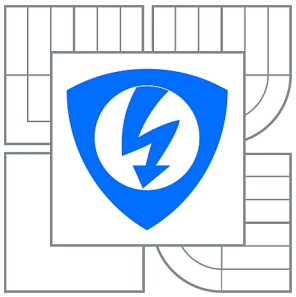
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MULTIMEDIÁLNÍ SLUŽBY V BEZDRÁTOVÝCH SÍTÍCH

MULTIMEDIA SERVICES IN WIRELESS NETWORKS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

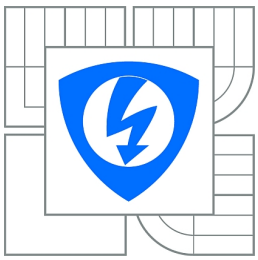
AUTOR PRÁCE — Bc. PETER BUČINA

AUTHOR

VEDOUCÍ PRÁCE — Ing. TOMÁŠ MÁCHA

SUPERVISOR

BRNO 2012



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student: Bc. Peter Bučina ***ID:*** 101847
Ročník: 2 ***Akademický rok:*** 2011/2012

NÁZEV TÉMATU:

Multimediální služby v bezdrátových sítích

POKYNY PRO VYPRACOVÁNÍ:

V průběhu řešení práce budou vytvořeny tři nové laboratorní úlohy. Nová akviziční jednotka bude sloužit jako softwarová pobočková ústředna spravující koncové uživatele, a zároveň bude sloužit pro sběr a zpracování dat určených k analýze multimediálních přenosů iniciovaných zakoupenými telefony, videotelefonem nebo kamerou. První úloha se bude zabývat problematikou QoS (Quality of Service) kabelových a bezdrátových komunikačních sítí, zejména integrací telekomunikačních služeb a sítí a analýzou způsobu přenosu dat v těchto sítích. Náplní druhé úlohy bude prozkoumat možnosti konvergované paketové sítě vytvořené pro videotelefonii mezi hardwarovým videotelefonem, softwarovým videotelefonem a pohyblivým účastníkem. Třetí úloha bude zaměřena na analýzu topologie a přenosu dat v konvergovaných bezdrátových sítích, zabývající se vzdáleným přístupem pohyblivého účastníka na video stream bezdrátové IP kamery.

DOPORUČENÁ LITERATURA:

[1] LABIOD, H., AFIFI, H., SANTIS, C. Wi-Fi(TM), Bluetooth(TM), Zigbee(TM) and WiMax(TM). Springer. 2007. ISBN-10: 978-1-4020-5396-2.

[2] MOLISCH, A., F. Wireless Communications, 2nd Edition. Wiley. 2010. ISBN: 978-0-470-74187-0.

Termín zadání: 6.2.2012 ***Termín odevzdání:*** 24.5.2012

Vedoucí práce: Ing. Tomáš Mácha
Konzultanti diplomové práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

ANOTACE

Hlavním tématem diplomové práce je problematika bezdrátových sítí především standardu IEEE 802.11. Teoretická část práce je rozdělena na tři hlavní kapitoly. Zaobírá se základním přehledem standardů, architektury, využití rádiového spektra a modulačních technik při zpracování signálu. Dále popisuje základní zabezpečení a požadavky na kvalitu služeb v bezdrátových WLAN sítích. Práci doplňují dvě samostatné laboratorní úlohy, ve kterých je popsán postup k vybrané problematice.

První z nich řeší způsoby prolomení šifrovaného protokolu WEP a WPA v bezdrátových WLAN sítích. K tomu byl použit linuxový program BackTrack 5, který poskytuje kompletní sadu nástrojů určených k testování zabezpečení WLAN sítí.

Druhá úloha se zabývá praktickými možnostmi proudového vysílání (video stream) v konvergovaných bezdrátových sítích a se vzdáleným přístupem mobilních účastníků na stream bezdrátové IP kamery.

Klíčová slova: IEEE 802.11, infrastrukturní mód, přístupový bod, bezpečnost, video stream.

ABSTRACT

The main topic of my diploma thesis is dedicated to the issue of wireless networks mostly aimed at IEEE 802.11 standard. Theoretical part of the thesis is divided into three main chapters. It deals with basic overview of standards, architecture, utilization of radio spectrum and modulating techniques in signal processing. Further, it describes basic security measures and quality of service requirements in WLAN networks. The thesis is complemented by two separate laboratory assignments focused on procedure related to the chosen problematic.

The first assignment handles common steps to break ciphered protocols WEP and WPA in WLAN's. Linux software called Back Track 5 was used to provide complete package of tools for WLAN security tests.

The second one is aimed at practical options on video streaming in converged wireless networks and also at remote access of mobile users to wireless IP camera video stream.

Keywords: IEEE 802.11, infrastructural mode, access point, security, video stream.

BUČINA, P. *Multimediální služby v bezdrátových sítích*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. 2012. 52 s. Vedoucí diplomové práce Ing. Tomáš Mácha.

PROHLÁŠENÍ

Prohlašuji, že svoji diplomovou práci na téma Multimediální služby v bezdrátových sítích jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením tohoto projektu jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.

V Brně dne ....

(podpis autora)

Poděkování

Děkuji vedoucímu diplomové práce Ing. Tomáši Máchovi za velmi užitečnou metodickou pomoc a cenné rady při zpracování diplomové práce.

V Brně dne…… .....

podpis autora

SIX research centre
sensor, information and communication systems

Faculty of Electrical Engineering
and Communication

Brno University of Technology
Purkynova 118, CZ-61200 Brno, Czechia

http://www.six.feec.vutbr.cz

Výzkum popsaný v této diplomové práci byl realizován v laboratořích podpořených z projektu SIX; registrační číslo CZ.1.05/2.1.00/03.0072, operační program Výzkum a vývoj pro inovace.

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

2007–13
OP Výzkum a vývoj pro inovace

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Bezdrátové sítě WLAN jsou v běžném životě velmi populární a získávají si stále více nadšenců. V devadesátých letech byla bezdrátová komunikace základem mobilních sítí. Lidé si rychle zvykli na komfort být mobilní kdekoliv a kdykoliv. S nástupem vysokorychlostního internetu byla kladena otázka, zda-li je možné, kromě hovorů přenášet i data podobnou rychlostí. V roce 1992 vznikla pod záštitou neziskové mezinárodní organizace IEEE (Institut pro elektrotechnické a elektronické inženýrství) jedenáctá pracovní skupina 802.11, která v roce 1997 vydala soubor protokolů a pravidel (standardů) pro vysokorychlostní bezdrátový přenos dat. Samotná technologie se opírá o přenos elektromagnetických vln vzduchovým médiem. Kmitočet, na kterém současné bezdrátové sítě pracují, byl zvolen tak, aby se jejich frekvenční pásmo nekrylo s pásmem jiných technologií (rádio, TV, CB, KV).

Bezdrátové sítě se dělí na několik podskupin podle své velikosti nebo použité technologie. Jedním z hlavních cílů bylo tyto sítě implementovat a propojit s pozemními drátovými sítěmi. Ze začátku byli WLAN sítě a jejich zařízení moc drahé a s konkurenční Ethernetovou technologií neměly šanci na úspěch, aspoň, co se rychlosti přenosu dat týče. Dnes je ovšem situace jiná a s rapidním vývojem IEEE 802.11 standardů a jeho doplňků se zvýšila její atraktivita.

Diplomová práce se zabývá základní problematikou bezdrátových sítí. Práce je členěna na pět hlavních kapitol a šestou poslední kapitolu, v které jsou shrnuty dosáhnuté výsledky. První kapitola obsahuje několik podkapitol. Podkapitola 1.1 se zabývá rozdělením WLAN sítí podle velikosti a použitých technologií. Podkapitola 1.2 popisuje vývoj jednotlivých standardů a jejich základních vlastností. Charakteristika WLAN sítí a využití v rozličných oblastech je probrána v podkapitole 1.3. Základní architektuře Wi-Fi sítí je věnována podkapitola 1.4. V podkapitole 1.5 se práce blíže zaobírá využitím pracovních pásem 2,4 GHz a 5 GHz. Podkapitola 1.6 stručně popisuje fyzickou a linkovou vrstvu standardu IEEE 802.11. Základní techniky zpracování signálu při přenosu v rozprostřeném spektru, jsou popsány v poslední podkapitole 1.7.

Druhá kapitola se zabývá bezpečností WLAN sítí a způsoby šifrování informace v bezdrátové komunikační cestě.

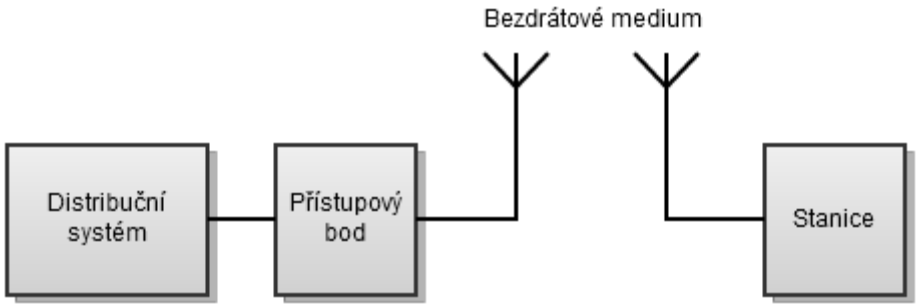
Kapitola třetí popisuje základní parametry při dosahování určitého stupně kvality služeb ve WLAN sítích.

Ve čtvrté kapitole práce popisuje laboratorní postup při testování bezpečnosti bezdrátových sítí standardu IEEE 802.11. Testování je zaměřeno na současné slabiny šifrovacích protokolů WEP a WPA, za využití volně dostupného linuxového balíčku Back Track 5.

Pátá hlavní kapitola se zabývá možnostmi bezdrátového přenosu video streamu v rámci konvergované WLAN sítě s využitím bezdrátové IP kamery v laboratorních podmínkách.

1 BEZDRÁTOVÉ SÍTĚ

Bezdrátové komunikace v současné době poskytují obrovskou dávku volnosti a svobody. Pomalu se zbavujeme nadbytečných kabelů, které dnes nahrazuje radiový spoj schopný napodobit jejich vlastnosti. Lidem se tak otevírají nové možnosti být „online“ všude, kde potřebují a navíc za dostupnou cenu. Téměř všude na světě ve vyspělých zemích se vyskytují místa (kavárny, restaurace, letiště a jiná veřejná místa), kde se mohou lidé připojit pomocí svých laptopů, iPhonů, PDA zařízení do veřejné sítě Internet. Tato místa se nazývají anglicky „hotspots“ a jsou to oblasti, kde jako prostředník mezi pevnou Ethernetovou sítí operují přístupové body (Access Points) viz obr. č. 1. Obvykle je připojení zadarmo. A právě pro tyto a jiné vlastnosti se bezdrátové sítě využívají více a více v každodenním životě. Tomu podléhá i neustálý vývoj bezdrátové technologie.



Obrázek 1. *Základní elementy bezdrátových sítí.*

1.1 Základní rozdělení bezdrátových sítí

Podle dosahu a velikosti pokrytí určité geografické oblasti rozlišujeme několik typů bezdrátových sítí [1]:

- **Wireless Body Area Network (WBAN)** pokrývá oblast, kde spolu komunikují zařízení přilehlé jedné osobě (např. mobilní headset do ucha). Dosah obvykle 1m.
- **Wireless Personal Area Network (WPAN)** tvoří síť v okolí 10m a je populární ve výpočetní technice (klávesnice, myši, tiskárny) a zábavních systémech (domácí kina, sluchátka).
- **Wireless Local Area Network (WLAN)** má využití v okolí cca 100m. Je realizovaná spojením několika uživatelských mobilních stanic přes přístupový bod (AP), který poskytuje rozhraní s distribuční sítí. Takto se mohou propojit na krátké vzdálenosti jednotlivé sítě v rámci města, dvou či více budov (firemní oddělení)
- **Wireless Metropolitan Area Network (WMAN)** pokrývá svým signálem rozlohu až 50km a vzniká spojením více WLAN sítí.

- **Wireless Wide Area Network (WWAN)** je sítí, která spájí příměstské části, sousední města a oblasti v dosahu několik desítek kilometrů.

Na sestavení různých typů sítí se používají také jiné technologie, které pracují v těchto kmitočtových pásmech:

- **Bluetooth IEEE 802.15** (WBAN, WPAN) pracuje v pásmu 2400 - 2480 MHz.
- **Wi-Fi (Wireless Fidelity) IEEE 802.11** (WLAN) pracuje v pásmech 2.4 GHz a 5 GHz.
- **ZigBee IEEE 802.15.4** (WPAN) pracuje v pásmu 2.4 GHz.
- **WiMax IEEE 802.16** (WMAN) pracuje v pásmu 2.3 GHz, 2.4 GHz a 3.5 GHz.

Ústředním tématem této práce, bude především technologie Wi-Fi 802.11, která byla publikována v roce 1997 mezinárodní standardizační institucí IEEE. Od tohoto roku se technologie neustále vyvíjí a jsou vydávány opravy a dodatky původního standardu 802.11. Kompletní přehled standardů a jejich doplňků je popsán v následující podkapitole.

1.2 Vývoj IEEE 802.11

Od svého vzniku se vývoj Wi-Fi standardů neustále zdokonaluje a dosahuje jistou dávku dospělosti. S nástupem vysokorychlostního internetu se zvyšovala také jeho popularita. S vývojem nových technologií vznikají nové standardy, které mají za úkol zlepšit vlastnosti stávajících standardů (např. snížení výkonu antén, úspora energie, zvýšení přenosové rychlosti a bezpečnosti). Za vývojem těchto norem stojí organizace IEEE (Institute of Electrical and Electronics Engineers), která v roce 1992 zformovala pracovní skupinu s názvem 802.11. Další organizace Wi-Fi Alliance (dříve WECA) testuje zařízení od mnoha výrobců a zajišťuje tak jejich funkčnost a kompatibilitu. Takto certifikované výrobky pak nesou její logo a jsou zárukou kompatibility s jinými výrobky. Ovšem jsou na trhu i výrobky bez certifikace (laciné výrobky z Asie). To však neznamená, že nemohou mezi sebou spolupracovat. Většina výrobců o certifikaci nemusí požádat a i bez ní mohou splňovat kritéria skupiny 802.11. Za zmínku stojí také organizace ETSI (European Telecommunications Standards Institute), která vyvinula konkurenční standard HIPERLAN [2].

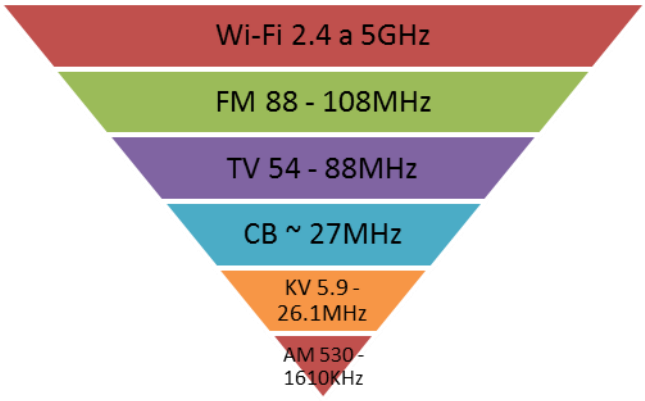
Většina důležitých standardů IEEE 802.11 (tučně označené) a jejich doplňků je popsána níže [1]:

- 802.11 – (1997) přenosová rychlost 1 a 2Mbps. Pracovní frekvence 2,4GHz, v které pracují také bluetooth a infračervené technologie, mikrovlnné trouby a některé bezdrátové telefony.
- **802.11b** – (1999) vylepšení 802.11 a zvýšení rychlosti na 5.5 Mbps a 11 Mbps.
- **802.11a** – (1999) pracovní kmitočet 5 GHz a rychlost přenosu 6 Mbps až 54 Mbps.
- **802.11g** – (2003) umožnuje větší rychlost přenosu dat (54 Mbps, stejně jako 802.11a) avšak na frekvenci 2,4 GHz. Využívá modulace OFDM. Zpětná kompatibilita s 802.11b.
- 802.11d – (2001) rozšíření mezistátního roamingu, úprava standardu 802.11b k využívaní kmitočtu jiného než 2.4 GHz, především kmitočtu 5 GHz.

- 802.11c - (1998) doplněk standardu 802.11d. Specifikuje komunikaci pomocí přístupových bodů (AP access points).
- 802.11e – (2005) je vylepšením 802.11 linkové vrstvy (Media Access Control) z hlediska dosahovaní kvality služeb (QoS). Původní 802.11 MAC vrstva používá dvě funkce přístupu a sdílení média (DCF a PCF). Obě vylepšuje hybridní koordinační funkce (HFC), která má dvě metody přístupu k médiu – HCCA(HCF Controlled Channel Access) a EDCA (Enhanced DCF Channel Access). Je aplikovaná na standardy 802.11a/b/g.
- 802.11f – (2003) komunikace mezi přístupovými body (AP).
- 802.11h – (2004) možnost obsluhy spektra 5 GHz pro 802.11a v Evropě.
- 802.11i – (2004) zvýšená bezpečnost. Aplikovaná na standardy 802.11a/b/g.
- 802.1X – poskytuje zabezpečený přístup pro několik typů médií včetně bezdrátového a to na základě silných autentizačních procedur při distribuci dynamického klíče.
- 802.11j – specifikace standardů pro Japonsko.
- 802.11k – vylepšení RRM (Radio Resource Measurement) vede k definování metod a měřících kritérií, které vyžadují protokoly vyšších vrstev k správě a údržbě funkcí.
- **802.11n** – vysokorychlostní přenos dat (108 Mbps až 600 Mbps) v pásmech 2.4 GHz a 5 GHz.
- 802.11p – bezdrátový přístup pro dopravní prostředky zvaný WAVE.
- 802.11r – rychlejší roaming mezi AP.
- 802.11s – bezdrátové sítě typu „mesh“.
- 802.11T – předpověď bezdrátového výkonu pomocí testovacích metod.
- 802.11u – kooperace se sítěmi jiných technologii, např. mobilní GSM.
- 802.11v – správa bezdrátových sítí a jejich prvků.
- 802.11w – ochrana rámců určených na správu zařízení.
- 802.11y – pracovní pásmo 3650 – 3700 MHz určené pro USA.

1.3 Charakteristika WLAN sítí a jejich vývoj

Technologie WLAN se opírá o přenos informací pomocí rádiových vln z jednoho zdroje (vysílače) k druhému (přijímač). Aby mohla tímto způsobem pracovat, musí využívat frekvence, která se nekryje s frekvencí jiných dosud známých technologií (viz obr. č. 2). Bezdrátové WLAN sítě tak využívají nelicencované ISM (Průmyslové, vědecké a lékařské) pásma 2,4 GHz a 5 GHz.



Obrázek 2. *Využití frekvenčního pásma [3].*

Hlavními vlastnostmi WLAN jsou [1]:

- Možnost vysílat ve volném bez-licenčním pásmu.
- Připojení k LAN sítím.
- Celosvětová kompatibilita díky standardům.
- Vyšší teoretické propustnosti než UMTS standardy třetí generace (3G).
- Nízká cena sítových prvků (AP a bezdrátových karet) a jejich provedení. Celkové náklady jsou konkurence-schopné s 3G mobilními sítěmi (licence a zařízení).
- Podpora roamingu/handoff mezi přístupovými body.
- Jednoduché zapojení.

Charakteristiky dnešních WLAN prošli několika generacemi vývoje, které můžeme shrnout následovně [1]:

- První generace, též známa jako IEEE 802.11 nebo WLAN/1G vznikla v roce 1997:
  - Propojení PC stanic mezi sebou nebo do LAN.
  - Přístupové body/mosty.
  - Roaming.
  - Možnost kooperace s jinými sítěmi, např. typu Ethernet LAN za pomoci přemostění.

- Druhá generace IEEE 802.11b v roce 1998 (WLAN/2G):
  - Efektivnější správa WLAN sítí.
  - Přizpůsobení se standardu 802.11b.

- Třetí generace IEEE 802.11a/g od roku 2000 (WLAN/3G):
  - Vysoká propustnost (high throughput HT).
  - Otevřený a integrovaný návrh sítí.
  - Minimalizace velkosti vysílacích a přijímacích antén.
  - Zlepšení citlivosti na straně příjemce.
  - Přizpůsobení se standardu IEEE 802.11a/g.

- Čtvrtá generace IEEE 802.11n (WLAN/4G):
  - Velmi vysoká propustnost (stovky Mbit/s).
  - Vysoká datová rychlost na velké vzdálenosti.
  - Použití technologie MIMO (multiple-in multiple-out) a STC (space time coding).

Jako každá technologie, tak i Wi-Fi se snaží zdokonalovat a vylepšovat své nedostatky, kterými jsou [1]:

- Nižší datové rychlosti v porovnání s kabelovými sítěmi.
- Omezení a vliv překážek, hlavně železo-betonové konstrukce (stěny, budovy).
- Sdílené pásmo s dalšími technologiemi.
- Riziko bezpečnostních útoků.
- Kvalita přenosu je závislá na prostředí.
- Nedostatek řízení kvality služeb QoS (Quality of Service).

1.3.1 Možnosti využití

Díky svým vlastnostem se bezdrátové sítě využívají v mnoha oblastech a na různé účely. Podle [1], jich můžeme rozdělit na tři typy:

- **Podnikové WLAN sítě** určené pro interní využití v rámci firmy. Poskytují profesionální řešení doplňkové sítě pro zaměstnance a hosty v „pohybu“. Vyžadují silné zabezpečení přístupu a nikým nerušené pásmo. Vybudováním této sítě se mnohé firemní podniky snaží o zvýšení své produktivity.
- **Domácí bezdrátové sítě** – pro běžné osobní použití v domácnostech s dosahem několik metrů. Jsou populární díky jednoduché implementaci, údržbě a hlavně ceně. Dalšími pozitivními vlastnostmi jsou možnost volného pohybu uvnitř domu, sdílená šířka pásma mezi více uživateli, přístup na Internet (vysokorychlostní ADSL) pomocí přístupového bodu a také správa domácích elektronických zařízení na dálku.
- **Hot spoty** – se rychle rozšiřují po celém světě a poskytují veřejné připojení pomocí přístupových bodů. Vyskytují se převážně na letištích, vlakových stanicích, v restauracích, kavárnách, nákupních centrech, hotelích, knihovnách, metrech, parcích a všude možně, kde to situace dovolují.

1.4 Architektura bezdrátových sítí

Podle standardu IEEE 802.11 se rozlišují dva typy komponentů [1]:

- Bezdrátová mobilní stanice (klient). Například PC nebo laptop, který má zabudovanou bezdrátovou síťovou kartu (NIC) nebo Wi-Fi adaptér dostupný v mnoha formátech (PCI, PCMCIA, USB, Wi-Fi čip).
- Přístupový bod (AP) jehož hlavní funkcí je přemostění (most) mezi pozemní sítí a stanicí. Většinou se skládá z radiové přijímací/vysílací antény, síťové karty (např. Ethernet 802.3) a softwaru zajišťujícím přemostění na druhé vrstvě.

Abychom tedy mohli vytvořit bezdrátovou síť, potřebujeme výše zmíněné zařízení. Přístupový bod (AP) hraje úlohu základní stanice (BS) Wi-Fi sítě, která může sdružovat

více mobilních stanic (PC, notebook, PDA, smartphone). Další podmínkou je kompatibilita standardů obou zařízení. AP může být vybaven skupinou standardů IEEE 802.11.

Rozlišujeme dva základní módy bezdrátového spojení založené na Wi-Fi standardech:

- Infrastrukturní mód
- Ad hoc mód

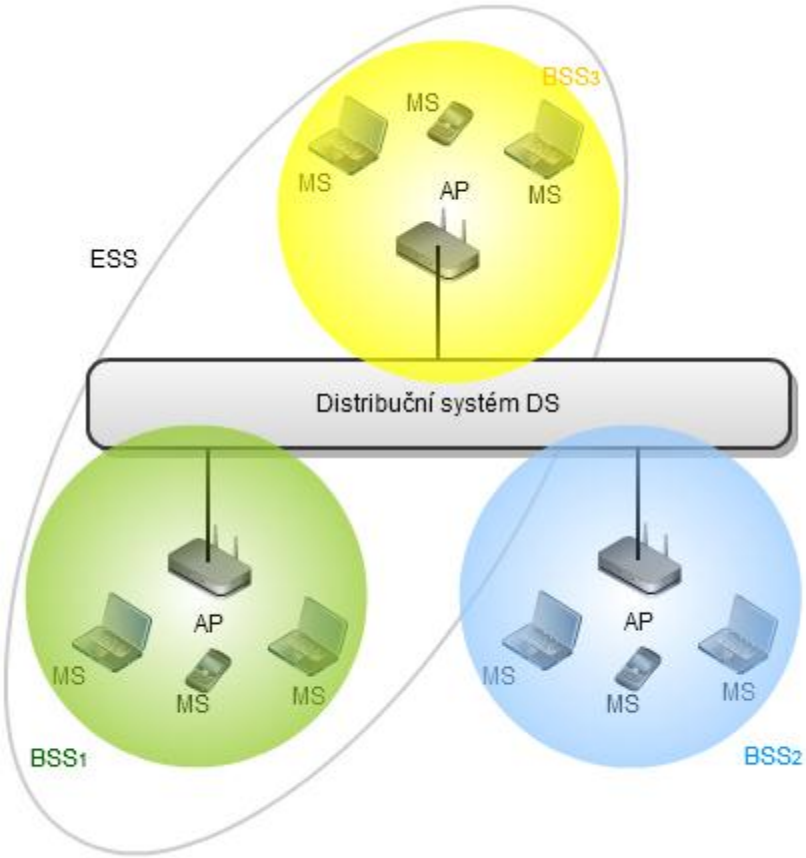
1.4.1 Infrastrukturní mód

V rámci infrastrukturního módu [1] musí být alespoň jeden AP (směrovač nebo přepínač) připojen fyzicky do distribučního systému (DS). K směrovači se může připojit několik mobilních stanic MS (klientů) a spolu tak tvoří jednu buňku nazývanou BSS (Basic Service Set). Takových buněk může být víc, které pak tvoří systém buněk zvaný ESS (Extended Service Set). Stanice jednotlivých buněk BSS spolu komunikují pomocí DS. Ten může být drátový (LAN) anebo bezdrátový (WLAN). Bezdrátový distribuční systém (WDS) je složen:

- z hlavního AP, obvykle připojeného do pevné LAN sítě.
- z výměnného (relay) AP, který distribuuje data mezi hlavním AP a vzdáleným AP nebo mezi klienty a další výměnnou stanicí.
- ze vzdáleného AP, který komunikuje přímo s klienty. Pro spojení mezi klienty se používají MAC adresy.

WLAN síť je tedy tvořena minimálně jedním AP, kde maximální vzdálenost klientů závisí na mnoha faktorech (např. vyzařovaný výkon antén, členění a překážky prostředí). Proto se do distribučního systému implementuje větší počet základních stanic. Klienti se pak mohou díky funkci roamingu volně pohybovat bez ztráty spojení. WLAN sítě poskytují přístup do služeb LAN (můžou to být tiskárny, servery nebo přístup k Internetu). Ukázku infrastrukturního módu a jeho základních prvků lze vidět na obr. č. 3.

V každé buňce je centrálním bodem AP, který udržuje a spravuje komunikaci mezi stanicemi v rámci pokrývané zóny (dosah AP). Abychom uměli rozlišit jednotlivé buňky mezi sebou, každá z nich je definovaná 48 bitovou adresou, tzv. BSSID (Basic Service Set Identifier), která odpovídá MAC adrese přístupového bodu. Abychom předešli nežádoucímu přístupu klienta do sítě, je obvykle na každém AP nastavován parametr SSID (Service Set Identifier). Je to jedinečný identifikátor každé WLAN sítě a může být sestaven z řetězce až 32 ASCII znaků. Jedná se v podstatě o klíč, pomocí kterého se mohou jednotliví klienti přihlašovat do Wi-Fi sítě. Tento parametr však není tajný zájemcům o přístup. Směrovač ho totiž vysílá v určitých časových intervalech v tzv. beacon rámcích. Klienti si pak mohou vybrat, do které sítě se připojí [1].

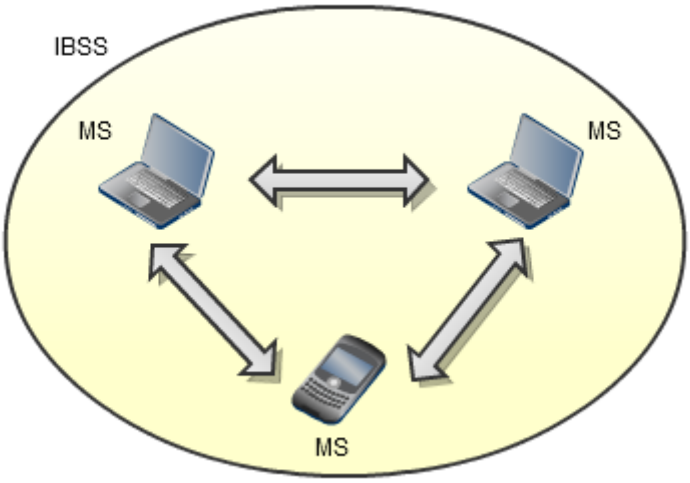


Obrázek 3. *Infrastrukturní mód standardu IEEE 802.11[1]* .

1.4.2 Ad hoc mód

Na rozdíl od infrastrukturního módu se v „ad hoc“ architektuře nevyskytuje přístupový bod AP, který by plnil funkci mostu. V zásadě se připojení do pevné sítě ani nevyžaduje. Jedná se spíš o tzv. peer-to-peer spojení mezi stanicemi. Tohoto spojení se využívá při potřebě přenosu nebo sdílení dat mezi minimálně dvěma uživateli. Vytvoření komunikace může inicializovat libovolná stanice s kýmkoliv v rádiovém dosahu. Propojené stanice spadají do nezávislé buňky zvané IBSS Independent Basic Service Set (viz obr. č. 4). Tak jako u infrastrukturního módu tak i tady je nutná SSID identifikace při přístupu do sítě. Ad hoc bezdrátové sítě mají kvůli své jednoduchosti široké uplatnění - zejména tam, kde není pevná infrastrukturní síť anebo kde není potřebná (hotelové pokoje, konferenční místnosti, restaurace, kavárny, letiště) a v neposlední řadě, kdy je přístup do pevné sítě zakázán nebo obtížně realizovatelný.

Za zmínku stojí, že existuje i síť v tzv. mesh módu a jedná se o hybridní konfiguraci kombinující infrastrukturní a ad hoc sítě.



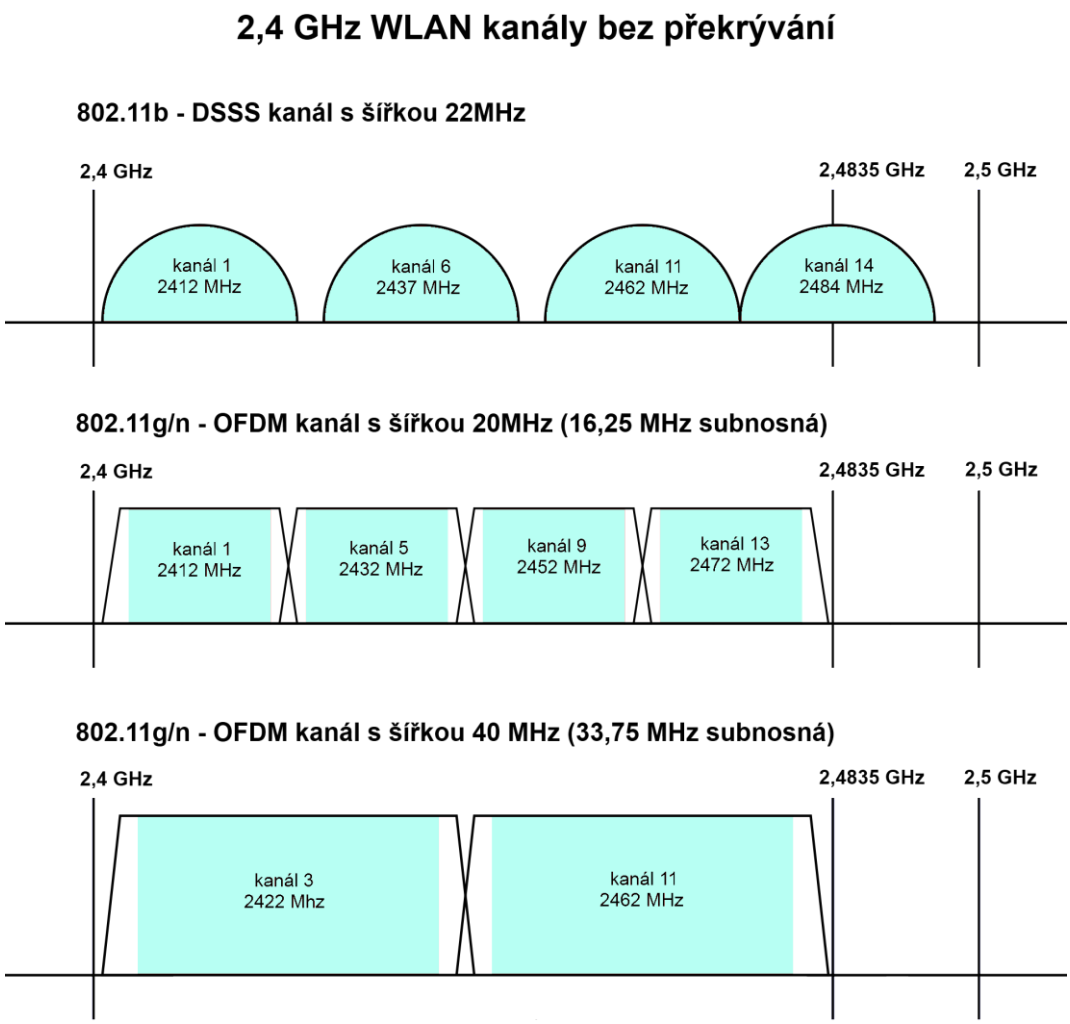
Obrázek 4. *Ad hoc mód standardu IEEE 802.11.*

1.5 Omezená pásma

Označení kmitočtových pásem 2,4 GHz a 5 GHz pro bezdrátový přenos je široký pojem a ve skutečnosti zahrnuje více užších pásem [4]:

- v rozsahu **kmitočtu 2,4 GHz** (standardy 802.11b/g/n) se vyskytuje 14 kanálů. První kanál má střed na kmitočtu 2,412 GHz a poslední na 2,484 GHz. Odstup od sousedních kanálů je 5 MHz, přičemž výjimku tvoří poslední 14. (přidělený Japonskem), který je vzdálený o 12 MHz. Každý kanál zabírá v šířce pásma kmitočet o velikosti 22 MHz. Pro standard 802.11b a techniku modulace DSSS se mohou vyskytovat jenom tři kanály – 1, 6 a 11. Co se týče standardů 802.11g/n, tam se v 2,4 GHz pásmu mohou vyskytovat čtyři kanály – 1, 5, 9 a 13. V tomto případě mají všechny kanály šířku 20 MHz a je použita modulace OFDM. K zvýšení rychlosti se pak použije stejná technika modulace a dva kanály o šířce 40 MHz, které se vzájemně nepřekrývají (standard 802.11n). Grafickou představu rozložení kanálů lze vidět na obr. č. 5.

- u rozsahu **kmitočtu 5 GHz** (standardy 802.11a/n) je situace odlišná. Ten je v Evropě definovaný 36. kanálem na kmitočtu 5,180 GHz až po 140. kanál na 5,700 GHz. V Evropě je dostupných 19 kanálů, ze kterých je prvních osm určeno pouze na použití uvnitř budov a jejich maximální vyzařovací výkon musí být nižší než 200 mW. Zbylých jedenáct kanálů už lze použít i mimo budovy (vyzařovací výkon do 1 W), vysílací zařízení musí ale být vybavena dynamickým výběrem frekvencí a regulací výstupního výkonu. Kanály jsou od sebe vzdáleny po 20 MHz krocích, takže má každé vysílací zařízení svůj vlastní a signál tak neinterferuje s okolními. Teoreticky lze provozovat až devatenáct 5 GHz Wi-Fi zařízení na jednom místě, aniž by se navzájem rušila, nebo devět vysokorychlostních kanálů využívajících šířku pásma 40 MHz.



Obrázek 5. *Rozložení nepřekrývajících se kanálů v pásmu 2,4 GHz [4].*

Pro srovnání se 5 GHz pásmo jeví jako výhodnější na sestavení bezdrátové WLAN sítě. Také v hustě zabydlených městech, kde je výskyt sítí na jednom místě značně velký, nehrozí, že se budou navzájem rušit. Pravda je ovšem taková, že zařízení podporující toto pásmo, jsou momentálně několikanásobně dražší a frekvenční spektrum není v některých krajinách dostupné v celé jeho šíři (pro většinu Evropy a USA to však neplatí).

1.6 Fyzická a linková vrstva IEEE 802.11

IEEE 802.11 standard klade důraz na dvě základní vrstvy ISO/OSI modelu. Jsou to fyzická a linková vrstva obsahující ještě podvrstvy MAC (Media Access Control) a LLC (Logical Link Control). Všechny typy WLAN sítí sdílejí stejný protokol přístupu k médiu právě přes MAC podvrstvu. Linková vrstva (a také MAC podvrstva) je dále zodpovědná za několik služeb [1]:

- autentizace (ověření).
- asociace (propojení zařízení – AP a MS), disasociace (odpojení) a reasociace (připojení na jiný AP při roamingu).
- podpora doručení MSDU (Mac Service Data Unit).
- CRC (Cycling Redundancy Check) – zajišťuje integritu dat.
- fragmentace paketů – rozdělení na menší dílčí časti při přenosu médiem.

Fyzická vrstva je zodpovědná za přenos dat (reprezentace 0 a 1) mezi zařízeními sítě. Dále na ni byly definované způsoby přenosu dat ve frekvenčních spektrech.

1.7 Rozprostřené spektrum

Radiová technologie zvaná modulace rozprostřeného spektra je hlavní technikou zpracování signálu ve Wi-Fi sítích (původně využívaná v armádě). Mezi její výhody patří vlastní zabezpečení přenosu, odolnost proti rušení z jiných rádiových zdrojů, zálohování (redundance) atd. Ve výsledku mohou systémy založené na modulační technice rozprostřeného spektra existovat v oblastech s vyšší hustotou dalších radiových systémů bez vzájemného rušení. Kromě výše zmíněných výhod mohou tyto systémy pracovat i v pásmech ISM [1].

1.7.1 Základní princip

Modulační techniky rozprostřeného spektra jsou definované jako techniky, v kterých [1]:

- je šířka pásma přenášeného signálu mnohem větší než šířka pásma originálního signálu.
- je šířka pásma přenášeného signálu dána přenosovým signálem a přídavným signálem známým jako kód šíření (Spreading Code)

Rozlišujeme dvě hlavní modulační techniky:

- FHSS – Frequency Hopping Spread Spectrum
- DSSS – Direct Sequence Spread Spectrum

1.7.2 Frequency Hopping Spread Spectrum

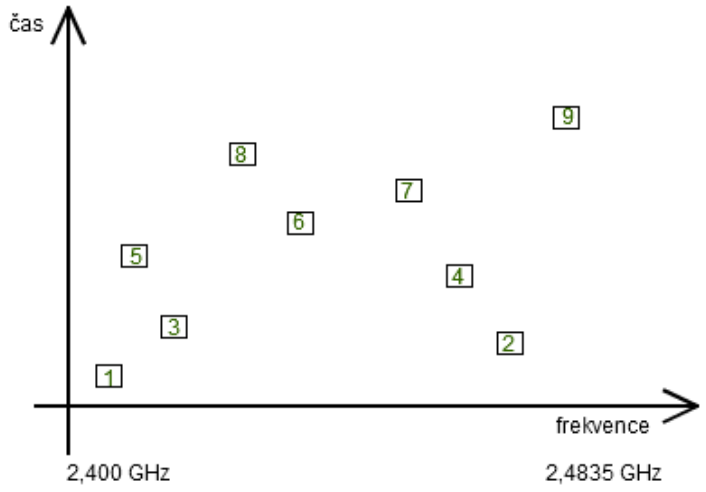
Metoda rozprostřeného spektra s přeskakováním frekvence přenáší radiový signál tím, že přepíná (skáče) nosnou složku signálu mezi více frekvenčních kanálů (viz obr. č. 6). Používá při tom pseudonáhodnou sekvenční posloupnost, která je známa vysílací i příjímací straně. Metoda nabízí propustnost 1 nebo 2 Mbps. Kanálů je 79 (USA) a 35 (Francie), kde každý zabírá 1 MHz v přenosovém pásmu od 2,4 GHz do 2,4835 GHz. Změna kanálu na jiný je vykonána přibližně každých 400 milisekund. Tato doba prodlevy na jinou frekvenci se nazývá skok a je dána určitými regulačními nastaveními. Je také nutná správná synchronizace frekvence [1].

Z popisu techniky vyplývá několik jejich výhod:

- zabraňuje celkové ztrátě signálu - je ztracen jenom kódovaný (modulovaný) signál na nosné frekvenci, který je však znovu vyslán na dalším skoku.
- poskytuje dobrou imunitu vůči interferencím a slabým šumům na pozadí.
- díky širokému frekvenčnímu spektru se v jedné geografické oblasti může vyskytovat mnohem víc WLAN sítí, které se navzájem nebudou rušit

Při přenosu signálu technikou FHSS jsou dosáhnuty dvě rychlosti přenosu. K tomu je použita GFSK (Gaussian frequency shift keying) modulace s různými úrovněmi:

- Frekvenční modulace GFSK se dvěma úrovněmi pro rychlost 1 Mbps
- Frekvenční modulace GFSK se čtyřmi úrovněmi pro rychlost 2 Mbps



Obrázek 6. *Pseudonáhodné přeskakování kanálů v FHSS modulovací technice [1].*

1.7.3 Direct Sequence Spread Spectrum

Modulační technika přímého rozprostřeného spektra (DSSS) využívá širší frekvenční pásmo pro jednotlivé kanály v porovnání s FHSS. Jak bylo řečeno v podkapitole 1.5, obsahuje 14 kanálu o šířce 22 MHz vzdálených od sebe po 5 MHz krocích. V původní verzi DSSS techniky se vyskytují dvě rychlosti a k jejich dosáhnutí jsou použité dvě modulace [1]:

- modulace DBPSK (Differential Binary Phase Shift Keying) pro rychlost přenosu 1 Mbps
- modulace DQPSK (Differential Quadrature Phase Shift Keying) pro rychlost přenosu 2 Mbps

Tyto dvě modulace jsou založené na principu rozdílné fázové modulace. Ve zkratce dochází k otáčení fáze každého nového přenášeného symbolu. Technika vyžaduje znalost referenčního poznatku o fázi pouze prvního vysílaného symbolu. Potom se přenosem symbolu otáčí fáze signálu v porovnání s předchozím symbolem a

dále už není nevyhnutné znát fázi referenčního symbolu. V binární frekvenční modulaci DBPSK je symbolem přenášen jenom jeden informační bit. K rotaci (inverzi) fáze je potřebný jenom bit „1“. U kvadratické DQPSK frekvenční modulaci symbol přenáší dva bity informace. Rychlost přenosu je tedy násobena dvakrát [1].

1.7.4 Orthogonal Frequency Division Multiplexing

Technika širokopásmové modulace OFDM (Ortogonální multiplex s kmitočtovým dělením) je součástí standardů 802.11a/g. OFDM tak jako předchozí techniky (FHSS, DSSS) využívá rozprostřeného spektra ke kmitočtovému dělení jednotlivých kanálu [1].

Jedná se o vysokorychlostní přenos dat na více nosných. Původní datový tok je rozdělen do více toků s nižšími rychlostmi a každý se moduluje na určitou nosnou pomoci více stavových modulací (QPSK,16-QAM nebo 64-QAM). Tím se potlačí vliv vícecestného šíření a může se dosáhnout vyšších přenosových rychlostí (teoreticky až 54 Mbps). Při této technice se před vysláním vytváří z modulovaných nosných pomocí FFT kompozitní signál, který se v přijímači pomocí IFFT rozloží zpět na dílčí úzkopásmové signály, které se demodulují a jednotlivé toky dat se pak skládají do původního vysokorychlostního datového toku [6][6].

2 BEZPEČNOST WLAN SÍTÍ

Ve světě informačních technologií hraje bezpečnost velkou roli. Každá síť, nehledě na to, jestli je to podniková, domácí nebo veřejná, musí být zajištěna vůči případným útokům nebo neautorizovaným přístupům. Vysoká míra popularity bezdrátových sítí umožnila vzniku nespočetného množství rizik, která mohou jejím uživatelům vzniknout. Radiový přenos dat je v bezdrátových sítích obzvlášť náchylný vůči zneužití. Dokonce i uživatelé, kteří se připojí do sítě legálním způsobem, mohou získat data z jiných počítačů. Poškozené můžou být i pevné LAN sítě, které sdílejí svůj prostor pohyblivým účastníkům přes přístupové body.

Zejména ve firemním a armádním sektoru se klade největší úsilí na ochranu citlivých údajů. Kromě ochrany přístupu se systémy chrání i proti různým typům virů, které mohou narušit správný chod a integritu sítě. Na bezpečnost se proto klade velký důraz a neustále se vyvíjejí nové způsoby a techniky ochrany. Tato kapitola se bude zabývat některými z nich.

2.1 Základní zabezpečovací způsoby přístupu

Přístupový bod (AP) jako hlavní rozhraní přístupu do pevné sítě poskytuje svému okolí mnohé identifikační údaje. Jedním z nich je už zmiňovaný beacon rámec vysílaný v určitých intervalech všem účastníkům, kteří jsou poblíž něho. Jak víme z kapitoly 1.4, rámec obsahuje identifikátor SSID daného přístupového bodu. Když se mobilní stanice – účastník, nachází v oblasti, kde operuje více AP, přijímá SSID informaci od každého z nich. Jakmile ji účastník detekuje, může se pokusit o připojení přes vybraný AP. Začíná Wi-Fi autentizační procedura, která vyžaduje znalost klíče generovaného přístupovým bodem.

Od vzniku standardu IEEE 802.11 se postupně vyvíjeli autentifikační techniky založené na šifrovacích klíčích. Probereme si jejich aktuální verze [1], [7]:

WEP – Wired Equivalent Privacy

WEP byl původní formou autentifikace v roku 1999 používanou ve Wi-Fi sítích. Cílem tohoto protokolu bylo udělat bezdrátovou síť stejně bezpečnou jako je pevná drátová. Po čase se ukázalo, že je lehko prolomitelná. Navzdory tomu se používá dodnes jako základní stupeň ochrany. WEP je implicitně nastavován komerčními výrobci přístupových bodů, čímž se běžní uživatelé, kteří jsou technicky neznalí, vystavují mnohým rizikům.

Princip spočívá v použití symetrické proudové šifry RC4, která šifruje odeslané rámce pomocí veřejného klíče, známého všem rádiovým stanicím. V cílové stanici se rámce pomocí tohoto klíče dešifrují. Na ověření integrity správy na přijímací straně se použije metoda CRC-32 kontrolního součtu. Existuje několik WEP protokolů, které se liší délkou šifrovacího klíče (40, 104 a 232 bitový). Ten s větší délkou je obtížnější na prolomení, ale jen co se týče času. Kterákoliv varianta klíče je však doplněna o 24 bitový inicializační vektor. Dohromady tak tvoří klíče o velikosti 64, 128 nebo 256 bitů.

Hlavním poznatkem pro úspěšné prolomení WEP se stala právě znalost inicializačního vektoru IV, kterým se v podstatě šifruje přenos. Při odchycení dostatečného množství rámců (profesionální programy: Aircrack, NetStumbler atd.) je možné tento vektor odhalit a tím získat původní zprávu.

WPA – Wi-Fi Protected Access

Důležitým dodatkem rodiny standardu IEEE 802.11 se stal právě standard 802.11i, který usiluje o vylepšování zabezpečovacích technik. Výsledkem jeho úsilí se stalo zabezpečení WPA (též známy jako WPA1 nebo WPAv1), které je firmwarovým vylepšením WEP. Ten se tak může jednoduše vyměnit pouhým nahráním do systému bezdrátových zařízení (bezdrátové směrovače, přepínače).

Hlavní změnou oproti WEP je implementace šifrovacího algoritmu TKIP (Temporal Key Integrity Protocol), který poskytuje bezpečnou utajenou výměnu šifrovacích klíčů mezi prvky sítě. V tomto případe, se každý paket šifruje jiným klíčem, který je tvořen základním klíčem (PTA – Pairwise Transient Key), MAC adresou příjímací stanice a pořadového čísla rámce. TKIP kromě jiného poskytuje základní podporu pro AES-CCMP algoritmus, který je preferovaný 802.11i standardem. Navzdory mnohým vylepšením se o WPA uvažovalo o jako dočasném řešení ochrany bezdrátové komunikace. S příchodem WPAv2 se měla situace změnit.

WPA2 - Wi-Fi Protected Access 2

Vznikl v roce 2004 a stal se současně nejlepším možným zabezpečením radiové komunikace. Zcela nahradil předešlé verze WPA, WPA1. Jeho nevýhodou je však výměna starého hardwaru za nový – obsahující WPA2 šifrovací protokol. To ovšem už nemusí být problémem většiny uživatelů, protože od roku 2006 musí být každé bezdrátové zařízení vyrobeno protokolem WPA2 (podmínky stanovené mezinárodní institucí Wi-Fi Alliance).

2.2 Další možnosti zabezpečení WLAN sítí

Stoprocentní zabezpečení neexistuje v žádných systémech. WLAN sítě nejsou také žádnou výjimkou. Ke kvalitnímu a vysokému zabezpečení se však můžeme přiblížit kombinací více technik a způsobů. Zde je přehled některých z nich [5]:

- Náhodná změna nebo modifikace sítových přístupových hesel.
- Využití nejvyšších kryptovacích algoritmů.
- Občasná změna SSID parametru sítě.
- Blokování vysílání beacon rámců – skryté SSID.
- Filtrování přístupu pomocí MAC adres.
- Vypnutí automatické detekce bezdrátového signálu – má za následek automatické připojení k sítí, o které uživatel nemusí vědět.
- Nastavení statických IP adres bezdrátovým stanicím. Většina sítí ovšem používá dynamické přidělení IP adres (DHCP), které je jednoduší na údržbu avšak méně bezpečné. Toto nastavení může být prakticky realizovatelné v menších, domácích sítích.
- Zapnutí firewallu na všech připojených stanicích také zvýší bezpečnost.

- Nastavení dosahu signálu přístupového bodu na omezenou vzdálenost. Obvykle na oblast využití – firemní budova nebo jiná strategická plocha. Tím se sníží možnost zachycení signálu vzduchem poblíž takového objektu.
- Přístup přes privátní virtuální síť (VPN).
- Krytí RF je praktické, jestli chceme zeslabit signál, který prochází stěnami nebo okny firemní budovy. Existují speciální barvy a fólie na to určené.
- Nasazení RADIUS (Uživatelská vytáčená služba pro vzdálenou autentizaci) serveru.
- Vypnutí bezdrátové sítě v čase její neaktivity (mimo pracovní dobu).

Je všeobecně známé, že WLAN sítě jsou méně bezpečné než drátové. Na zlepšení se neustále pracuje a v kombinaci s mnohými dostupnými technikami se zvyšuje ochrana. Je to však i o lidech a jejich disciplinovanosti na pracovišti. Proto se setkáváme i s firemní politikou, která vyžaduje od svých zaměstnanců dodržovat jistá bezpečnostní pravidla.

3 KVALITA SLUŽEB VE WLAN SÍTÍCH

Kvalita služeb označovaná i jako QoS (Quality of Service) je souhrnem všech možných prostředků, které poskytují určitý stupeň spolehlivosti sítě. Spolehlivost neboli kvalita se definuje jako výkon toků jednotlivých paketů na komunikační cestě ze zdroje do cíle.

V současné době, kdy se vyskytuje velké množství aplikací citlivých na spolehlivost, je kvalita služby velice důležitá. Na činnost aplikací všeho druhu jsou kladeny různé nároky na spolehlivost. Můžeme klidně hovořit o tzv. priorizaci aplikací v sítích. To znamená, že ne každá aplikace bude mít stejnou prioritu v přenosovém kanále. Aby to dávalo smysl, jsou aplikace jako video nebo audio přenos upřednostňované před prohlížením webových stránek nebo e-mailů. Videokonference nebo VoIP (Voice over IP) jsou totiž více časově závislé (přenos v reálném čase) na doručení paketů do cílové stanice. Kromě toho se kvalita služby dá posuzovat i jinými parametry, které se dotýkají právě výkonnosti přenosu paketů v síti [1].

Hovoříme o těchto základních parametrech QoS:

- ztrátovost paketů (loss of packets)
- zpoždění paketů (delay, latence)
- kolísaní zpoždění (jitter)
- šířka pásma (bandwidth)

V následující tabulce č. 1 je vyjádřena přibližná citlivost některých aplikací na výše zmíněné parametry kvality služeb:

Tab. 1 Citlivost síťových aplikací na parametrech kvality služby QoS [1].

Aplikace	Citlivost na parametr kvality služby QoS			
	ztrátovost	zpoždění	kolísání zpoždění	šířka pásma
Prohlížení web stránek	velká	střední	malá	střední
Prohlížení e-mailů	velká	malá	malá	malá
Přenos souborů	velká	malá	malá	velká
Přenos video signálu	střední	velká	velká	velká
Přenos audio signálu	střední	velká	velká	malá

3.1 IEEE 802.11e

Zajištění kvality služeb je hlavní úlohou doplňku standardu IEEE 802.11e, který vylepšuje podvrstvu MAC linkové vrstvy. Ta disponuje dvěma funkcemi sdílení média [1]:

- HCCA (HCF Controlled Channel Access) – Přístupová metoda ke kanálům řízená HCF.
- EDCA (Enhanced DCF Channel Access) - Vylepšená DCF přístupová metoda ke kanálům.

Obě funkce vycházejí z původních metod sdílení media, kdy se o přístup k němu uchází více sítových zařízení:

- DCF (Distributed Coordination Function) je založena na metodě mnohonásobného přístupu s naslouchánim nosné se zamezením kolize (CSMA/CA).
- PCF (Point Coordination Function) je vyžívaná v komunikaci mezi přístupovým bodem a více účastníky sítového provozu. Identifikační beacon rámce jsou PCF funkci děleni na dva časové úseky, kde v prvním se použije klasicky DCF a v druhém AP oznamuje uživateli, kdy může vysílat v přenosovém médiu.

4 ZABEZPEČENÍ WLAN SÍTÍ

4.1 Cíl

Cílem laboratorní úlohy je získaní znalostí o bezpečnosti současných WLAN sítí a o metodách prolomení zabezpečení WEP, WPA/WPA2. Teoretický úvod má za úkol objasnit problematiku šifrované komunikace v bezdrátových sítích (2,4 GHz). V praktické části se student obeznámí s nástrojem BackTrack 5 Linux pomocí něhož lze dosáhnout dešifrování bezdrátové komunikace v infrastrukturním módu (AP + klient) a tím získaní přístupových údajů. Úloha má studentům objasnit hlavní rysy a nedostatky známých zabezpečovacích ochran WLAN sítí. Postupy jak tyto nedostatky překlenout ve svůj prospěch mají mít pouze naučný charakter a student by se tak k nim měl i stavět.

4.2 Požadavky na pracoviště

Bezdrátový směrovač D-Link DIR-855, bezdrátový adaptér AirLive X.USB-3, 1xPC, mobilní terminál.

4.3 Zadání

- Sestavte WLAN síť v infrastrukturním módu (AP + MT).
- Nakonfigurujte zabezpečení WLAN sítě (64 a 128bit WEP, 64 a 128bit WPA2).
- Seznamte se s BackTrack 5 Linux nástrojem pro penetrační testy.
- Analyzujte bezdrátové lokální sítě v blízkém dosahu pomocí BT5.
- Aplikujte proceduru na prolomení přístupových údajů vybrané testovací sítě nejdříve pro WEP a pak proceduru se slovníkovým útokem na WPA/WPA2.

4.4 Teoretický úvod

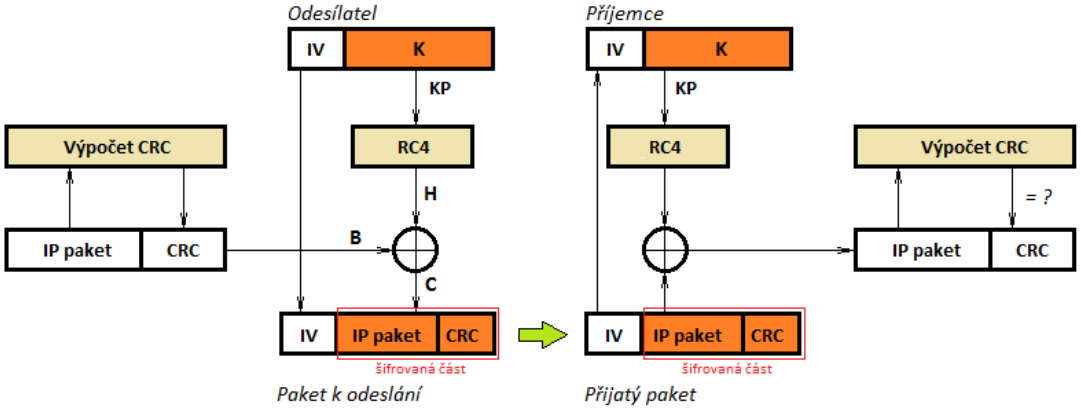
Zabezpečení bezdrátových sítí podle standardu IEEE 802.11 (WLAN) je v mnoha ohledech velice sensitivní problematikou, která se snaží všemi možnými prostředky ochránit informace (aktiva) před nelegálním zneužitím, modifikací nebo trvalé ztrátě. Víme však, že žádný systém ochrany není stoprocentní a ke stavu maximální bezpečnosti se můžeme jenom přiblížit. O bezpečnou ochranu dat se starají komunikační protokoly, které jsou založeny na poznatcích z kryptografie. Přístup k aktivům je podmíněn na základě vyřešení nějakého matematického problému (dále jen kryptografický problém), který je prakticky neřešitelný (např. výpočet diskrétního logaritmu). Oprávnění uživatelé mají před útočníky jednu výhodu a tou je znalost tajné informace – dešifrovací klíč. Pomocí něho lze snadno kryptografický problém vyřešit. Informační systémy s rádiovou komunikací jsou obecně vystaveny největším hrozbám.

Wired Equivalent Privacy (WEP) protokol

WEP patří do skupiny symetrických kryptosystémů a k šifrování komunikace používá proudovou šifru RC4. Tyto systémy se vyznačují vysokou rychlosti a zaručují dobrou důvěryhodnost a autentičnost přenášených informací. Na druhé straně jsou oproti blokovým šifrám méně bezpečné.

Princip šifrování WEP 64-bit [8]:

V protokolu WEP je každý paket šifrován proudovou šifrou RC4 na základě 64 bitového klíče $KP = IV \,||\, K$. Náhodný inicializační vektor IV o délce 24 bitů se generuje pro každý paket a tajný parametr K o délce 40 bitů je klíčem daného přístupového bodu. Tento klíč se musí do AP i MS vkládat ručně.



Obrázek 7. *Schéma protokolu WEP[8]*

Pro přenášený *IP paket P* se nejprve vypočítá kontrolní součet $CRC = CRC(P)$ o délce 32 bitů. V této souvislosti je zapotřebí upozornit, že CRC kontrola integrity dat („Cyclic Redundancy Check“) je vhodná pouze k detekci nahodilých přenosových chyb. Pro svou linearitu je zcela nevhodná pro detekci záměrných modifikací dat. Útočník totiž pro daný CRC součet dokáže jednoduše zjistit, jak data upravit, aby příjemce modifikaci dat nezjistil. U kryptografických autentizačních kódů (haš – MAC nebo HMAC) to možné prakticky není. Vypočítaný CRC součet se připojí na konec IP paketu, čímž vznikne blok $B = P \,||\, CRC$. Poté odesílatel vygeneruje náhodný inicializační vektor IV, ke kterému připojí klíč K a tak vytvoří klíč pro šifrování daného paketu $KP = IV \,||\, K$. Pomocí tohoto klíče algoritmem RC4 vygeneruje heslo $H = RC4(KP)$ potřebné délky a k němu přičte modulo 2 jednotlivé bity bloku B. Před takto zašifrovaný blok bitů $C = B \oplus H$ ještě předřadí použitý inicializační vektor IV a výsledek zašle příjemci. Ten k IV připojí klíč K a s jeho pomocí vygeneruje stejné heslo jako odesílatel. Jeho přičtením k zašifrovaným datům získá původní IP paket a kontrolní součet. Z dešifrovaného IP paketu vypočítá nový CRC součet a porovná jej s přijatým součtem. Pokud jsou stejné, paket předá nadřízené (tj. síťové) vrstvě. V opačném případě jej vymaže. Tento postup lze vidět na obr. č. 7.

Hlavním nedostatkem zabezpečení WLAN sítí je klíčové hospodářství. Klíče přístupových bodů a terminálů K se mění ručně (tzn. prakticky vůbec) a tak jedinou

proměnnou hodnotou u každého paketu je *IV*. Jeho délka je však pouze 24 bitů a tak pro daný AP existuje pouze 2^{24} = 16777216 různých heslových postupností. Útočník může provoz daného přístupového bodu monitorovat, ukládat zachycené pakety a třídit je podle inicializačního vektoru *IV*.

Nyní si ukážeme jednotlivé hrozby popsaného zabezpečení. První hrozbou je možnost tzv. **analýzy provozu**. V tomto případě útočník pouze monitoruje rámce přenášené v linkové vrstvě. K tomu jednoduše využije vlastní terminál vybavený speciálním softwarem a případně použije ke zvýšení dosahu svého monitorování směrovou anténu (dosah až stovky metrů). Monitorováním sítě může zjistit časový průběh aktivity v síti a intenzitu provozu. Tak může určit charakter použití a význam sítě.

Druhou hrozbou je poměrně jednoduchá **modifikace paketů**. Jak již bylo řečeno autentizace paketu se provádí zašifrovaným *CRC* součtem. Slabinou funkce CRC je skutečnost, že pro IP pakety P_1 a P_2 platí:

$$\mathrm{CRC}(P_1 \oplus P_2) = \mathrm{CRC}(P_1) \oplus \mathrm{CRC}(P_2) \tag{4.1}$$

Analýzou provozu nebo jinými cestami může útočník odhadnout IP adresu určitého zařízení v síti (např. poštovního serveru) a identifikovat pakety jemu určené. Z odhadnuté IP adresy serveru *S* potom může zjistit část hesla pro šifrování adres $H_A = C_A \oplus S$, kde C_A je ta část kryptogramu, kde je zašifrována IP adresa příjemce. Kryptogram *C* útočník zmodifikuje na kryptogram *C′*, kde v části adresy příjemce bude jeho vlastní adresa *U*:

$$C'_A = H_A \oplus U = C_A \oplus (S \oplus U) \tag{4.2}$$

a v části kontrolního součtu bude:

$$CRC' = \mathrm{CRC} \oplus CRC(\mathrm{S} \oplus \mathrm{U}) \tag{4.3}$$

Takto modifikovaný paket odešle, a pokud byl jeho odhad adresy správný, tak zařízení AP kryptogram *C′* dešifruje na IP paket *P′*, který mu bude prostřednictvím Internetu doručen. Pokud jeho odhad správný nebyl, tak pokus opakuje. Z přijatého paketu *P′* útočník může odvodit celou heslovou postupnost *H* pro daný inicializační vektor:

$$H = C' \oplus P' \tag{4.4}$$

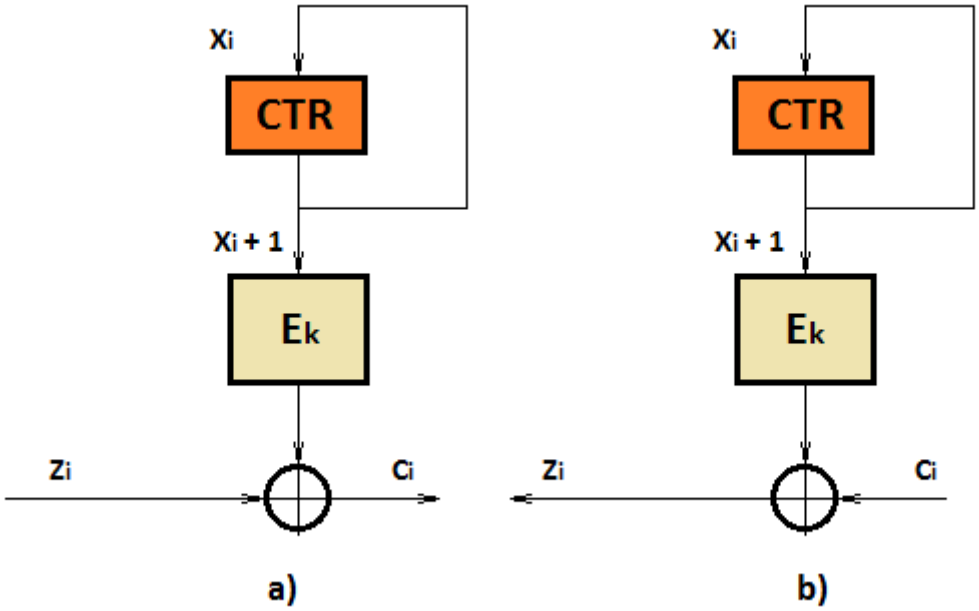
Popsaný postup může útočník opakovat pro jiné hodnoty *IV* nebo jej kombinovat se statistickou kryptoanalýzou, takže nakonec má po určité době k dispozici databázi všech přiřazení $IV \rightarrow H$. Tímto je naplněna třetí hrozba - zabezpečení WLAN je zcela prolomeno, neboť útočník může dešifrovat všechny informace, může využívat informační zdroje napadeného a může do informačního systému zasílat klamné informace.

Tím se zabezpečení WLAN pomocí protokolu WEP považuje za zcela nevhodné, protože potencionálnímu útočníkovi stačí vynaložit minimální úsilí k prolomení komunikace za pomoci dostupných komerčních zařízení. Tento nedostatek se však rychle podařilo odstranit protokolem WPA (Wi-Fi Protected Access). Momentálně je

nejbezpečnějším protokolem WPA2, který byl vydán v rámci standardu IEEE 802.11i.

Wi-Fi Protected Access 2 (WPA2) protokol [8]:

Jádrem zabezpečení podle standardu 802.11i je nový šifrovací mód CCM („Counter mode encryption with CBC-MAC“) a centrální oboustranná autentizace zařízení v síti. Šifrovací mód CCM je blokově orientovaný režim, který zajišťuje šifrování i autentičnost přenášených rámců. K šifrování se používá moderní americký standard AES („Advanced Encryption Standard“) s délkou bloku 128 bitů a volitelnou délkou klíče 128, 192 nebo 256 bitů. Provozní režim CCM prakticky sestává ze dvou módů – mód CBC je určen k výpočtu autentizačního kódu celého rámce MIC („Message Integrity Code“) a mód CTR zajišťuje šifrování paketu přenášeného v daném rámci. Provozní mód CTR („Counter mode“) je ilustrován na obr. č. 8.

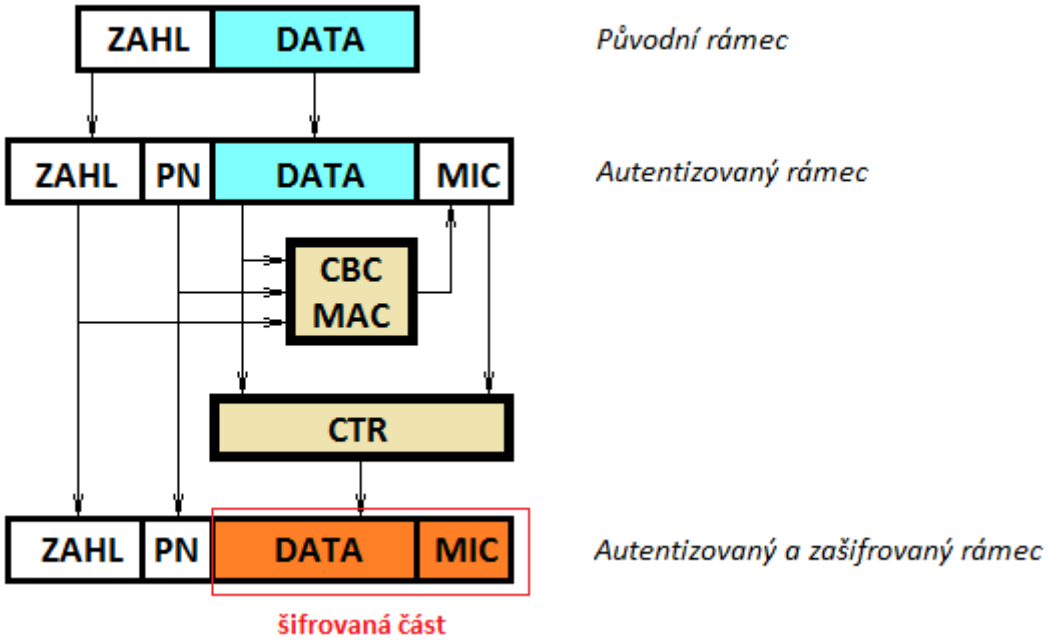


Obrázek 8. *Schéma režimu CTR, a) šifrování, b) dešifrování [8].*

Režim CTR je prakticky proudová šifra, kde je blokový šifrátor použit jako generátor hesla. Na počátku komunikace má vysílající i přijímající strana stejnou počáteční hodnotu *CTR = X1*. Jejím zašifrováním se získá první blok hesla, který se sečte *modulo 2* s prvním blokem zprávy, respektive kryptogramu. Číslo CTR je poté zvětšeno o 1, znovu zašifrováno a získá se tak druhý blok hesla. Opakováním popsaného postupu se vygeneruje tolik bloků hesla, kolik je bloků zprávy, respektive kryptogramu.

Na obr. č. 9 je zobrazen princip protokolu CCM. Na straně odesílatele se do původního rámce vloží mezi záhlaví (ZAHL) a data (DATA) pořadové číslo rámce *PN*. Poté je na základě tohoto čísla a dalších služebních údajů ze záhlaví vygenerován inicializační vektor *IV*. S jeho pomocí je zašifrován řetězec *ZAHL || PN || DATA* v klasickém režimu *CBC*. Polovina bitů z posledního zašifrovaného bloku (tj. 64 bitů) tvoří autentizační kód celého rámce *MIC*. Dalším krokem je odvození počáteční

hodnoty čítače *CTR* na základě znalosti čísla rámce *PN* a dalších služebných údajů. V režimu *CTR* je pak zašifrován blok *DATA* || *MIC*. Před takto zašifrovaný blok se připojí záhlaví *ZAHL* a pořadové číslo rámce *PN* čímž vznikne zašifrovaný a autentizovaný rámec, který je následně odeslán příjemci. Příjemce zpracovává rámec inverzně. Odvodí hodnotu *CRT* a následně dešifruje zašifrovanou část rámce, čímž získá blok *DATA* || *MIC*. V režimu *CBC-MAC* vypočítá vlastní hodnotu *MIC* a porovná ji s dešifrovanou hodnotou. V případě shody jsou *DATA* předány vyšší vrstvě. V opačném případě jsou *DATA* smazána.



Obrázek 9. *Schéma CCM protokolu [8].*

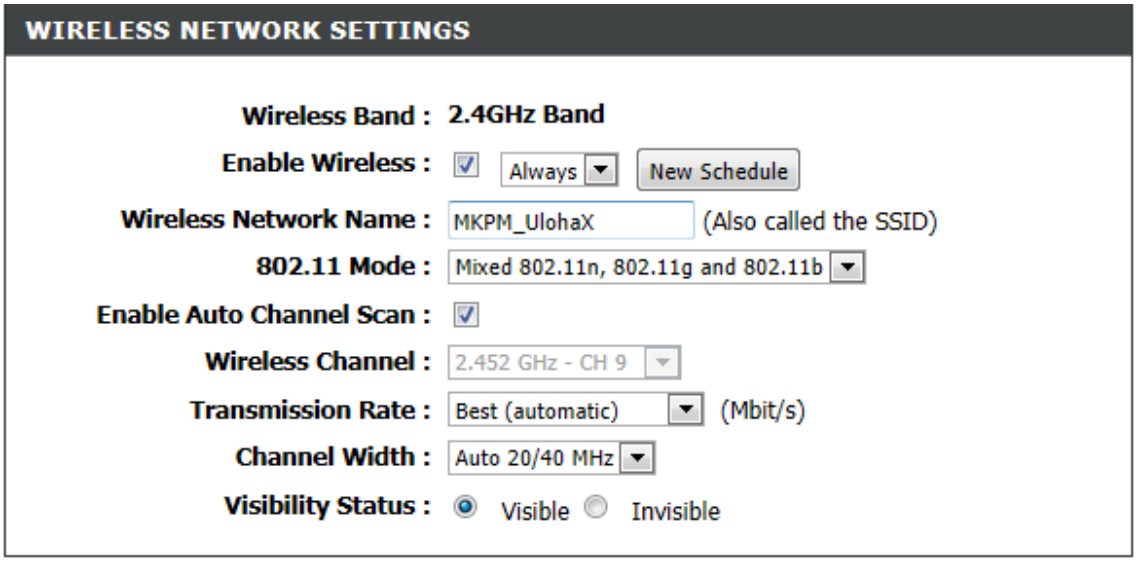
4.5 Pracovní postup

Úkol 1 – Nastavení WLAN sítě s AP

Spusťte počítač a přihlaste se jako Student do OS Windows 7. Wi-Fi směrovač D-Link DIR-855 připojte do vnitřní sítě Ethernetovým kabelem. Zjistěte IP adresu, která byla směrovači přidělena v záložce: *Device Info>Internet* (192.168.x.x). Přes webový prohlížeč (IE) se připojte na tuto adresu zadáním: http://192.168.x.x:8080. Přihlašovací údaje do webového rozhraní směrovače:

Login: *Admin*, Password: nechte prázdný.

Nastavení WLAN sítě proveďte následovně (viz obr. č. 10): *Setup>Wireless Settings>Manual Wireless Network Setup.*



Obrázek 10. *Nastavení WLAN sítě ve webovém rozhraní D-Link DIR-855 směrovače.*

SSID sítě si zvolte sami, nejlépe jednoduchý a ne moc dlouhý název (např. MKPM_ulohaX). Zabezpečení sítě nastavte pro každý úkol následovně.

Základní zabezpečení WLAN sítě:

1) WEP – 64 bit. klíč, autentizace Both (kombinace otevřené autentizace a sdíleného klíče Shared key)
2) WEP – 128 bit. klíč, autentizace Both
3) WPA2-PSK – zvolte Security Mode: *WPA Personal*, WPA mode: *WPA2 Only*, Cipher Type: *AES*, Group Key: *3600*

Úkol 2 – Nastavení monitorovacího módu v prostředí BackTrack 5 R1

Účelem těchto kroků je nastavení bezdrátového adaptéru do tzv. monitorovacího módu, kdy je schopný naslouchat pakety v okolních WLAN sítích. V monitorovacím módu pak můžeme do sítě pakety i vstřikovat za účelem, který si objasníme v následujícím postupu.

Na stolním PC připojte bezdrátový adaptér Airlive X.USB v zapojení se dvěma anténami. Na ploše otevřete virtuální systém VMware a spusťte z disku linuxový nástroj BackTrack 5 R1 (BT5R1-GNOME-VM-32). Po načítání systému BT5 zadejte přihlašovací údaje – login: *root*, password: *toor*. Grafické rozhraní BT5 spustíte příkazem `startx`. Otevřete si zatím jednu terminálovou konzolu a postupujte podle následujících pokynů (vždy jako *root*).

Příkazem `iwconfig` ověřte, jestli je bezdrátové zařízení aktívní. Aktívní zařízení by mělo být `wlan0`, které je momentálně ve stavu *managed*. Nejdříve rozhraní zastavte: `airmon-ng stop wlan0` a pak ho znova aktivujte: `airmon-ng start wlan0`. Příkazem iwconfig znova ověřte stav rozhraní. V tomto případě byl vytvořen alternatívní název pro wlan0. V monitorovacím módu by se mělo objevit rozhraní `mon0`. Komunikace bude od tohoto kroku monitorována jenom tímto rozhraním [9]:

```
root@bt:~# iwconfig mon0
mon0      IEEE 802.11abgn  Mode:Monitor  Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

Úkol 3 – Prolomení WEP (64 a 128 bit.)

WEP - 64 bitový klíč:

Nejprve musíme vytvořit testovací síť se zabezpečením podle bodu 1) - (Úkol 1 – Základní zabezpečení WLAN sítě). Heslo do sítě si zvolte sami (pozn. heslo si můžete navzájem zatajit a jeden z vás se ho pak bude snažit prolomit). Konfiguraci sítě uložte a mobilní stanicí se připojte do nově vytvořené sítě.

Přepnete se zpět do prostředí BT5. Teď je potřeba prohledat okolní WLAN sítě a najít tu správnou, kterou jsme si za účelem prolomení klíče vytvořili. *Pozn.: Mějte na paměti, že kdybyste chtěli přistupovat tímto způsobem do jiné cizí sítě, potřebujete svolení jeho správce nebo vlastníka!*

a) Prohledávaní okolních sítí

V konzoli zadejte příkaz:

`airodump-ng mon0` – vypíše se seznam všech dostupných sítí a jejich specifických parametrů

Tento seznam je neustále aktualizován novými sítěmi v dosahu, proto si všimněte řádku s vaší testovací sítí a přerušte monitorování (CTRL+C). S vypsaných parametrů nás zatím zaujímá BSSID (MAC adresa AP), CH (kanál), ESSID (název) naší testované sítě [9].

b) Odchytávaní inicializačních vektorů

Dalším krokem je zachytit generované inicializační vektory IV z našeho testovaného AP do souboru a to pomocí příkazu [9]:

`airodump-ng -c (kanál) -w (název souboru) --bssid (MAC adresa AP) (rozhraní)`, kde

- ***c*** je číslo monitorovaného kanálu.
- ***w*** název souboru (např. *wep64*), do kterého se budou ukládat IV.
- ***bssid*** je MAC adresa AP.
- rozhraní zvolte ***mon0***.

c) Autentizace a asociace k AP

Aby mohl AP akceptovat příchozí pakety, musí být zdrojová MAC adresa bezdrátového adaptéru asociována. Jestli zdrojová MAC adresa není asociována, nemůže AP vstřikované pakety přijmout a posílá de-autentizační paket v otevřeném textu. V tomto případě nejsou žádné nové IV vytvořené, protože AP ignoruje vstřikované pakety. Za předpokladu, že bezdrátová síť je nakonfigurována bez filtrace MAC adres, můžeme vykonat klamnou autentizaci (proveďte v novém terminálovém okně) [9]:

`aireplay-ng -1 0 -e (essid) -a (bssid) (rozhraní)`, kde

- ***1*** indikuje klamnou autentizaci.
- ***0*** je časování reasociace v sekundách.
- ***e*** je název WLAN sítě.
- ***a*** je MAC adresa AP, na který se autentizujeme.

Při správnosti předchozích kroků obdržíte následovný výpis do konzole:

```
16:23:05  Sending Authentication Request
16:23:05  Authentication successful
16:23:05  Sending Association Request
16:23:05  Association successful :-)
```

Někdy se může stát, že vás AP odpojí a vy dostanete hlášku: `Got a deauthentication packet!` Proto se občas podívejte, jestli jste pořád asociovaný a pokud ne tak zopakujte předchozí příkaz.

d) Odposlech ARP protokolů

Cílem dalšího příkazu je zapnout mód, v kterém budeme poslouchat žádosti ARP protokolu a následně je vstřikovat zpět do sítě. Vyplývá to hlavně z charakteru této služby, při které AP normálně tyto žádosti pošle na všesměrovou adresu, a spolu s ní se generují nové IV. Našim úkolem je nasbírat co největší počet IV v co nejkratším čase. Otevřeme si třetí terminálové okno a zadáme tento příkaz [9]:

`aireplay-ng -3 -b (bssid) (rozhraní),` kde

- ***3*** značí vstřikování ARP paketů do sítě.
- ***b*** je MAC adresa AP.

Nástroj *aireplay-ng* balíčku BT5 začne naslouchat ARP dotazy a když uslyší alespoň jeden, začne je okamžitě vstřikovat zpět. To se zobrazí v okně, ve kterém jsme zadali pokyn pro naslouchání ARP paketů. Může to vypadat takto:

```
Saving ARP requests in replay_arp-0321-191525.cap
You should also start airodump-ng to capture replies.
Read 629399 packets (got 316283 ARP requests), sent 210955
packets...
```

Může se ovšem stát, že nejsou přijaty žádné ARP pakety (`got 0 ARP requests`), tehdy je třeba si pomoci tím, že v prohlížeči na MS se připojíme na nějakou webovou stránku (např. www.google.com).
Pokud se přepnete do prvního okna, kde probíhá aktualizace sítě, vidíte rapidní zvýšení rychlosti přenosu datových paketů v sloupci #Data (sloupec *#/s* určuje datový tok za vteřinu). Pro zachycení dostatečného množství IV počkejte, až číslo přesáhne 15000 paketů a pak kombinací kláves CTRL+C pro přerušení. To by mělo stačit na prolomení 64 bitového klíče WEP protokolu.

e) Získaní WEP klíče

Posledním krokem k získání klíče WEP protokolu je analýza inicializačních vektorů, které jsme si zachytili a filtrovali jen pro náš testovaný AP. Implicitně je použita metoda PTW (podle tvůrců Pyshkin, Tews, Weinmann), která je v porovnání

s metodou FMS/KoreK mnohem rychlejší a efektivnější. Nejprve pro metodu PTW zadáme příkaz [9]:

`aircrack-ng -b (bssid) wep64-01.cap`, kde

- aircrack-ng je nástroj pro dešifrování WEP klíče.
- ***b*** je MAC adresa našeho AP.
- ***wep64-01.cap*** je soubor, který se uložil do našeho domovského adresáře *root*.

Pokud náhodou nebude 15000 zachycených paketů stačit na prolomení klíče, nástroj *aircrack* vás o tom informuje a nabídne vám další pokus při počtu 20000. Tehdy zopakujte krok s odposlechem ARP protokolu a spusťte *aircrack-ng* znova. Tímto způsobem pokračujte, až se vám nepodaří prolomit WEP klíč a nezobrazí se vám podobný výsledek:

```
KEY FOUND! [ 12:34:56:78:90 ]
Probability: 100%
```

Našli jste heslo do vámi vytvořené sítě (WEP, 64 bitový klíč).

f) Metoda FMS/KoreK

Pro porovnání si vyzkoušejte i metodu FMS/KoreK. Ta pro změnu potřebuje přibližně 250000 zachycených IV. Následující příkaz můžete spustit i během generování paketů [9]:

`aircrack-ng -K -b (bssid) wep64-01.cap`, kde

- ***K*** značí použití FMS/KoreK metody.

WEP - 128 bitový klíč:

Podobně postupujete i při hledání 128 bitového WEP klíče (zabezpečení sítě podle bodu 2)). V tomto případě je však zapotřebí nasbírat větší počet IV (přibližně 40000 až 85000 paketů), čímž se zvýší čas potřební na prolomení klíče.

Úkol 4 – Prolomení WPA/WPA2 Pre-Shared Key

V zabezpečení pomocí WPA existuje několik rozdílů oproti WEP protokolu. Ten používá 40 nebo 104 bitový šifrovací klíč, který se musí manuálně vložit do AP a klienta a dále se už nemění. WPA používá stejnou proudovou šifru RC4 ovšem s jiným způsobem šifrování paketů. TKIP (Temporal Key Integrity Protocol) je protokol, který pro každý paket dynamicky generuje nový 128 bitový klíč, čímž chrání před útoky použitelnými v zabezpečení s WEP. Standard IEEE 802.11i (WPA2) využívá zdokonalenou techniku šifrování AES (výše popsanou). Před-sdílený klíč (Pre-Shared Key) byl navržen pro sítě v malých firmách a domácnostech, které nedisponují autentizačním serverem. Uživatel před vstupem do sítě musí zadat heslo (8 až 63 znaků ASCII nebo 64 hexadecimálních číslic). Hešovací funkce pak toto heslo upraví na délku 256 bitů.

Hlavním rozdílem při lámaní WPA/WPA2 oproti WEP je v použité technice útoku. Zatímco u WEP jsme schopni využít statistických metod, u WPA/WPA2 můžeme

použít jenom techniky hrubé síly (brute force). Protože klíč už není statický, nemůžeme využít inicializační vektory IV ke zrychlení procesu prolomení hesla, jak tomu bylo u WEP. Jedinou alternativou k inicializaci útoku je zachycení „handshake“ komunikace mezi klientem a přístupovým bodem. Handshake je ukončen, když je klient připojen do sítě. Jedním z problémů jak prolomit WPA/WPA2 je v délce použitého klíče. Při použití klíče sestaveného z 8 – 63 znaků (číslice, speciální znaky) je toto zabezpečení prakticky neprolomitelné. Pro účely tohoto úkolu je možné použít **slovníkový útok**, který je v porovnání s útokem hrubou silou časově nenáročný. Heslo se musí vyskytovat v použitém slovníku, jinak je metoda neúčinná. Autentizační metody jsou pro WPA i WPA2 v podstatě stejné a také technika k prolomení je identická [9].

K demonstraci této techniky můžeme tedy využít rovnou bezdrátovou síť s WPA2 zabezpečením (viz základní zabezpečení WLAN sítě, bod 3)). Před tím než nastavíme heslo sítě, je zapotřebí nějaké si vybrat z lokálního slovníku uloženého v adresáři `/root/password.lst`. Vyberte si heslo nejlépe z konce seznamu. Připojte MS do sítě a pokračujte následujícím postupem:

Shrnutí kroků potřebných k prolomení WPA2:

a) Spuštění monitorovacího módu na vybraném kanálu.
b) Spuštění zachytávání autentizačního handshake s filtrováním pro MAC adresu našeho AP.
c) Použití de-autentizační správy pro bezdrátového klienta.
d) Spuštění procesu pro prolomení PSK klíče.

a) Spuštění monitorovacího módu na vybraném kanálu.

Postup pro nastavení monitorovacího módu je stejný jako ***v úkolu č. 2***. V monitorovacím módu jsme pak schopni naslouchat i komunikaci, která nám nenáleží a zachytit tak čtyř-cestnou handshake komunikaci. Později budeme schopni také de-autentizace klienta ze sítě. V případě, že je rozhraní *mon0* aktivní, můžete tento krok vynechat a pokračovat dále [9].

b) Spuštění zachytávaní autentizačního handshake s filtrováním pro MAC adresu našeho AP.

Nejdříve si v prvním terminálovém okně příkazem `airodump-ng mon0` prohledáme okolní sítě a zjistíme, na jakém kanále pracuje naše síť (MKPM_ulohaX). Ve sloupci CIPHER a AUTH je vidět použití AES (nebo CCMP) šifrování a PSK klíče. Použijeme příkaz [9]:

`airodump-ng -c (kanál) --bssid (MAC adresa AP) -w (název souboru) (rozhraní),` kde

- ***c*** je číslo monitorovaného kanálu.
- ***bssid*** je MAC adresa AP.
- ***w*** název souboru (např. *psk*), do kterého se bude ukládat zachycení handshake mezi AP a klientem.
- rozhraní ***mon0***.

V tomto momente, zachytáváme komunikaci mezi klientem a AP, avšak nemůžeme zachytit handshake, protože spojení jsme navázali ještě před tímto krokem. Tuto situaci můžeme řešit dvěma způsoby. Zaprvé máme možnost odpojit a znovu připojit klienta do sítě. Druhá možnost je přinutit klienta k re-asociaci s AP a tím k inicializaci handshake mezi nimi. Ukážeme si tu druhou možnost.

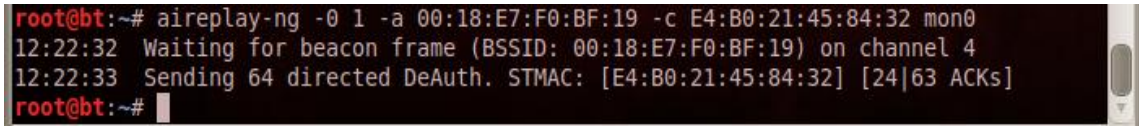
c) Použití de-autentizační zprávy pro bezdrátového klienta.

Do druhého terminálového okna zadáme následující příkaz [9]:

`aireplay-ng -0 1 -a (bssid) -c (MAC klienta)(rozhraní),` kde

- ***0*** znamená de-autentizaci.
- ***1*** značí počet de-autentizačních správ (je možné jich poslat i více).
- ***a*** je MAC adresa AP.
- ***c*** je MAC adresa klienta, kterého de-autentizujeme.
- rozhraní ***mon0***.

Dostanete výstup podobný jako je na obr. č. 11:



Obrázek 11. *Oznámení o de-autentizaci klienta od AP.*

Pro potvrzení zachycení handshake se podívejte do prvního t. okna a v pravém horním rohu se zobrazí informace `[ WPA2 handshake (MAC adresa AP) ]`.

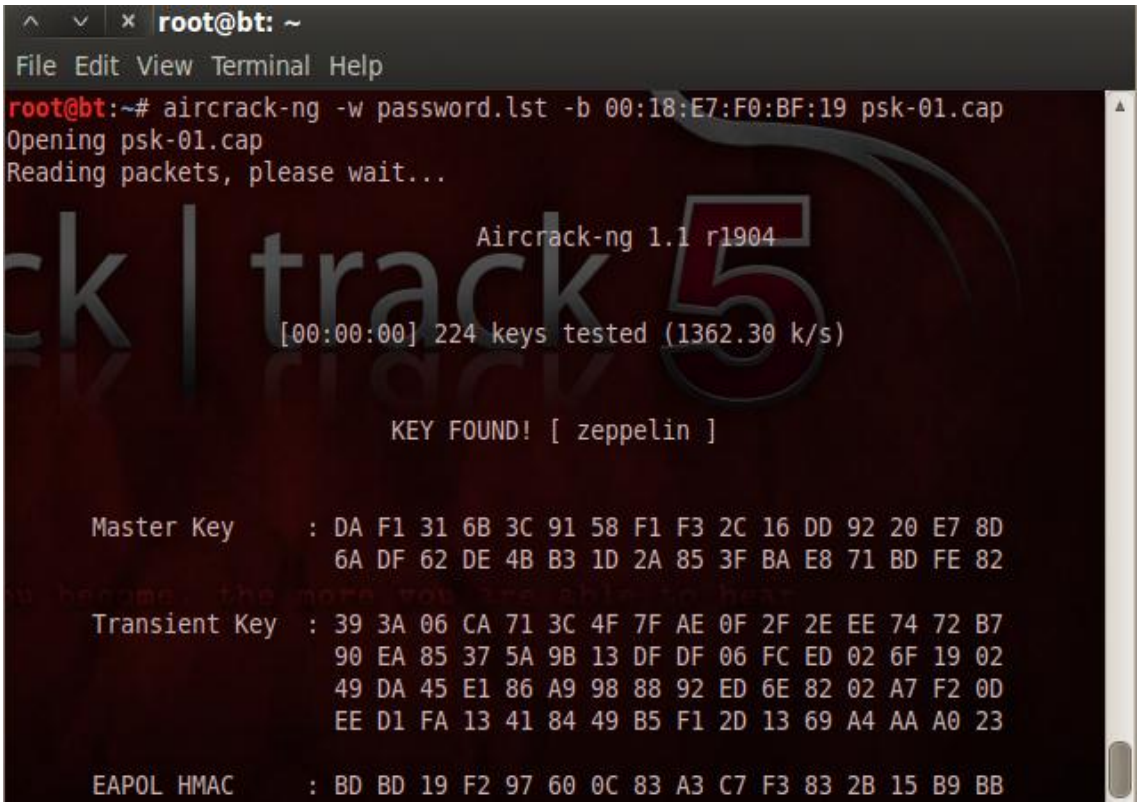
d) Spuštění procesu pro prolomení PSK klíče.

Cílem posledního kroku je prolomit získaný před-sdílený klíč ze souboru, který jsme si uložili do adresáře /root pod názvem např. *psk*. V třetím okně zadáme příkaz [9]:

`aircrack-ng -w password.lst -b (bssid) psk-01.cap,` kde

- ***w*** password.lst je název slovníku, z kterého BT5 testuje každé slovo a srovnává ho se zachycením PSK klíčem.
- ***psk-01.cap*** s označením -01 značí první soubor, ve kterém jsou zachyceny pakety z handshake komunikace. Těchto zachycení může být více, a proto se toto číslo inkrementuje. K prohledání vícero souborů použijeme hvězdičku (*psk*.cap*).

V tomto bodě se prohledává slovník a zjišťuje se PSK klíč (viz obr. č. 12). Záleží na velikosti slovníku a rychlosti CPU, jak dlouho bude trvat nalezení klíče. V našem případě je to téměř hned, protože slovník není moc rozsáhlý, i když jste vybrali heslo z jeho konce.



Obrázek 12. *Prolomení PSK klíče.*

Úklid pracoviště

Vymažte všechny soubory z hlavního adresáře *root* týkající se uložení komunikace v úlohách č. 3 a č. 4 (využijte k tomu správce souboru Midnight Commander, příkazem *mc*). Příkazem *halt* se odhlašte z BT5. Odpojte směrovač D-Link DIR-855 ze sítě a bezdrátový modul AirLive X.USB-3 z USB.

5 MOŽNOSTI VIDEO STREAMU BEZDRÁTOVÉ IP KAMERY

5.1 Cíl

Cílem této laboratorní úlohy je prozkoumat možnosti video streamu v konvergovaných bezdrátových sítích. K tomuto účelu bude vytvořena lokální bezdrátová WLAN síť, připojena ke školní vnitřní síti s bránou do vnější sítě internetu. Vlastnosti systému bezdrátové kamery umožnují stream pomocí komprese videa v některých známých formátech (H.264, MPEG4, MJPEG, 3GPP). Úlohou je najít kompromis mezi kvalitou a plynulostí zobrazovaného streamu použitím různých nastavení kodeků a ostatních parametrů videa. Poslední úloha je zaměřena na nastavení zasílání notifikačních obrázků na FTP server, k čemuž slouží funkce automatické detekce pohybu nebo zvuku ve snímaných zónách.

5.2 Požadavky na pracoviště

Bezdrátová IP kamera AirCam WL-350HD, bezdrátový směrovač D-Link DIR-855, bezdrátový adaptér AirLive X.USB-3, 1xPC, mobilní terminál.

5.3 Zadání

- Konfigurace WLAN sítě a jejich prvků.
- Konfigurace bezdrátové IP kamery.
- Bezdrátový příjem video streamu mobilními účastníky.
- Nastavení komprese video streamu a dalších parametrů závislých na jeho kvalitě.
- Konfigurace FTP serveru a automatického zasílání snímků na základě detekce pohybu nebo zvuku ve snímané oblasti.

5.4 Teoretický úvod

Poskytování telekomunikačních služeb v GSM (Global Systém for Mobile communication) síti je dnes už samozřejmostí a s nástupem nových technologií se zvyšují i nároky jejich uživatelů. Kromě základných a doplňkových služeb (hovor, fax, SMS, hlasová schránka, identifikace volajícího CLIP atd.) poskytuje GSM síť i řadu datových služeb (prohlížeč Internetu WAP, stahování různých typů dat – hudba, video,

obrázky atd.). Služby tohoto i jiného podobného typu mají na starosti technologie HSCSD (High Speed Circuit Switched Data), GPRS (General Packet Radio System), EGPRS/EDGE (Enhanced GPRS/Enhanced Data Rates for GSM), které se stali součásti 2,5 fáze vývoje GSM služeb. Nás budou zajímat poslední dvě jmenované. Nejprve však něco stručně o GSM síti, její struktuře a vlastnostech jednotlivých prvků [10].

Struktura GSM sítě

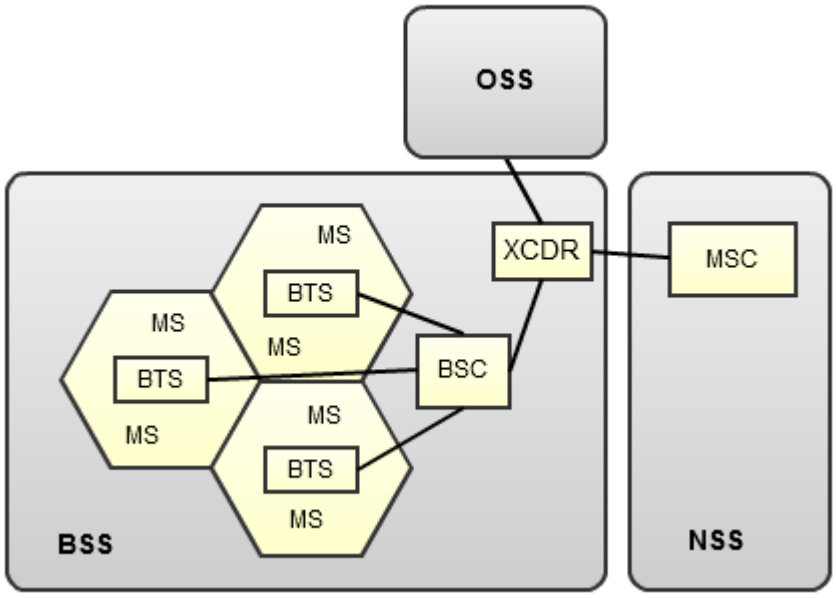
Základní části mobilní sítě GSM (viz obr. č. 13) tvoří podle [10]:

- **MS (Mobile Station) –** mobilní stanice pozůstávající z mobilního terminálu ME (Mobile Equipment) a identifikační kartou SIM (Subscriber Identity Module) účastníka.

- **BSS (Base Station Subsystem) –** bázový subsystém skládající se ze soustavy bázových transceiverů vysílačů/přijímačů BTS (Base Transceiver Station), kontrolérů bázových stanic BSC (Base Station Controller) a transkodérů XCDR.

- **OSS (Operation and Support System)** – systém monitorování a řízení činnosti sítě GSM a správy účtů uživatelů.

- **NSS (Network Switching Subsystem)** – síťový subsystém tvořený z mobilních ústředen MSC (Mobile Switching Centre), bran do různých jiných systémů GMSC (Gateway MSC) a taky je tvořen několika registry obsahující informace o uživatelích a jejich mobilních terminálech.



Obrázek 13. *Základní architektura GSM sítě [10]*.

Frekvenční pásma a počet kanálů v GSM [10]:

- **GSM 900 (Primary GSM)** – Uplink 890 – 915 MHz, Downlink 935 – 960 MHz

a 124 kanálů.

- **Extended GSM (EGSM)** – Uplink 880 – 915 MHz, Downlink 925 – 960 MHz a 174 kanálů.
- **GSM 1800** – Uplink 1710 – 1785 MHz, Downlink 1805 – 1880 MHz a 374 kanálů.
- **GSM/PCS 1900** – Uplink 1850 – 1910 MHz, Downlink 1930 – 1990 MHz a 299 kanálů.

Kapacita jednotlivých systémů GSM je dána počtem rádiových kanálů. Každý kanál je rozdělen na 8 časových slotů, tzv. timeslotů (jeden TDMA rámec), přičemž 1 timeslot tvoří 156,25 bitů. Dalších 26 nebo 56 rámců tvoří multirámec. Superrámec je pak tvořen z 51 nebo 26 multirámců. A největším sdružovaným fyzickým kanálem je hyperrámec tvořen z 2048 rámců [10].

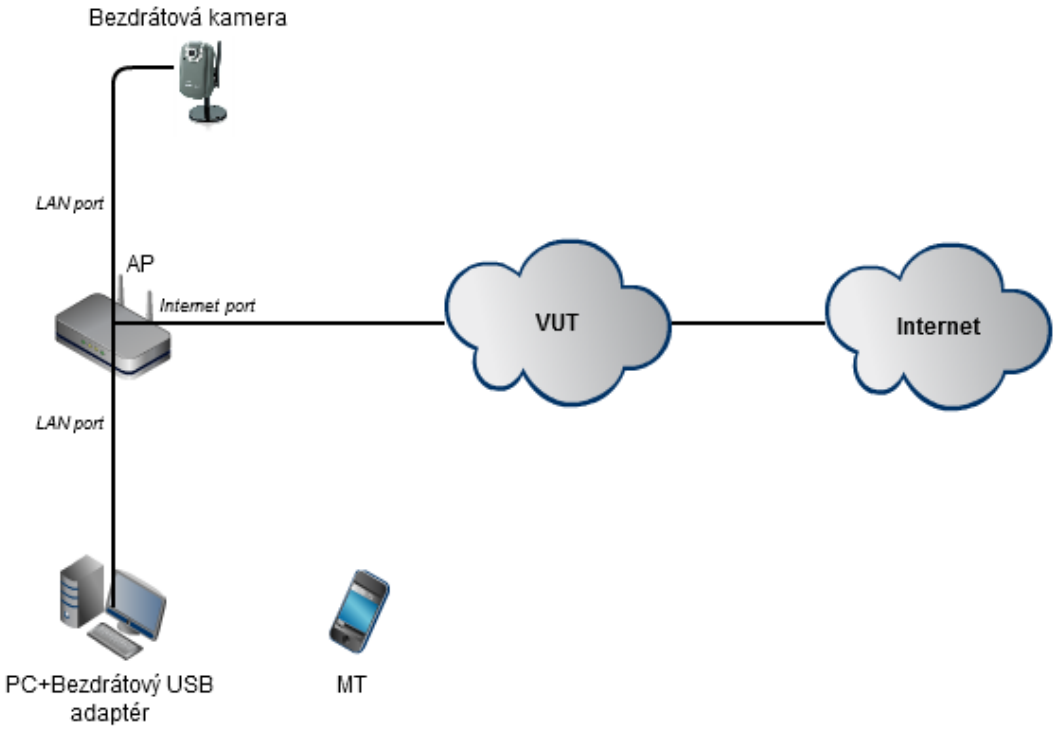
Kanály jsou pak rozděleny do dvou kategorií [10]:

1. **Provozní**
    - *s plnou rychlostí (full rate)* – přenosová rychlost na fyzické vrstvě je 22,8 kb/s (užitečná přenosová rychlost pro hlas je 13 kb/s a pro data je 9,6 kb/s).
    - *s poloviční rychlostí (half rate)* – přenosová rychlost na fyzické vrstvě je 11,4 kb/s (užitečná přenosová rychlost pro data je 4,8 kb/s).
2. **Signalizační**
    - *všesměrové (Broadcast Channels BCH)* – ve směru od BTS k MS, které se ještě dělí na řídicí, kmitočtově opravný a synchronizační kanály
    - *společné řídicí* – zajišťující řízení přístupu MS ke GSM síti a dělící se na vyvolávací, přidělovací kanál a kanál s náhodným přístupem.
    - *vyhrazené řídicí* – určené pro signalizaci s konkrétní MS.

5.5 Pracovní postup

Úkol 1 – Základní konfigurace WLAN sítě a bezdrátové IP kamery

Pro účely video streamu z bezdrátové IP kamery si nejprve vytvořte vlastní WLAN síť. Zapojte Wi-Fi směrovač, PC a kameru podle obr. č. 14.

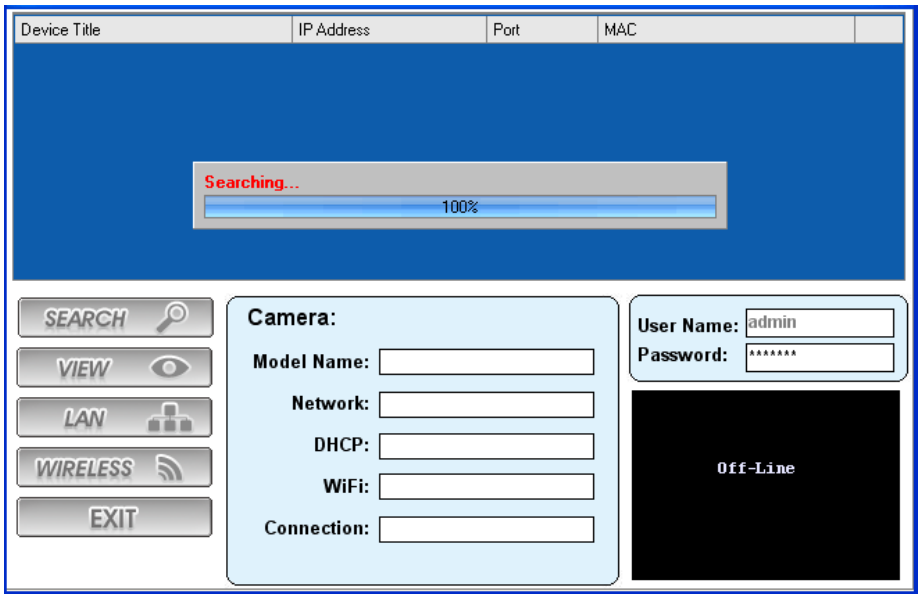


Obrázek 14. *Topologie WLAN sítě s bezdrátovou kamerou [11].*

Nastavení Wi-Fi směrovače a IP kamery:

1. Přes webové rozhraní (IP adresa směrovače) nastavte SSID sítě, heslo a zabezpečení (libovolné, není podmínkou v této úloze). Nastavte přidělovaní dynamických adres (DHCP). Vše uložte a potvrďte.
2. Spusťte software *AirLive IP Wizard II* pro nastavení kamery a kliknete na ikonku *Search* (viz obr. č. 15), kdy se připojená kamera zobrazí se svým jménem IP adresou, portem a MAC adresou. Občas se může stát, že kamera přes tento software nekomunikuje správně. Tehdy je potřebné zadat přidělenou IP adresu do prohlížeče. IP adresu zjistíte ve webovém rozhraní směrovače nebo v příkazovém řádku *cmd*. Dvakrát kliknete na zobrazený řádek. Otevře se přihlašovací okno [11]:

   Jméno: ***admin***, Heslo: ***airlive*** (defaultní nastavení, ***neměňte***!)



Obrázek 15. *Hledání připojené kamery.*

3. Zobrazí se úvodní okno s video streamem. V levé horné části jsou tři možnosti volby. Zatím vás bude zajímat menu *Setting*. To je rozděleno na *BASIC* a *Advanced*. V sub-menu *BASIC>System>Date/Time* nastavte lokální časové pásmo a potvrďte tlačítkem *OK* (od této chvíle všechny změny aplikujte tímto tlačítkem).
4. Pro nastavení bezdrátového vysílání rozklikněte *BASIC>Network>Wireless*. Zaškrtněte volbu *On*. Ze seznamu WLAN sítí vyberte tu svou. Vyznačená MAC adresa je fyzickou adresou bezdrátového rozhraní kamery. Do pole *Passphrase* a *Re-type* zadejte heslo WLAN sítě. Zvolte dynamické přidělování adresy z DHCP serveru. Nastavení potvrďte a vyčkejte, než se seznam WLAN sítí znovu obnoví a uvidíte přidělenou IP adresu.

Úkol 2 – Bezdrátové vysílání ve WLAN síti

Po nastavení základní konfigurace a bezdrátového módu vysílání, můžete Ethernetový kabel z kamery odpojit. V tomto momentě probíhá auto-konfigurace bezdrátového rozhraní se směrovačem (žádost o připojení do WLAN, autentifikace, asociace, přidělení IP adresy DHCP serverem). V následujících krocích budete přijímat multicast různými způsoby. V menu *Advanced>System Log* můžete sledovat průběžné změny vysílání (přes jaký port a protokol je vysíláno, jakým formátem, a které adresy jsou příjemci a další užitečné informace).

1. Připojte se na nově přidělenou IP adresu kamery v okně prohlížeče. Zatím nenastavujte nic.

2. Mobilním terminálem (MT) se připojte k běžící WLAN síti. Mezi Android aplikacemi spusťte *MX Player* přehrávač. Z menu vyberte položku *Stream v síti* a zadejte URL adresu v tomhle formátu [11]: *rtsp://<IP>:<Port>/video.3gp*. <IP> je veřejná IP adresa kamery a <Port> je její defaultní RTSP port s hodnotou 554 (ten lze změnit, ale není to v našem případě potřebné). Video se

vysílá v konvertovaném formátu 3GP (3GPP formát souboru) určeném pro 3G telefony a zařízení. Uživatel s datovým tarifem je tak schopen se připojit na stream odkudkoliv, kde je v dosahu signálu UMTS sítě. Také telefony se starší 2,5G technologií (GPRS, EDGE) jsou schopny tento multicast zachytávat. V libovolném internetovém prohlížeči v telefonu zadejte následující adresu *http://<IP>/mobile.wml*. V tomto případě získáváte aktuální snímky na vyžádání kliknutím na odkaz *Refresh*.

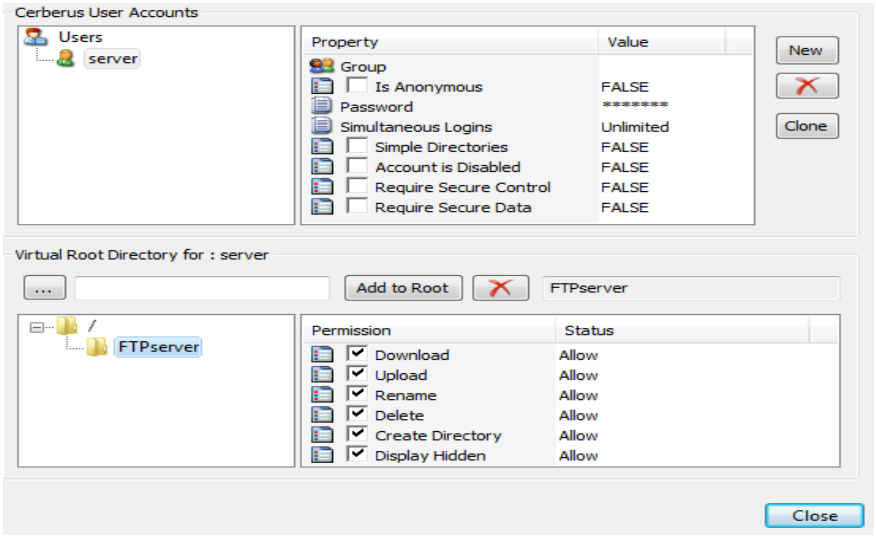
3. Dalším účastníkem multicastového příjmu může být PC s bezdrátovou USB kartou nebo notebook. V tomto případě využijte bezdrátový USB modul a připojte se k WLAN síti. V PC tento stream otevřete např. ve VLC přehrávači. V menu *Medium>Otevřít stream v síti* zadejte stejnou URL adresu jak v bodě předešlém (zadejte přístupové údaje kamery).

4. V tomto momentě můžete sledovat video z kamery na třech místech – webové rozhraní kamery (úvodní menu – Live View), VLC přehrávač a MX Player v mobilu. Můžete si však všimnout menšího zpoždění mezi VLC přehrávači a webovým rozhraním. Mnohem větší zpoždění je viditelné na mobilu (>10s). To je ovšem jenom dočasný problém. Po nějakém čase (max. 10 minut) se video ustáli a jsou vidět minimální rozdíly. Kvalita streamu se dá ovlivnit změnou komprese videa pomocí čtyřech formátů (H.264,MPEG4,MJPEG a 3GPP) a jejich nastavení (rozlišení snímku, počet snímku ze vteřinu, kvalita snímku). V menu *BASIC>Camera>H.264, MPEG4, MJPEG, 3GPP* prozkoumejte možnosti vysílaného formátu videa a zjistěte, který soubor nastavení je nejoptimálnější z hlediska kvality videa a zpoždění ve WLAN síti. Mějte na paměti, že stream vysílán do mobilního telefonu a do VLC přehrávače je defaultně komprimován ve formátu 3GPP. Změny ostatních formátů lze vidět jenom ve webovém rozhraní kamery. Vaše výsledky diskutujte s vyučujícím.

Úkol 3 – bezpečnostní vlastnosti bezdrátové kamery AirLive WL-350HD

Jednou z hlavních vlastností této kamery je možnost detekce pohybu nebo zvuku ve snímané oblasti. Na základě této rozlišovací schopnosti je možné poslat snímky nebo krátké video na lokální/vzdálený FTP, SMTP server a interní/externí úložiště. Vyzkoušíme si to na praktickém příkladů pomocí lokálního FTP serveru.

1. Nejdříve si nakonfigurujte jednoduchý FTP server. Z plochy spusťte program *Cerberus FTP Server*. Z menu *Configuration* kliknete na User manager. Vytvořte nového uživatele (např. server) a zvolte jeho virtuální kořenový adresář (Virtual Root Directory – např. *d://studenti/FTPserver*). Kliknete na tlačítko *Add to Root*. Nastavte heslo pravým kliknutím na položku *Password* a pak *Properties* - zvolte libovolné heslo. Zaškrtnete všechna povolení pro uživatele (viz obr. č. 15) a uložte kliknutím na tlačítko *Close*.



Obrázek 16. *Nastavení FTP serveru.*

FTP server defaultně naslouchá na všech rozhraních připojených k WLAN síti na portu 21.

2. Přepněte se do webového rozhraní kamery a v menu *Advanced>FTP client>General* zaškrtněte kolonku *On*. Jednotlivé položky vyplňte následovně:

FTP server name - *<IP adresa PC>/<Název adresáře>* , např. *192.168.x.x/FTPserver*.
User name, Password – vaše vlastní.

K ověření funkčnosti FTP serveru slouží tlačítko *Test*, při kterém se přenese testovací soubor z kamery na FTP server. Výstup z něho by měl vypadat jako na obr. č. 16, až na jinou adresu a cestu k FTP adresáři.

```
Send file to
ftp://server:xxxxx@192.168.1.3:21/FTPserver/tes
le
Connecting to 192.168.1.3:21... ! connected
Logging in as server ... Logged in!
File transmit :

    success
Transfered 7 bytes in 1 file
.............FTP Test Success.............
```

Obrázek 17. *Úspěšné spojení mezi FTP serverem a bezdrátovou kamerou.*

Funkčnost je sice ověřena, avšak k tomu, abychom jste mohli aplikovat posílání snímků na základě detekce pohybu nebo zvuku, musíte ponechat v poli *FTP server name*, jenom IP adresu serveru. Pod tímto nastavením vše uložte.

3. Přepněte se do sub-menu *Alarm sending* a zaškrtněte kolonku *On*. Zvolte vzdálenou cestu FTP serveru (*Remote path*) – cesta k vašemu kořenovému

adresáři (např. FTPserver). Název snímku je také libovolný (bude se inkrementovat jenom pořadové číslo snímku, podle toho, co zvolíte – *Date Time, Sequence number*). Při položce *Alarm* zaškrtněte kolonku *Motion detection* a klikněte na tlačítko *Motion detection*. Zde si můžete pohrát s nastavením tří detekčních oken ve snímané oblasti. Nastavit lze práh a citlivost jednotlivých oblastí (viz obr. č. 17). Po uložení vašeho nastavení je kamera v aktívním režimu a každý pohyb, který překročí práh citlivosti ve snímané oblasti, zašle jeden snímek na FTP server. Ověřte si to v *System Log*, a také se připojte na FTP server např. pomocí programu *Total Commander* (CTRL+N), kde najdete tyto snímky. Můžete si vyzkoušet i zaslání krátkého videa (*FTP client>General>Video clip*). Vyzkoušejte si také detekci na základě nějakého zvuku v blízkosti kamery.

Obrázek 18. *Nastavení zón detekujících pohyb.*

Úklid pracoviště

Po ukončení všech vašich úloh vraťte konfiguraci bezdrátové IP kamery do továrního nastavení (Setting>BASIC>System>Initialize>Factory default). NEVYPÍNEJTE kameru, pokud nebude restartována. Vymažte konfiguraci FTP serveru, a také jeho složky na disku. Rozpojte WLAN síť a všechna jeho zařízení.

6 ZÁVĚR

Účelem diplomové práce bylo získat jisté teoretické základy v problematice řešení bezdrátových WLAN sítí. Práce klade důraz převážně na technologii sítí 802.11 vytvořených mezinárodní standardizační organizací IEEE. Poskytuje přehled některých jejich standardů. Dále se zabývá dvěma hlavními způsoby zapojení WLAN sítí – a to v infrastrukturním a ad hoc módu. Právě v infrastrukturním módu hraje důležitou roli přístupový bod, který tvoří rozhraní mezi pozemní drátovou infrastrukturou. Pracovní pásma WLAN sítí se mohou dělit na několik kmitočtů. Jsou probírána hlavně dvě frekvenční pásma – 2,4 GHz a 5 GHz, přičemž první z nich je stále masově rozšířenější i navzdory nízkému počtu neinterferujících kanálů v rozmezí 2,412 – 2,484 GHz. Pásmo 5 GHz je mnohem širší, zde může v jedné oblasti pracovat více bezdrátových zařízení. Ty však nejsou momentálně komerčními výrobci podporovány pro svou vysokou cenu. V budoucnu se s nimi ovšem počítá, hlavně v hustě zabydlených aglomeracích. Princip rozprostřeného spektra je základem pro efektivní využití přenosového pásma.

S rapidním nástupem IEEE 802.11 technologie se zvyšovalo riziko prolomení bezpečnosti sítí. Jelikož se jedná o radiový přenos informací vzduchem, zachycení komunikace je mnohem jednodušší než u pevných drátových sítí. Proto se využívá několik technik šifrování přenosu a kombinuje se s dalšími způsoby ochrany. V současné době jsou veřejností vyžadovány multimediální služby, které jsou citlivé na kvalitativní parametry. Jedním z nich je i hodnota zpoždění, která má dopad na spolehlivost celkem rozšířené videokonferenční služby.

Na základě získaných teoretických znalostí byly vytvořeny dvě laboratorní úlohy, které jsou součástí práce. V první z nich bylo prolomeno šifrované zabezpečení dvou známých protokolů WLAN sítí. Při protokolu WEP stačilo bezdrátovou komunikaci mezi přístupovým bodem a klientem pouze analyzovat a zachytit potřebný počet inicializačních vektorů (IV) k prolomení 64 nebo 128 bitového klíče. Prolomit protokol WPA statistickou metodou není z hlediska šifrování každého vysílaného paketu novým IV prakticky možné. Časově náročná by byla i metoda útoku hrubou silou (brute force attack). Využita byla proto metoda slovníkového útoku, která se v laboratorních podmínkách jeví jako nejvhodnější. Prolomení klíče samozřejmě závisí na použité databázi slov. Proto byl využit méně rozsáhlý slovník linuxového balíčku Back Track 5 pro testování bezpečnosti bezdrátových sítí. Za těchto podmínek je prolomení ještě mnohem efektivnější oproti předešlé statistické metodě. Úloha tak může být pro studenti velice zajímavá, ale měli by zohlednit, že uvedené postupy slouží k testování bezpečnosti WLAN sítí a tím pomáhají odstraňovat její nedostatky.

V druhé úloze byly prozkoumány možnosti video streamu v bezdrátové WLAN síti, který vysílala bezdrátová IP kamera. Studenti si mohou vyzkoušet práci ze specifickou bezdrátovou IP kamerou, která skrývá v sobě širokou škálu možností. Od jednoduchého streamování ve WLAN síti až po její bezpečnostní charakter, kdy pomocí senzorů citlivých na pohyb nebo zvuk notifikuje svého administrátora o činnosti v monitorované zóně.

LITERATURA

[1] LABIOD, H., AFIFI, H., SANTIS, C. *Wi-Fi(TM), Bluetooth(TM), Zigbee(TM) and WiMax(TM)*. Springer. 2007. ISBN-10: 978-1-4020-5396-2.

[2] VÁVRA, Š. *Současné normy a trendy WLAN aneb kam směrují technologie bezdrátových sítí standardu 802.11*. 2006, s. 11. Dostupné z: <http://radio.feld.cvut.cz/personal/mikulak/MK/MK06_semestralky/SoucasneNormyAtrendyWLAN_VavraS.pdf>.

[3] Wi-fi.org [online]. 2011 [cit. 2011-10-28]. Wi-Fi Alliance: Discover and Learn. Dostupné z: <http://www.wi-fi.org/discover_and_learn.php>.

[4] Wi-Fi na všechny způsoby. *Computer*. 2011, 22, s. 116.

[5] *Wifinotes.com* [online]. [201?] [cit. 2011-11-10]. 10 tips for wireless network security - Tips for wireless network security. Dostupné z: <http://www.wifinotes.com/10-tips-for-wireless-network-security.html>.

[6] NOVOTNÝ, V. *Architektura sítí*. 2002.

[7] Radio-electronics.com [online]. [cit. 2012-01-27]. IEEE 802.11i Wi-Fi Security: WEP & WPA / WPA2. Dostupné z: <http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11i-security-wpa2-wep.php>.

[8] BURDA, K. Bezpečnost informačních systémů. 1. Brno: FEKT VUT Brno, 2005. s. 1 (s.).

[9] Návod k balíčku instrukcí Aircrack-ng pro auditorské činnosti v IEEE 802.11 sítích. Dostupné z: <http://www.aircrack-ng.org>.

[10] NOVOTNÝ, V. *Komunikační prostředky mobilních sítí.* 2002.

[11] Auto Light Sensor Wireless-G MegaPixel IP Camera. *AirLive AirCam WL-350HD* User's *Manual*, s. 98. Dostupné z: <http://fs.airlive.com/manual/AirLive_WL-350HD_Manual.pdf>.

SEZNAM ZKRATEK

ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AP	Access Point
ASCII	American Standard Code for Information Interchange
BS	Base Station
BSS	Base Service Set
BSSID	Base Service Set Identifier
CB	Citizens Band
CCMP	CCM mode Protocol
CRC	Cycling Redundancy Check
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution Systém
DSSS	Direct Sequence Spread Spectrum
EDCA	Enhanced DCF Channel Access
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FFT	Fast Fourier Transform
FHSS	Frequency Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
GSM	Global System for Mobile Communications
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HIPERLAN	High Performance Radio LAN
HT	High Throughput
IBSS	Independent Basic Service Set
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
ISM	Industrial, Scientific and Medical
ISO	International Organization for Standardization
KV	Krátke vlny
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MIMO	Multiple-in Multiple-out
MS	Mobile Station
MSDU	Mac Service Data Unit
NIC	Network Interface Card
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PCI	Peripheral Component Interconnect
PDA	Personal Digital Assistant
PCF	Point Coordination Function

PCMCIA	Personal Computer Memory Card International Association
PTA	Pairwise Transient Key
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RRM	Radio Resource Measurement
RADIUS	Remote Authentication Dial In User Service
SSID	Service Set Identifier
STC	Space Time Coding
TKIP	Temporal Key Integrity Protocol
UMTS	Universal Mobile Telecommunications Systém
VoIP	Voice over Internet Protocol
WAVE	Wireless Access for the Vehicular Environment
WBAN	Wireless Body Area Network
WECA	Wireless Ethernet Compatibility Association
WEP	Wired Equivalent Privacy
WDS	Wireless Distribution Systém
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network