/508RFDF1.pdf (květen 2007).

[139] Omerovic, S.: WiMax Overview, University of Ljubljana, 2006. Dokument dostupný na URL: http://www.lkn.fe.uni-lj.si/publikacije/Seminarji_06/mobilne/s_omerovic.pdf (květen 2007).

[140] Pužmanová, R.: Bezpečnost ve WiMAX, 2007. Dokument dostupný na URL: http://www.wimax.cz/index.php?option=com_content&task=view&id=172&Itemid=33 (květen 2007).

[141] Pužmanová, R.: Mobilní WiMAX: management a politika bezpečnosti, 2006. Dokument dostupný na URL: http://www.wimax.cz/index.php?option=com_content&task=view&id=171&Itemid=33 (květen 2007).

[142] Pužmanová, R.: Normalizace WiMAX: přehled a vývoj, 2005.
Dokument dostupný na URL:
http://www.wimax.cz/index.php?option=com_content&task=view&id=56&Itemid=33
(květen 2007).

[143] Pužmanová, R.: Technologi WiMAX, 2005. Dokument dostupný na URL:
http://www.wimax.cz/index.php?option=com_content&task=view&id=48&Itemid=33
(květen 2007).

[144] Pužmanová, R.: Technologie mobilního WiMAX, 2006. Dokument dostupný na URL:
http://www.wimax.cz/index.php?option=com_content&task=view&id=122&Itemid=33
(květen 2007).

[145] Wongthavarawat, K.: IEEE 802.16 WiMax Security, 2005.
Dokument dostupný na URL:
http://www.first.org/conference/2005/papers/kitti-wongthavarawat-slides-1.pdf
(květen 2007).

[146] Wright, J.: WiMAX security issues, 2006. Dokument dostupný na URL:
http://www.networkworld.com/columnists/2006/121106-wireless-security.html
(květen 2007).

[147] Wu, S.: The 802.16 WirelessMAN, 2005. Dokument dostupný na URL:
http://www.auburn.edu/~jiyimin/paper/The802.16WirelessMAN.ppt
(květen 2007).

[148] Hardjono, T.: Security in Wireless LANs and MANs, Artech House, 2005.

[149] Ibe, O. C.: Fixed Broadband Wireless Access Networks and Services, Wiley, 2002.

[150] Eklund, C., aj.: WirelessMAN: Inside the IEEE 802.16 Standard for Wireless Metropolitan Area Networks , IEEE Press, 2006.

[151] Bersani, F.: Moving forward on IEEE 802.20 security: where are we and where want to go?, IEEE, 2004. Dokument dostupný na URL:
http://www.ieee802.org/20/Contribs/C802.20-04-62r1.ppt (květen 2007).

[152] System Requirements for IEEE 802.20 Mobile Broadband Wireless Access Systems, Version 14, Draft 802.20 Permanent Document, IEEE, 2004.
Dokument dostupný na URL:
http://www.ieee802.org/20/P_Docs/IEEE%20802.20%20PD-06r1.doc
(květen 2007).

[153] Zou, F., aj.: IEEE 802.20 Based Broadband Railroad Digital Network.
Dokument dostupný na URL:
http://129.118.51.86/zlin/pdf/BDRN-ICEB04.pdf (květen 2007).

[154] Olexa, R.: Implementing 802.11, 802.16, and 802.20 Wireless Networks, 2005.

[155] Albanese, R.: Handover issues in heterogenous environments, 2006.
Dokument dostupný na URL:
http://net.infocom.uniroma1.it/seminari/pdf/seminario_albanese_handover.pdf
(květen 2007).

[156] Dutta, A., aj.: Secured Seamless Convergence across Heterogenous Access Networks, 2006. Dokument dostupný na URL: http://www1.cs.columbia.edu/~dutta/research/dutta-wtc-full-paper-submit.pdf (květen 2007).

[157] Chouinard, G.: Status of work in the IEEE 802.22 WG, 2005. Dokument dostupný na URL: http://www.rabc.ottawa.on.ca/e/Files/RABC%20802.22%20Presentation.ppt (květen 2007).

[158] Cordeiro, C.: Report on IEEE 802.22, 2006. Dokument dostupný na URL: http://www.eecs.ucf.edu/tccn/meetings/Report_06.ppt (květen 2007).

[159] Hu, W., aj.: Dynamic Frequency Hopping Communities for Efficient IEEE 802.22 Operation, 2005. Dokument dostupný na URL: http://www.tkn.tu-berlin.de/publications/papers/neue_journalpublikation.pdf (květen 2007).

[160] Mangold, S., Jarosch, A., Monney, C: Cognitive Radio - Trends and Research Challenges, 2005. Dokument dostupný na URL: http://www.swisscom-comtec.ch/pdf/comtec032005242.pdf (květen 2007).

[161] Sutherland, E.: 16 vs. 22: Which Will Get the TV Spectrum?, 2005. Dokument dostupný na URL: http://www.wi-fiplanet.com/columns/article.php/3494676 (květen 2007).

Seznam zkratek a symbolů

AAA	Authentication-Authorization-Accounting
ACK	Acknowledge
ACL	Access Control List / Asynchronous Connection Less
ACO	Authenticated Ciphering Offset
AES	Advanced Encryption Standard
AFH	Adaptive Frequency Hopping
AIDS	Anomaly-based Intrusion Detection System
AK	Authorization Key
AKA	Authentication and Key Agreement
ANSI	American National Standards Institute
AP	Access Point
APL	ZigBee Application Layer
APS	ZigBee Application Support Sublayer
ARP	Address Resolution Protocol
ARQ	Automatic Repeat Request
AS	Authentication Server
ASCII	American Standard Code for Information Interchange
AU_RAND	Authentication Random Number
BBC	The British Broadcasting Corporation
BD_ADDR	Bluetooth Device Address
BPI+	Baseline Privacy Interface Plus Specification
BPSK	Binary Phase Shift Keying
BS	Base Station
BSS	Basis Service Set
BWA	Broadband Wireless Access
CA	Certification Authority
CBC	Cipher Block Chaining
CBC-MAC	Cipher Block Chaining Message Authentication Code
CDMA	Code Division Multiple Access
CEPT	European Conference of Postal and Telecommunications Administrations
CER	Crossover Error Rate
CID	Connection Identifier
CMAC	Cipher-based Message Authentication Code
CN	Core Network
CPE	Customer Premise Equipment
CPS	Common Part Sublayer
CRC	Cyclic Redundancy Check
CRTC	Canadian Radio-television and Telecommunications Commission

CSMA/CA	Carrier Sense Multiple Access With Collision Avoidance
CSS	Chirp Spread Spectrum / Cascading Style Sheets
CTN	Candidate Target Network
CTR	Counter Mode
CTS	Clear To Send
ČTÚ	Český Telekomunikační Úřad
DCF	Distributed Coordination Function
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DEV	Device
DFWMAC	Distributed Foundation Wireless MAC
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specifications
DOM	Document Object Model
DoS	Denial of Service
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EAPOR	EAP Over RADIUS
EAPOW	EAP Over Wireless
ECB	Electronic Code Book
EN_RAND	Encryption Random Number
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
ETSI	European Telecommunications Standards Institute
FAST	Flexible Authentication via Secure Tunnelling
FBWA	Fixed Broadband Wireless Access
FCC	Federal Communications Commission
FDD	Frequency Division Duplex
FEC	Forward Error Correction
FFD	Full Function Device
FHSS	Frequency Hopping Spread Spectrum
FNR	False Negative Rate
FPR	False Positive Rate
GEK	Group Encryption Key
GIK	Group Integrity Key
GMH	Generic MAC Header
GMK	Group Master Key
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
GSS	Generic Security Service
GTK	Group Transient Key
HARQ	Hybrid Automatic Repeat Request
HDLC	High-level Data Link Control

HIDS	Host-based Intrusion Detection System
HIPERACCESS	High Performance Radio Access
HIPERLAN	High Performance Radio Local Area Network
HIPERMAN	High Performance Radio Metropolitan Area Network
HMAC	Hashed Message Authenticated Code
HTML	Hypertext Markup Language
HUMAN	High-speed Unlicensed Metropolitan Area Network
IAPP	Inter Access Point Protocol
ICMP	Internet Control Message Protocol
IBSS	Independent Basis Service Set
IBSSID	Independent Basis Service Set Identifier
ICV	Integrity Check Value
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IEEE-SA	IEEE Standards Association
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security Protocol
IR	Infrared
IrDA	Infrared Data Association
ISM	Industrial, Scientific, Medical
ISO	International Organization for Standardization
ITU	International Telecommunication Union
IV	Initialization Vector
K_A	Unit Key
K_{AB}	Combination Key
K_c	Encryption Key
K_{init}	Initialization Key
K_{master}	Master Key
KCK	Key Confirmation Key
KEK	Key Encryption Key
KeyID	Key Identifier
KSA	Key Scheduling Algorithm
LAN	Local Area Network
LEAP	Lightweight EAP
LLC	Logical Link Control
LMSC	IEEE 802 LAN/MAN Standards Committee
LR-WPAN	Low Rate WPAN
L2F	Layer-2 Forwarding
L2TP	Layer-2 Tunnelling Protocol
M	Master
MAC	Medium Access Control
MBWA	Mobile Broadband Wireless Access
MD5	Message Digest 5
MIC	Message Integrity Check
MICS	Media Independent Command Service
MIES	Media Independent Event Service
MIH	Media Independent Handover

MIHF	Media Independent Handover Function
MIIS	Media Independent Information Service
MITM	Man-In-The-Middle
MK	Master Key
Mobile-Fi	Mobile Fidelity
MPA	Media-independent Pre-Authentication
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NAS	Network Access Server
NIDS	Network-based Intrusion Detection System
NWK	ZigBee Network Layer
Ofcom	Office of Telecommunications
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiplexing Advanced
O-QPSK	Offset Quadrature Phase Shift Keying
OSI	Open Systems Interconnection
P	Parked
PAE	Port Access Entity / Password Authenticated Exchange
PAN	Personal Area Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PEAP	Protected EAP
PIN	Personal Identification Number
PKM	Privacy Key Management
PMK	Pair-wise Master Key
PNC	Piconet Coordinator
PPK	Per-Packet Key
PPTP	Point-to-Point Tunnelling Protocol
PRF	Pseudo-Random Function
PTK	Pair-wise Transient Key
POS	Personal Operating Space
PPP	Point-to-Point Protocol
PRNG	Pseudo-Random Number Generator
PSK	Pre-Shared Key
PTP	Point-To-Point
PTMP	Point-To-Multipoint
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial In User Service
RC4	Ron's Code No. 4
RFD	Reduce Function Device
RM ISO/OSI	Reference Model ISO/OSI
RSA	Rivest Shamir Adleman
RSN	Robust Security Network
RTS	Request To Send

S	Slave
SA	Security Association
SAID	Security Association Identifier
SAKE	Shared-secret Authentication and Key Establishment
SAX	Simple API for XML
SB	Stand-By
SC	Single Carrier
SCa	Single Carrier
SCO	Synchronous Connection Oriented
SCTP	Stream Control Transmission Protocol
SG	Study Group
SHA	Secure Hash Algorithm
SIDS	Signature-based Intrusion Detection System
SIG	Special Interest Group
SIM	Subscriber Identity Module
SKE	Shared Key Exchange
SNAP	Subnetwork Access Protocol
SOFDMA	Scalable Orthogonal Frequency Division Multiplexing Advanced
SRES	Signed Response
SS	Subscriber Station / Security Sublayer
SSCS	Service Specific Convergence Sublayer
SSID	Service Set Identifier
SSL	Secure Sockets Layer
STA	Station
TACACS	Terminal Access Controller Access-Control System
TAG	Technical Advisory Group
TCM	Trellis Coded Modulation
TCP	Transmission Control Protocol
TDD	Time Division Duplex
3DES	Triple Data Encryption Standard
TDMA	Time Division Multiple Access
TEK	Temporary Encryption Key / Traffic Encryption Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TLV	Type-Length-Value
TMK	Temporary MIC Key
TSC	TKIP Sequence Counter
TSN	Transient Security Network
TTAC	TKIP-mixed Transmit Address and Key
TTLS	Tunnelled Transport Layer Security
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UMTS	Universal Mobile Telecommunications System
UWB	Ultra Wide Band
VHF	Very High Frequency
VLAN	Virtual LAN
VoWLAN	Voice Over WLAN
VPN	Virtual Private Network

WBAN	Wireless Body Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WG	Working Group
Wi-Fi	Wireless Fidelity
WIDS	Wireless Intrusion Detection System
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WLANA	Wireless LAN Association
WLL	Wireless Local Loop
WMAN	Wireless Metropolitan Area Network
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WRAN	Wireless Regional Area Network
WSN	Wireless Sensor Network
xDSL	x Digital Subscriber Line
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations
ZDO	ZigBee Device Object

Seznam příloh

Příloha 1: CD s elektronickou verzí technické zprávy a realizačními výstupy