

Praktické využití programů pro analýzu a aktivitu kanálu WiFi sítě

Practical Application programs WiFi Network analysis and channel
activity

Bc. Andrea Malotová

Diplomová práce
2012



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Andrea MALOTOVÁ**
Osobní číslo: **A10457**
Studijní program: **N 3902 Inženýrská informatika**
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Praktické využití programů pro analýzu a aktivitu kanálu WiFi sítí**

Zásady pro vypracování:

1. Seznamte se s problematikou WiFi sítí a jejich využitím v praxi.
2. Uvedte možné útoky do WiFi sítí.
3. Provedte praktické odzkoušení programů pro monitorování WiFi sítí ve vybraných exponovaných místech budovy U5 Fakulty aplikované informatiky UTB.
4. Prozkoumejte zabezpečení WiFi sítí pomocí programu inSSIDer budovu U5 metodou warstrollingu.
5. Verifikujte získaná data pomocí software Wi-Spy Chanalyzer Lite.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. Brno: Computer Press, a.s., 2008. ISBN 978-80-251-2073-6.
2. ZANDL, Patrick. Bezdrátové sítě WiFi : Praktický průvodce. Brno : Computer Press, a.s., 2003. ISBN 80-7226-632-2.
3. BARKEN, Lee. Jak zabezpečit bezdrátovou síť Wi-Fi. Brno : Computer Press, a.s., 2004. ISBN 80-251-0346-3.
4. PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G. Brno: CP Books, a.s., 2005. ISBN 80-251-0791-4.
5. IVANKA, Ján a Marek ČANDÍK. Konfigurace a zabezpečení WiFi sítí. In: Security magazín. Praha: Familymedia, 2007, 4 - 8. ISSN 1210 - 8723.
6. IVANKA, Ján a Petr NAVRÁTIL. Standardizace WiFi sítí a jejich využití v průmyslu komerční bezpečnosti. In: Security magazín. Praha: Familymedia, 2009, 25 - 31. ISSN 1210 - 8723.

Vedoucí diplomové práce:

Ing. Ján Ivanka

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

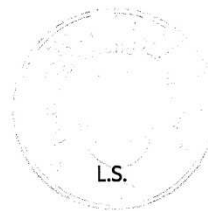
24. února 2012

Termín odevzdání diplomové práce:

15. května 2012

Ve Zlíně dne 24. února 2012

prof. Ing. Vladimír Vašek, CSc.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce řeší problematiku WiFi sítí a je rozdělena na 6 základních částí. Teoretické kapitoly se zaměřují na začlenění WiFi sítě do bezdrátové technologie, popisují jejich zabezpečení a jsou specifikovány antény, které se využívají k šíření elektromagnetického signálu. V praktické části se zabývám softwary sloužící ke skenování WiFi sítí. Součástí práce je mapování WiFi sítí softwarem inSSIDer na budově U5 FAI UTB a následné vyhodnocení získaných dat.

Klíčová slova:

WiFi, elektromagnetický signál, WPA, warstrolling, inSSIDer, Wi-Spy

ABSTRACT

The dissertation deals with WiFi issues and is divided into 6 basic parts. Theoretical chapters focus on the involvement of WiFi into wireless technology, describes its securing and there are also specified antennas which serves for spreading electromagnetic signal. In the practical part, I am dealing with software products which serve for WiFi networks scanning. Part of this dissertation is WiFi networks mapping by means of inSSIDer software at U5 FAI UTB building and subsequent evaluation of gained data.

Keywords:

WiFi, electromagnetic signal, WPA, warstrolling, inSSIDer, Wi-Spy

Poděkování:

Na tomto místě bych ráda poděkovala panu Ing. Jánovi Ivankovi za vedení mé diplomové práce a poskytnutí materiálů. Děkuji svým rodičům, že mi umožnili studovat vysokou školu a sourozencům za psychickou podporu.

Motto:

„Délka života závisí na vnějších věcech a nikoli na mně. Na mně jen záleží, jak prožiji čas, který mi byl určen.“

Seneca

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD.....	9
I TEORETICKÁ ČÁST.....	10
1 WIFI V RÁMCI BEZRÁTOVÝCH SÍTÍ.....	11
1.1 TYPOLOGIE BEZRÁTOVÝCH SÍTÍ	11
1.1.1 Wireless Personal Area Network	11
1.1.2 Wireless Local Area Network	12
1.1.3 Wireless Metropolitan Area Network	12
1.1.4 Wireless Wide Area Network	14
1.2 ARCHITEKTURA SÍTĚ	14
2 ZABEZPEČENÍ WIFI SÍTÍ.....	16
2.1 ÚTOKY NA WIFI SÍTĚ	16
2.1.1 Rozluštění klíče WEP	16
2.1.2 Zjištění MAC adresy	16
2.1.3 Útok „Muž uprostřed“	17
2.1.4 Slovníkový útok	17
2.1.5 Session Hijacking.....	17
2.1.6 DoS útoky.....	17
2.2 BEZPEČNOST VE WIFI SÍTÍCH	17
2.2.1 WEP	18
2.2.2 WPA.....	18
2.2.3 802.1x.....	19
3 ANTÉNY UŽÍVANÉ PRO WIFI SÍTĚ.....	20
3.1 PARAMETRY ANTÉN	20
3.2 TYPY ANTÉN.....	20
3.2.1 Všesměrové antény	21
3.2.2 Sektorové antény	21
3.2.3 Směrové antény	22
3.3 ZÁKLADNÍ PROBLÉMY PŘI ŠÍŘENÍ SIGNÁLU VE WIFI SÍTÍCH.....	23
II PRAKTICKÁ ČÁST	26
4 MĚŘENÍ DOSTUPNÝCH SIGNALŮ WIFI SÍTÍ SPECIÁLNÍMI PROGRAMY NA BUDOVĚ U5	27
4.1 SOFTWAREY K MONITOROVÁNÍ WIFI SÍTÍ.....	28
4.1.1 Použitý nástroj k měření.....	28
4.1.2 WirelessMon	28
4.1.3 Vistumbler.....	30
4.1.4 InSSIDer.....	32
4.1.5 NetSurveyor	33
4.1.6 XiRRUS Wi-Fi Monitor.....	35
4.2 METODIKA MĚŘENÍ WIFI SÍTÍ JEDNOTLIVÝMI SOFTWAREY NA VYBRANÝCH MÍSTECH BUDOVY U5	37
4.2.1 Zhodnocení výsledků z měřených stanovišť	39
5 SPEKTRÁLNÍ ANALYZÁTOR WI-SPY 2.4I.....	47
6 DETAILNÍ MAPOVÁNÍ WIFI SÍTĚ EDUROAM NA BUDOVĚ U5	

PROGRAMEM INSSIDER.....	52
6.1 METODIKA MĚŘENÍ DAT	52
6.2 SUMARIZACE A ZHODNOCENÍ ZÍSKANÝCH DAT	54
ZÁVĚR	59
CONCLUSION	61
SEZNAM POUŽITÉ LITERATURY.....	63
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	66
SEZNAM OBRÁZKŮ	68
SEZNAM TABULEK.....	70
SEZNAM PŘÍLOH.....	71

ÚVOD

Diplomová práce prezentuje v úvodní literární rešerzé o tématice WiFi sítí. Stěžejní část je zaměřena na monitorování WiFi sítí a jejich následný průzkum na budově U5 Fakulty aplikované informatiky Univerzity Tomáše Bati na Jižních Svazích ve Zlíně softwarem inSSIDer a za využití metody warstrolling.

Hlavním cílem práce je praktické seznámení se s freewarovými programy pro měření WiFi sítí a s cenově přijatelným Wi-Spy 2.4i s USB rozhraním. Její přínos spočívá v podrobném zmapování kvality dostupných signálů WiFi sítí eduroam na budově U5 a následné zhodnocení změřených dat.

Práce je rozdělena na 6 základních kapitol. V úvodu představuji základní členění bezdrátových sítí se zaměřením na WLAN sítě, kam spadá standard WiFi. Dále prezentuji možné útoky potencionálních pachatelů do klientských stanic v rámci WiFi sítí. Teoretická část poskytuje informace o primárním zabezpečení bezdrátových sítí autentizačními standardy a šifrovacími technikami.

V třetí kapitole představuji základní typy antén využívaných k šíření elektromagnetického signálu a jejich parametry. Jedná se zejména o všesměrové, sektorové a směrové antény.

Čtvrtý bod práce je věnován freewarovým programům pro monitorování WiFi sítí - jejich základní charakteristika, funkce a pracovní prostředí. Prakticky jsou odzkoušeny na exponovaných místech budovy U5 a výsledky měření jsou následně tabulkově zpracovány. Dále se zabývám uplatněním spektrálního analyzátoru Wi-Spy 2.4i.

V následující části je provedeno detailní zkoumání zabezpečení WiFi sítí, kde se soustředuji na kvalitu signálu místní školní sítě eduroam. Měření praktikuji na vybraných trasách na budově U5 pomocí programu inSSIDer a za využití metody warstrolling. Závěrem práce jsou získaná data měření zobrazena a zhodnocena.

I. TEORETICKÁ ČÁST

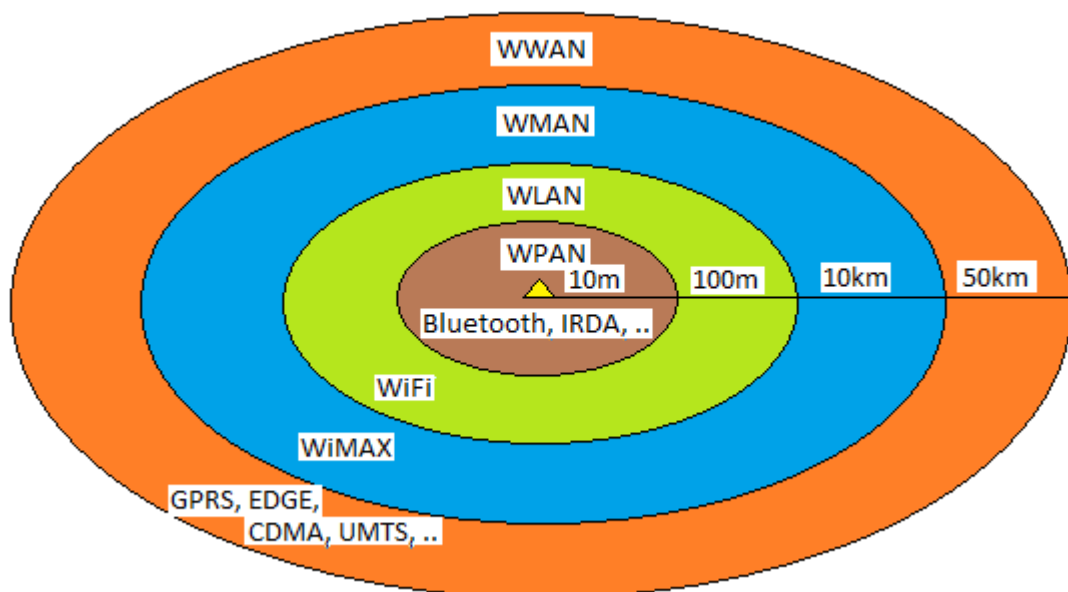
1 WIFI V RÁMCI BEZRÁTOVÝCH SÍTÍ

Bezdrátová síť je druh počítačové sítě, ve které se signál mezi jednotlivými účastníky přenáší pomocí elektromagnetického vlnění, které patří v současné době mezi nejvíce využívané přenosové médium.

Nelicencované frekvence 2,4 GHz a 5 GHz jsou primárně určeny pro bezdrátové sítě. Pásmo 2,4 GHz je volně použitelné, čímž dochází častěji k přetížení a ke stále většímu vzájemnému rušení jednotlivých přenosů. Kromě bezdrátových sítí je využívají také technologie bluetooth či bezdrátové telefony. Pásmo 5 GHz, jehož provoz je regulován Českým telekomunikačním úřadem, je příznivější pro použití v prostředí měst z důvodu nižšího zarušení. Radary či některé satelitní systémy pracují v pásmu 5 GHz. [1]

1.1 Typologie bezdrátových sítí

Bezdrátové datové technologie se nejobvykleji dělí na základě vzdálenosti uživatele od přípojného bodu k Internetu.



Obrázek 1: Vzdálenosti bezdrátových sítí [4]

1.1.1 Wireless Personal Area Network

Připojení Wireless Personal Area Network (dále jen WPAN), **bezdrátové soukromé sítě**, k Internetu je prakticky realizováno v jedné místnosti. Slouží k propojování zařízení jako mobilního telefonu či Personal Digital Assistant (dále jen PDA) mezi sebou, nejčastěji

v seskupení Ad-hoc. Použitelný dosah u WPAN je okolo 10 metrů. WPAN je využívána především u technologií bluetooth, IrDA, vzácněji Zigbee. The Institute of Electrical and Electronic Engineers (dále jen IEEE) ji normalizuje ve skupině s číslem 802.15. [4]

1.1.2 Wireless Local Area Network

Zástupcem Wireless Local Area Network (dále jen WLAN), **bezdrátové místní sítě**, je standard **Wireless Fidelity** (dále jen WiFi). **WiFi** je certifikát, který obdrží výrobek vyhovující standardům IEEE a splňující požadavky na vzájemnou kompatibilitu daného výrobku s ostatními. Standardizační skupina 802.11 společnosti IEEE je zaměřená na standardy lokálních sítí. [4]

Nálepku WiFi uděluje aliance, založená hlavními výrobci bezdrátové technologie, **WiFi Alliance**, dříve Wireless Ethernet Compatibility Alliance – Sdružení pro kompatibilitu bezdrátového Ethernetu. [1]

Jednotlivá zařízení WLAN pracují většinou v režimu infrastrukturní sítě, ale mohou fungovat i v seskupení Ad-hoc. Se vznikajícími normami a zlevňováním techniky si WLAN našla daleko větší uplatnění. Vznikaly tzv. **hot spoty** (zóny s přístupovým bodem k WiFi síti) na letištích, v restauracích, hotelích, školách, aj. [3]

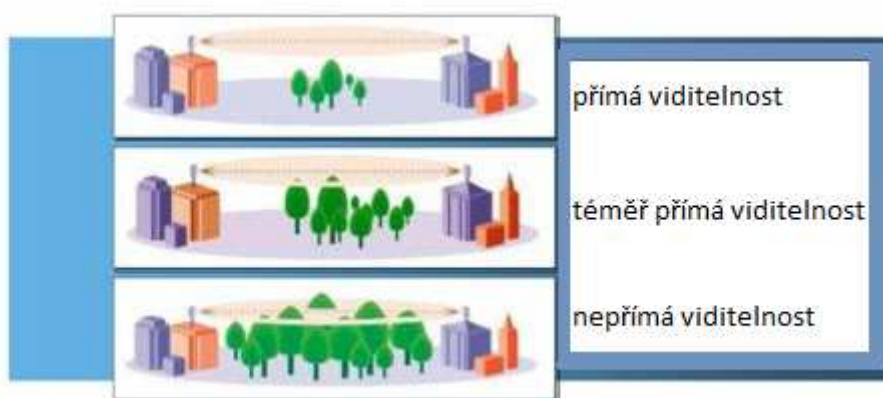
Název technologie	Rok uvedení	Přenosová frekvence	Maximální teoretická rychlost datového přenosu	Maximální vzdálenost vysílače a přijímače
WiFi (IEEE 802.11a)	1999	5 GHz	54 Mbps	100/30 m
WiFi (IEEE 802.11b)	1999	2,4 GHz	11 Mbps	110/35 m
WiFi (IEEE 802.11g)	2003	2,4 GHz	54 Mbps	110/35 m
WiFi (IEEE 802.11n)	2006	2,4/5 GHz	150 Mbps	160/70 m

Tabulka 1: Vlastnosti technologie WLAN [4]

1.1.3 Wireless Metropolitan Area Network

Wireless Metropolitan Area Network (dále jen WMAN), **bezdrátová metropolitní síť**, je zastoupena stále se rozrůstající technologií **Worldwide Interoperability for Microwave**

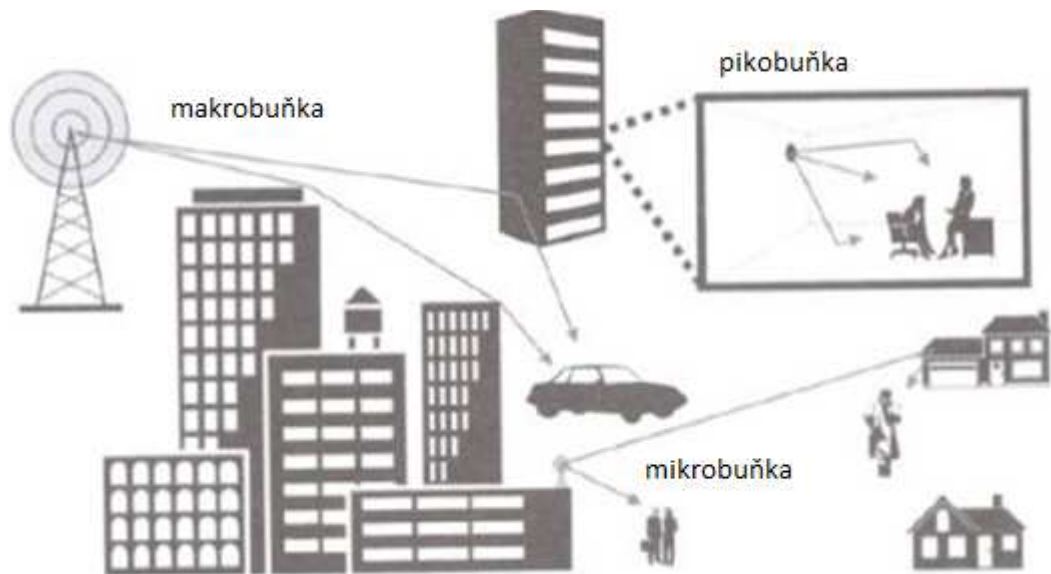
Access (dále jen WiMAX) normalizovanou ve skupině IEEE 802.16. **WiMAX** je standard zaměřený na bezdrátovou komunikaci ve venkovních sítích. Přenos dat u WMAN je uskutečňován bez nutnosti přímé vizuální viditelnosti. Rádiová viditelnost zahrnuje pomyslnou přímku mezi vysílačem a přijímačem a určitou oblast kolem této spojnice. Jde o tzv. **Fresnelovu zónu**, jež má elipsovité tvar. [4]



Obrázek 2: Režimy viditelnosti ve Fresnelově zóně

Technologie WiFi je primárně určena pro přenos dat v lokálním vnitřním prostředí (pikobuňka či mikrobunčka), **vyloučeno není ani vnější prostředí** v rámci makrobunčky. Zde **musí být zachována přímá vizuální a rádiová viditelnost** mezi vysílačem a anténou klienta. Jde o tzv. **režim Line of Sight** (přímá viditelnost). [4]

- Pikobuňka – šíření signálu je možné v rámci budov či institucí, dosah se pohybuje okolo desítek metrů.
- Mikrobunčka – signál pokryje vzdálenost od stovek metrů až po několik kilometrů.
- Makrobunčka – signál může zastřešit celou osídlenou oblast až do vzdálenosti několika desítek kilometrů (cca 30 kilometrů).



Obrázek 3: Šíření signálu v rámci buněk [4]

1.1.4 Wireless Wide Area Network

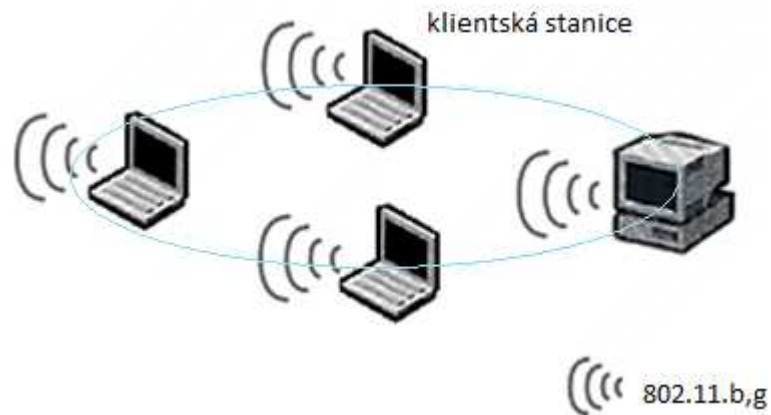
Technologie Wireless Wide Area Network (dále jen WWAN), **bezdrátové rozsáhlé sítě**, nabízí vyšší dosah bezdrátového přenosu dat a nejvyšší mobilitu ze všech typologií bezdrátových sítí. Je využívána především mobilními sítěmi pro **Global System for Mobile Communications** (dále jen GSM), **Universal Mobile Telecommunications System** (dále jen UMTS) či **Code Division Multiple Access 2000** (dále jen CDMA2000). Technologie UMTS je standard pro 3G systém mobilních telefonů, jenž brzy nahradí síť GSM. Kódový multiplex CDMA2000 zajišťuje přenos více digitálních signálů používajících odlišné kódování pomocí jediného sdíleného média. [4]

1.2 Architektura sítě

Existují různé způsoby vybudování bezdrátových sítí v závislosti na požadované funkci. Vždy klíčovou roli zaujímá identifikátor **Service Set Identifier** (dále jen SSID). SSID představuje řetězec 32 ASCII znaků rozlišující jednotlivé sítě v daném dosahu.

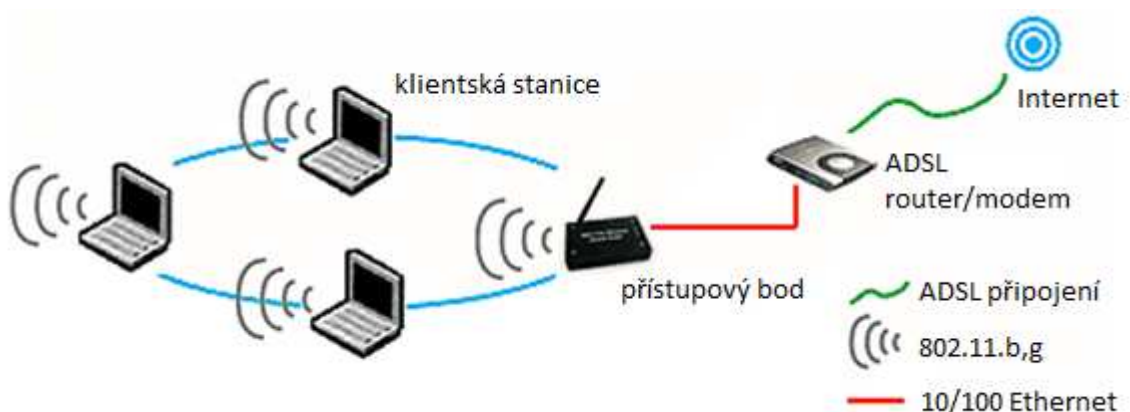
Jedna z možností vybudování sítě je **Ad-hoc síť**. Zde se navzájem spojují klientské stanice, jež vysílají své SSID do prostoru a které jsou v rovnocenné pozici neboli peer-to-peer. Klienti spolu mohou komunikovat pouze v přímém rádiovém dosahu do vzdálenosti několika metrů, což je typické například pro propojení menšího počtu notebooků v jedné místnosti. Struktura Ad-hoc je spíše příležitostní síť pro nárazovou výměnu dat mezi

klientskými stanicemi a méně využívanou kvůli časové náročnosti pro nakonfigurování celé sítě. [2]



Obrázek 4: Struktura sítě Ad-hoc [2]

Síť obsahující jeden nebo více přístupových bodů, spíše známých pod anglickým názvem Access Point (dále jen AP), se nazývá **infrastrukturní síť**. AP se rozumí jednoúčelové zařízení s potřebným softwarem. Jednotlivé stanice nemusí být ve vzájemném dosahu, ale v dosahu AP vysílající své SSID do prostoru. Klient poté pohodlně volí, ke kterému z viditelných WiFi APs v dosahu se připojí. Díky infrastrukturní typologii lze navrhnout síť mnohem větších rozměrů a spravovat ji centrálně, proto je také nejvíce a nejběžněji využívaným typem WiFi sítí. [2]



Obrázek 5: Infrastrukturní síť [2]

2 ZABEZPEČENÍ WIFI SÍTÍ

Zabezpečení WiFi sítí je důležitým krokem k ochraně informací přenášených bezdrátovou komunikací. Potenciálním útočníkům využívajícím nejběžnější metody útoků na bezdrátové sítě se musí zamezit volný vstup k uchovávaným datům. Klient musí praktikovat v zásadě dvě bezpečnostní opatření:

- **autentizace**, tzn. oprávnění přidání nového uživatele do WiFi sítě a
- **kódování**, tzn. šifrování přenášených dat.

2.1 Útoky na WiFi sítě

Obecně se útoky mohou dělit dle toho, jakým typem šifrovacího protokolu je daná síť zabezpečena. Praktičtější je výčet metod používaných potenciálními útočníky a uvést možnou ochranu proti nim.

2.1.1 Rozluštění klíče WEP

Wired Equivalent Privacy (dále jen WEP) klíč se dá rozluštit pomocí open source programů jako AirSnort nebo WEPCrack, jenž má útočník k dispozici. Programy zachytávají komunikaci mezi AP a samotným klientem, kdy se útočník spoléhá na to, že klient nezmění během scanování sítě svůj WEP klíč.

Možná obrana spočívá v použití šifrování a autentizačních mechanismů, např. Virtual Private Network (dále jen VPN) a 802.1x. VPN se využije v případě, kdy AP nebo bezdrátový směrovač domácí sítě se chce připojit do firemní sítě. [6]

2.1.2 Zjištění MAC adresy

Media Access Control (dále jen MAC) adresa je označována jako fyzická adresa, která plní úkol jedinečného identifikátoru síťového zařízení. Princip zachytávání komunikace je stejný jako u metody útoku rozluštění WEP klíče a útočník si hlavičku MAC adresy může vyhledat, přečíst, podstrčit a vystupovat jako oprávněný uživatel.

Útoku zjištění MAC adresy se dá předcházet aplikováním autentizačních mechanismů stejně jako u útoku rozluštění klíče WEP. [6]

2.1.3 Útok „Muž uprostřed“

„Muž uprostřed“ je útok technicky náročnější a doslova znamená, že útočník vstoupí a přeruší veškerý provoz mezi WiFi AP a klientem. Získává o nich základní informace, díky kterým může vytvořit podvržený AP a změnit připojení klienta přes něj. Útočník se obohatí o všechna data a i hesla klienta.

U obrany před útokem „Muž uprostřed“ je dobré mít detailní mapu své sítě a čas od času ji kontrolovat, zda se někde neobjevil nežádoucí AP. Rovněž se vyplatí používat VPN a autentizační mechanismus 802.1x. [6]

2.1.4 Slovníkový útok

Útočník využívá slovník, databázi přihlašovacích jmen a hesel, díky níž se snaží prolomit šifru. Existují různé a snadno získatelné open source programy pomáhající odhalit uživatelská jména a hesla. Výhodou pro českého správce sítě je, že přednostně jsou zaměřené na anglofonní uživatele.

Obranou je zde správně zvolené heslo za použití kombinace velkých a malých písmen, čísel a symbolů s minimální délkou osmi znaků. [6]

2.1.5 Session Hijacking

Session Hijacking je útok velmi složitý. Útočník zde může odposlouchávat síť, ale i vkládat a odesílat své vlastní informace, jako by to byly původní data od klienta či AP.

Obrana se dá zesílit použitím autentizace 802.1x a VPN. [6]

2.1.6 DoS útoky

Denial of Service (dále jen DoS) útokem může vetřelec vyřadit síť z provozu tím, že zahlcuje AP velkým množstvím nesmyslných dat. Způsobí tak zpomalení přenosového pásma či znemožní připojení dalších uživatelů.

Útoku DoS se dá účinně zabránit filtrováním MAC adres a používáním firewallu neboli tzv. kontrolního bodu definující pravidla komunikace mezi oddělenými sítěmi. [6]

2.2 Bezpečnost ve WiFi sítích

V rámci zabezpečení WiFi sítě nesmí chybět **firewall**, dále se musí **zablokovat SSID vysílání**, aby potenciální útočník nemohl zjistit název sítě a informace o ní. **MAC filtr** je

základní ochrana před nabouráním, tzn. na AP se nastaví MAC adresy mající, ale i nemající přístup do bezdrátové sítě. Dalším důležitým krokem je zvolení si takové **antény**, která pokryje signálem jenom požadovaný prostor. Poslední a nepostradatelnou součástí ochrany je použití **šifrování**. [9]

2.2.1 WEP

WEP byl integrován již do WiFi zařízení od protokolu 802.11b a ověřuje se zde MAC adresa síťové karty. Princip WEP tkví v použití stejného klíče pro šifrování odesílané zprávy a i dešifrování přijaté zprávy příjemcem. Výhoda WEP klíče je v jednoduchosti a výpočetní nenáročnosti.

Standardní délka klíče je 64 bitů, ale výrobci WiFi zařízení dokáží délku klíče natáhnout až na 128 či 256 bitů. V dnešní době se nejběžněji používá 128bitová verze WEP klíče. K používání 256bitového klíče se dnes nepřistupuje, neboť bezpečnostním standardem se stal **WiFi Protected Access** (dále jen WPA). [9]

2.2.2 WPA

Protokol WPA je podmnožinou normy 802.11i od roku 2003. Výhodou WPA je průběžná a automatická výměna vytvářených klíčů pro šifrovací taktiky a dostatečná délka klíče pro šifrování (až 256 bitů). **Temporal Key Integrity Protocol** (dále jen TKIP) se rozumí šifrovací klíče, které jsou známy jen klientským stanicím připojícím se do sítě a po jejím odhlášení se smažou. [1]

WPA2 přináší kvalitnější šifrování pomocí šifry **Advanced Encryption Standard** (dále jen AES), jenž nelze použít ve starších zařízeních, neboť vyžaduje větší výpočetní výkon. Symetrická bloková šifra AES používá stejný klíč pro šifrování i k dešifrování a vyznačuje se vysokou rychlostí šifrování. [7]

Existuje i šifrovací sada **AES-CCMP** (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), která je zahrnuta v normě IEEE 802.11i. Obsahuje dvě důmyslné kryptografické techniky provádějící šifrování i dešifrování 128bitovým klíčem. CCMP je bezpečnostní protokol, který je nutný k ověření komunikace mezi klientem a AP.

2.2.3 802.1x

Šifrovací mechanismus 802.1x dovoluje používat protokol **Extensible Authentication Protocol** (dále jen EAP) v bezdrátových sítích. EAP umožňuje kvalitnější úroveň přihlašování uživatelů a blokuje přístup neoprávněným uživatelům. Autorizační server RADIUS provádí samotné ověřování uživatele podle seznamu povolených klientů.

Produkty s podporou autentizace podle standardu 802.1x jsou praktikovány do Windows XP a především v zařízeních určených pro firmy, jež vyžadují vyšší bezpečnost a nevdají jim za ni zaplatit. [7]

3 ANTÉNY UŽÍVANÉ PRO WIFI SÍTĚ

WiFi se přednostně využívá pro šíření signálu uvnitř budov. V posledních letech ale nachází své uplatnění k propojování i pět kilometrů vzdálených bodů, či na českém telekomunikačním trhu k řešení problému tzv. „*poslední míle*“, čímž se rozumí distribuce připojení k Internetu. [6]

Kvalitní externí anténa je klíčová část komplexního návrhu WiFi sítě využívané zejména pro větší vzdálenosti. Smyslem antény je vyzařovaný radiový signál zaostřit do daného místa, určitým směrem či tvarem, nikoliv jej zesílit.

3.1 Parametry antén

Při výběru antén hrají důležitou roli její parametry, na základě kterých se určují provozní a výkonnostní charakteristiky. [6]

Směrovost udává, v jakém směru, tvaru či pod jakým úhlem dokáže anténa vyzařované elektromagnetické pole vysílat či přijímat.

Polarizace představuje rovinu šíření signálu. Existují dva základní typy a to lineární (horizontální a vertikální) a kruhová polarizace. Šíření signálu je nejčastější ve vertikálním směru. [6]

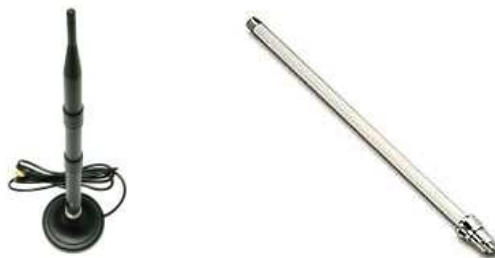
Zisk antény se měří v decibelech na isotop (dBi) a říká, čím větší bude ziskovost, tak tím vzdálenější signál anténa zachytí. Prakticky jde o poměr intenzit vyzařování v daném směru k intenzitě rovnoměrného vyzařování do všech směrů tzv. isotropní anténou. Isotropní zářič z jednoho bodu distribuuje energii v úhlu 360 stupňů. Zisk antény se pohybuje od 9 dBi až do 24 dBi. Záleží na typu antény a úhlu, pod kterým je signál vyzařován. [6]

Dalším důležitým parametrem je **frekvence**, v které daná anténa může fungovat. Jedná se o pásma 2,4 GHz nebo 5 GHz. Existují i tzv. **dual-band antény**, které lze použít pro obě frekvenční zóny. [4]

3.2 Typy antén

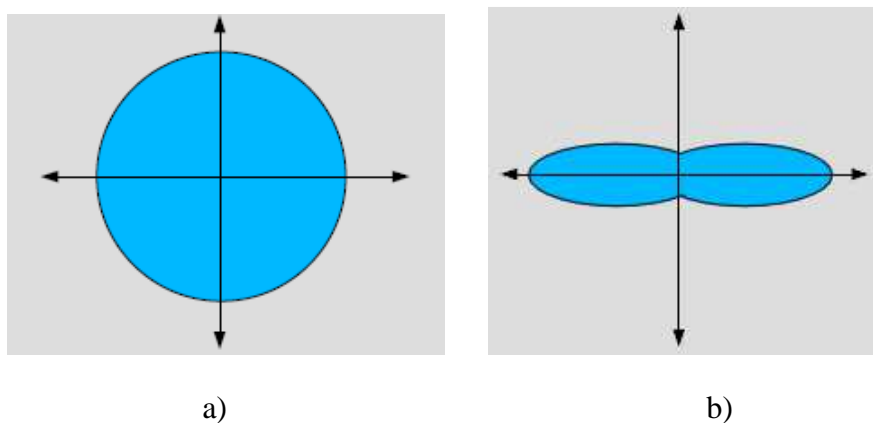
Z parametru antén - **směrovost** - vyplývá jejich základní dělení a to na všesměrové, sektorové a směrové.

3.2.1 Všesměrové antény



Obrázek 6: Všesměrové antény [4]

Všesměrová anténa šíří signál do všech stran a pokrývá tak úhel 360 stupňů v horizontální rovině. Úhel je znatelně menší při šíření signálu ve vertikálním směru. Vyzařované pole má tvar prstence. Umísťují se tam, kde je nutnost souvislého pokrytí, např. na sloupy, stožáry, stropy. [6]



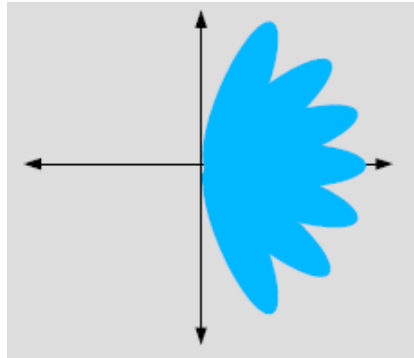
Obrázek 7: Vyzařovací diagram všesměrové antény a) v horizontálním směru a b) ve vertikálním směru [12]

3.2.2 Sektorové antény



Obrázek 8: Sektorové antény [9]

Sektorová anténa, nebo taky panelová či patch anténa, vyzařuje signál do určitého úhlu, většinou jde o 30 – 120 stupňů, maximálně až 180 stupňů v horizontální a vertikální rovině. Uplatnění nacházejí v místech, kde je potřeba vykryt speciálně omezené oblasti či je nutné zabránit proniknutí signálu mimo danou oblast. [6]



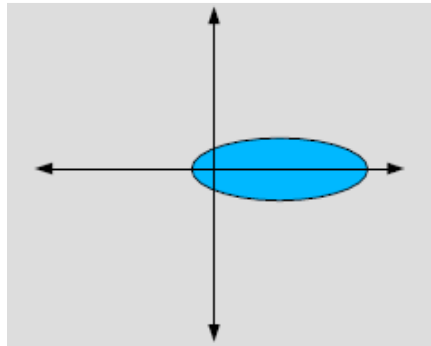
Obrázek 9: Vyzařovací diagram sektorové antény [12]

3.2.3 Směrové antény



Obrázek 10: Směrové antény [2]

Směrová parabolická anténa, označovaná též jako parabolická síťová anténa, směřuje signál do jednoho bodu, jenž může být od antény vzdálený i několik kilometrů. Ziskovost antény je vysoká a směrovost úzká. Úhel se pohybuje maximálně do 10 stupňů. Umísťují se většinou na střechy. [6]



Obrázek 11: Vyzařovací diagram směřové antény [12]

Yagi anténa je jedním z typů vysoce směrových antén. Yagi antény jsou menší a levnější. Uplatňují se zejména pro menší vzdálenosti, a proto nemají problémy se šířením signálu při silném větru. [9]



Obrázek 12: Yagi anténa [9]

3.3 Základní problémy při šíření signálu ve WiFi sítích

Existuje velké množství faktorů, jež mohou značně zkomplikovat šíření rádiových signálů ve WiFi sítích. Rádiový signál se musí vyrovnat se základními komplikacemi.

Rušení jinými systémy nacházející se ve stejném pásmu patří k nejdůležitějším komplikacím při šíření signálu. Technologie Breeze Net vysílá krátké signály a dokáže krátkodobě přerušit komunikaci ve WiFi spojeních v místech, kde se technologie setkávají. Omezený počet kanálů, které se nepřekrývají, způsobuje rušení komunikace ve WiFi zařízeních vyskytujících se v blízké vzdálenosti. Frekvenční pásmo 2,4 GHz poskytuje pouhé tři zcela oddělené kanály (1, 6 a 11) z celkového počtu 13, jež jsou využívány v Evropě. [10]

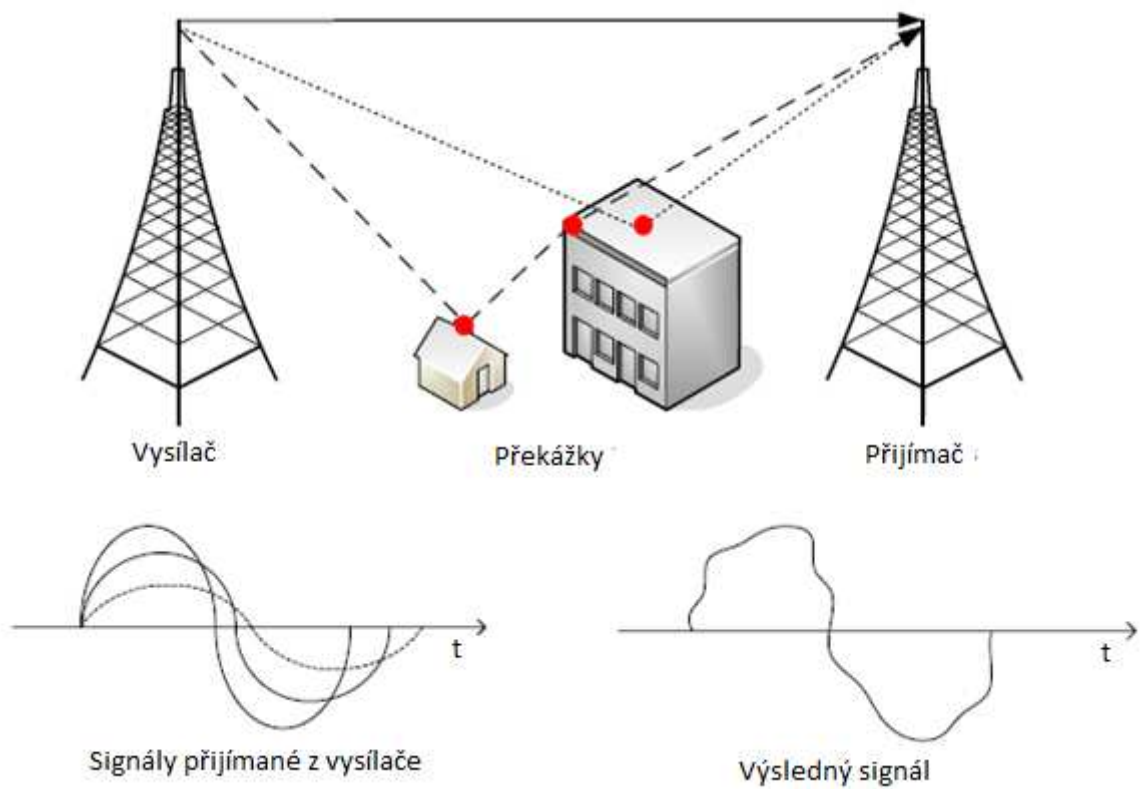
Kanál	Střední Kmitočet v GHz
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472

Tabulka 2: Kanály v pásmu 2,4 GHz využívané v Evropě [9]

Rušení způsobují také bezdrátové telefony, bluetooth, tzn. obecně zařízení pracující na frekvenci 2,4 GHz. [10]

Mezi anténami WiFi musí být zajištěna **přímá viditelnost**, jinak mohou nastat výpadky spojení či vznikat chyby při komunikaci. Nepříjemným faktorem rušení přímé viditelnosti jsou různé překážky jako budovy ze železobetonu, cihlového zdiva, dále stromy, zejména po dešti. Voda pohlcuje signál a to vede ke vzniku nepřekonatelné překážky. Na šíření signálu má negativní vliv i **počasí** (prudké deště, průtrže mračen), hlavně na větší vzdálenosti. [10]

Poslední komplikací při šíření signálu je **vícecestné šíření signálu (vícecestné interference)**. Při využití všesměrové antény u vysílače i přijímače je signál odrážen od různých překážek, a tím se vytvoří větší množství cest pro přenos signálu. [13]



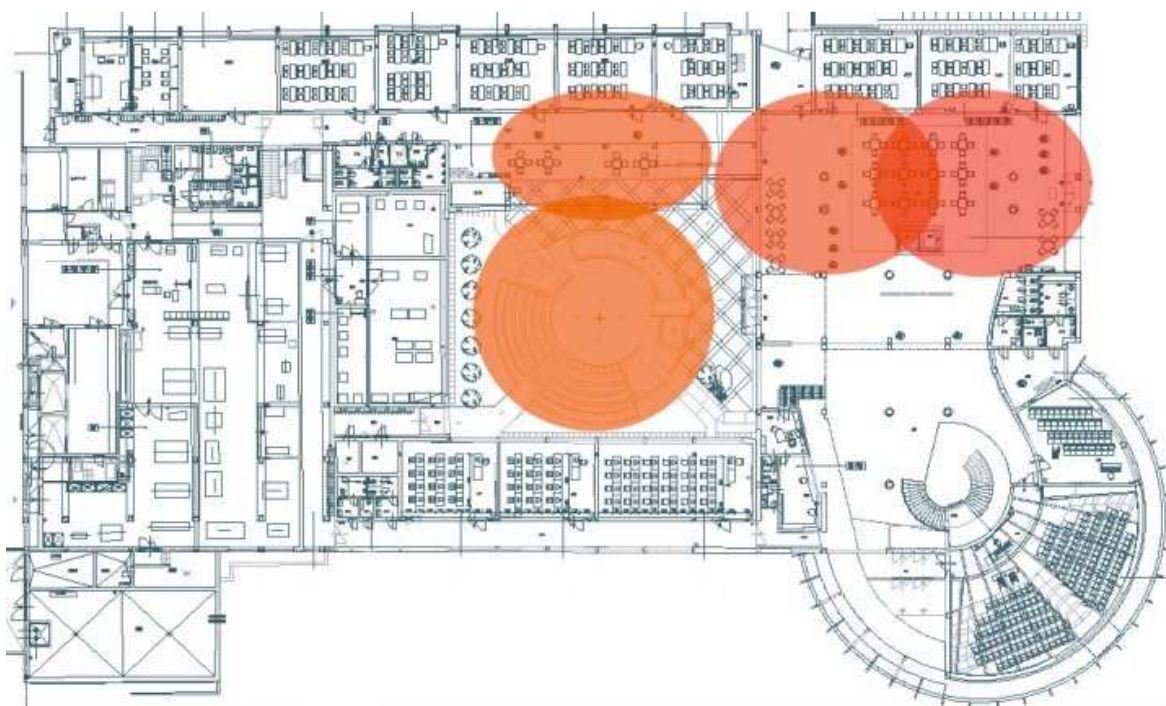
Obrázek 13: Princip vícecestného šíření signálu [13]

II. PRAKTICKÁ ČÁST

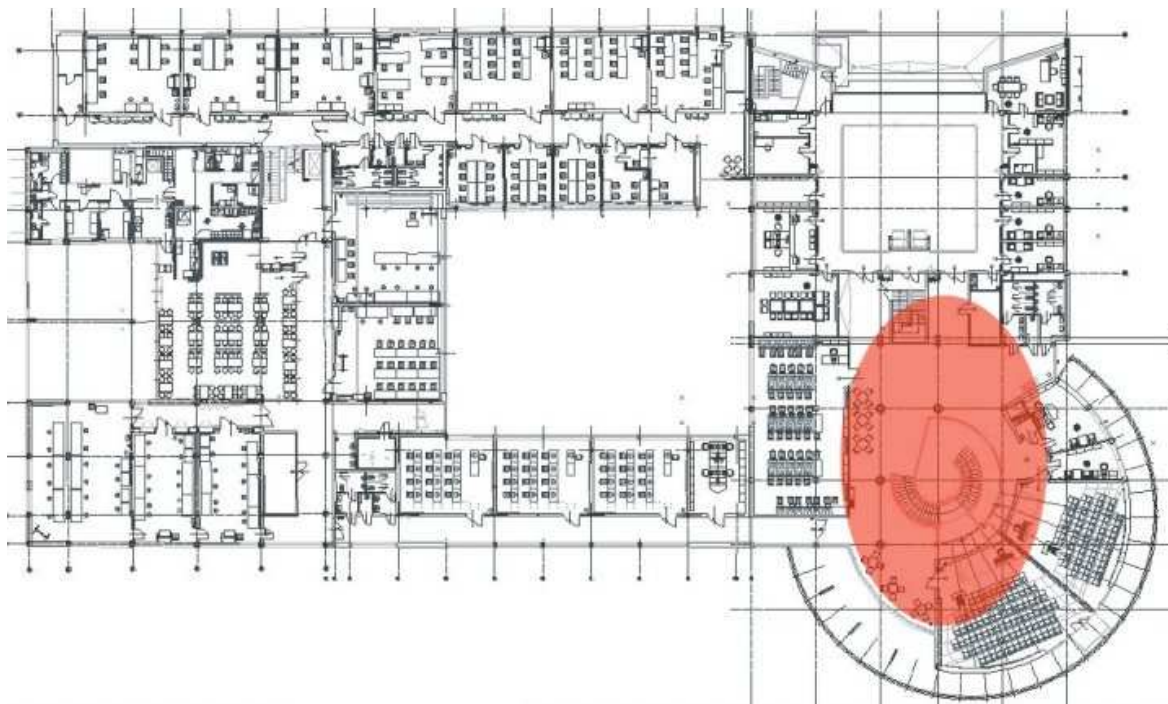
4 MĚŘENÍ DOSTUPNÝCH SIGNALŮ WIFI SÍTÍ SPECIÁLNÍMI PROGRAMY NA BUDOVĚ U5

WiFi síť jsem měřila na vybraných místech budovy U5 Fakulty aplikované informatiky Univerzity Tomáše Bati (dále jen FAI UTB), kde se studenti nejčastěji připojují k místním WiFi sítím s názvem eduroam. Přihlášení uživatelů do školní sítě probíhá na základě předchozí žádosti o registraci a následného přiřazení přihlašovacího jména a hesla žadateli. Každý uživatel má poté v rámci své domovské sítě svůj účet, jenž jej opravňuje k užívání bezdrátové sítě.

Sdružení CESNET z.s.p.o. zaštiťuje projekt eduroam.cz zaměřený na podporu Internet Protocol (dále jen IP) mobility v rámci České republiky a provoz RADIUS serverů, které jsou nutné pro propojení s Evropskou roamingovou strukturou. [19]



Obrázek 14: WiFi síť eduroam v prvním patře budovy U5 FAI UTB [20]



Obrázek 15: WiFi síť eduRoam ve druhém patře budovy U5 FAI UTB [20]

4.1 Softwary k monitorování WiFi sítí

4.1.1 Použitý nástroj k měření

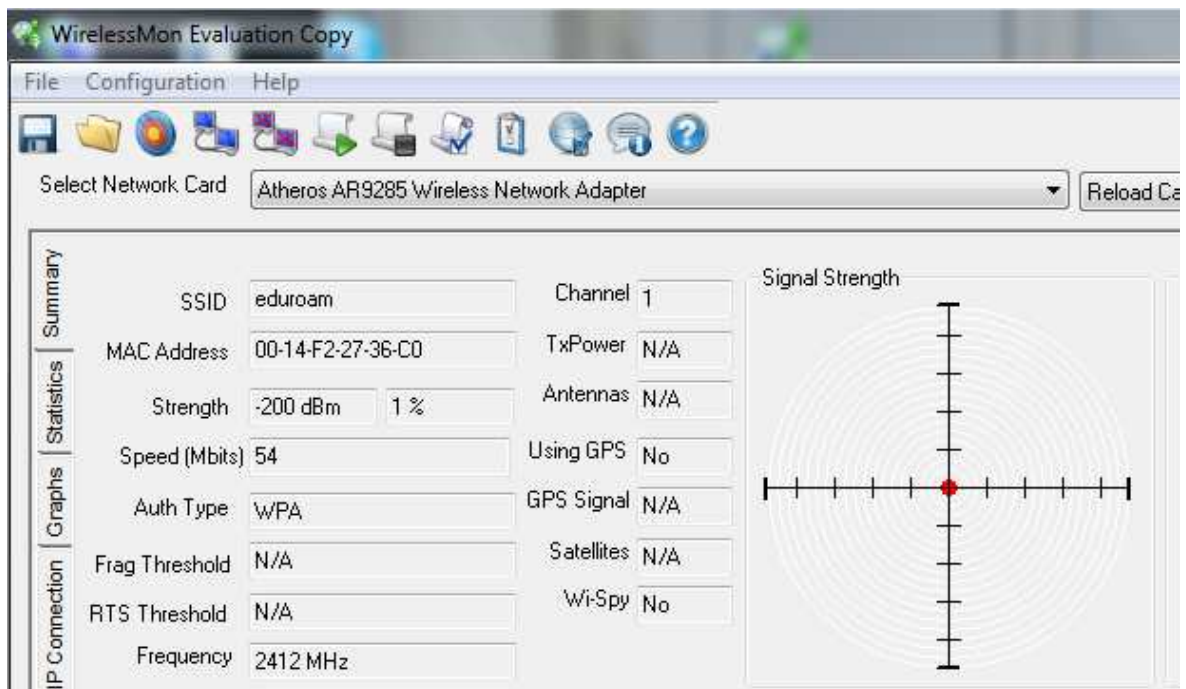
Softwary jsou nainstalované na notebooku ASUS K50IN-SX 139 s operačním systémem Professional Windows 7 a procesorem Intel Pentium® Core™ Duo T4300, jehož frekvence je 2,1 GHz. Notebook ASUS má síťovou kartu Atheros AR9285 Wireless Network Adapter, která podporuje standard 802.11 b/g/n + LAN 10/100/1000.

4.1.2 WirelessMon

WirelessMon slouží k monitorování bezdrátových sítí v reálném čase. Zobrazuje informace o stavu WiFi adaptéru, blízkých APs a hot spotech. Poskytuje i grafické zobrazení síly signálu v odlišných provedeních jako radar nebo různé druhy trojúhelníků.

WirelessMon nabízí příjemné uživatelské prostředí a práce se softwarem je jednoduchá a přehledně zobrazená v jednom okně. Skenování WiFi sítí není možné zastavit a pracovat pouze s určitými výsledky. Software WirelessMon detekuje WiFi sítě v okolí každých cca 10 sekund a dochází tak k neustálému nacházení či ztrátě dané sítě nebo k její změně viditelnosti.

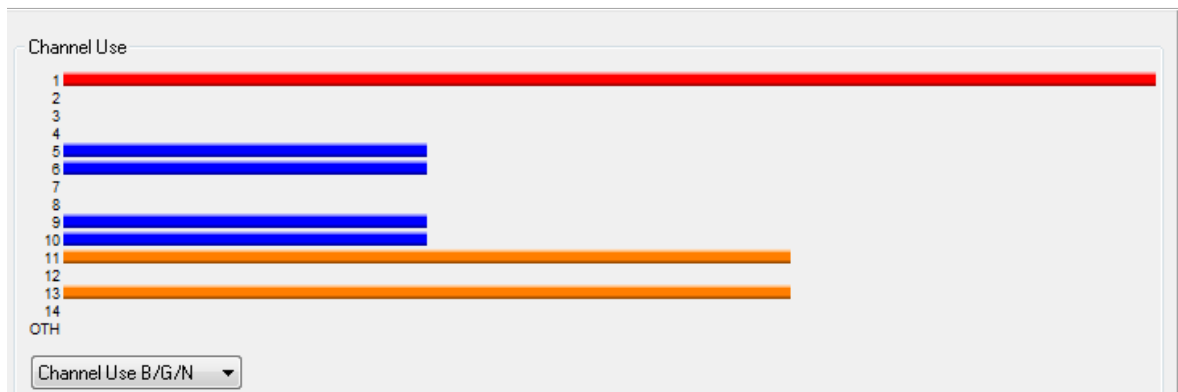
Při spuštění programu se zobrazí základní informace o WiFi síti, ke které jsem právě připojena jako SSID, MAC adresa, síla signálu v procentech a Received Signal Strength Indication (dále jen RSSI) v dBm, rychlost v Mb/s, šifrování, frekvence a použitý kanál. RSSI je veličina kvality signálu a platí, že čím vyšší hodnota RSSI, tím lepší signál. Můžu si zvolit i jinou síťovou kartu k měření.



Obrázek 16: WirelessMon - Informace o WiFi síti

Na postranním panelu se nachází kromě shrnutí dat o měřených WiFi sítích též statistika, časový graf síly signálu nebo graf přenášených dat kterékoliv dostupné sítě, dále záložka IP připojení zobrazující údaje síťové karty v Internetu.

Použité kanály WiFi sítěmi jsou vykresleny ve specifickém zobrazení. Je možné tak lépe vidět přetíženost daného kanálu.



Obrázek 17: WirelessMon - Použité kanály měřených WiFi sítí

Dostupné WiFi sítě v dosahu počítače se vypíší do dolní části obrazovky. Software o nich vypíše veškerá data, např. zda jsou dostupné, jejich SSID, použitý kanál, typ zabezpečení, počet výpadků, typ zařízení, atd. WirelessMon jako jediný poskytuje informace o typu sítě neboli o použitém standardu IEEE 802.11 a dále k němu v závorce zobrazuje použitou modulaci.

Status	SSID	C.	▲	Security	RSSI	Rates Supported	MAC Address	Network T...	Infrastructure	First Time S...
Available	eduroam	1		Yes (W...	-83	54,48,36,24,18,...	00-14-F2-27-37-A0	G (OFDM24)	Infrastructure ...	15:59:41 8-...
Available	51-616	1		Yes (W...	-87	54,48,36,24,18,...	00-22-75-E7-1F-...	N (HT)	Infrastructure ...	15:59:41 8-...
Available	eduroam	1		Yes (W...	-93	54,48,36,24,18,...	00-1E-7A-A9-38-...	G (OFDM24)	Infrastructure ...	16:00:13 8-...
Available	eduroam	5		Yes (W...	-61	54,48,36,24,18,...	00-14-F2-27-36-20	G (OFDM24)	Infrastructure ...	15:59:41 8-...
Not Available		6		Yes (W...	N/A ...	54,48,36,24,18,...	00-22-15-0E-7D-...	G (OFDM24)	Infrastructure ...	15:59:44 8-...
Available	eduroam	9		Yes (W...	-82	54,48,36,24,18,...	00-3A-98-40-F3-...	G (OFDM24)	Infrastructure ...	15:59:41 8-...
Available	A9F1BDF1DA...	10		Yes (W...	-85	11,5,2,1 Mb/s	0E-D3-CD-CA-1...	B (DSSS)	Ad Hoc mode	15:59:41 8-...
Available	512U51	11		Yes (W...	-82	54,48,36,24,18,...	90-84-0D-D8-9A-...	N (HT)	Infrastructure ...	15:59:44 8-...
Not Available	512U51 - host	11		Yes (W...	N/A ...	54,48,36,24,18,...	96-84-0D-D8-9A-...	N (HT)	Infrastructure ...	15:59:44 8-...
Available	eduroam	13		Yes (W...	-75	54,48,36,24,18,...	00-14-F2-27-3C-...	G (OFDM24)	Infrastructure ...	15:59:41 8-...
Available	eduroam	13		Yes (W...	-81	54,48,36,24,18,...	00-14-F2-27-37-E0	G (OFDM24)	Infrastructure ...	15:59:44 8-...

Obrázek 18: WirelessMon - Dostupné WiFi sítě

4.1.3 Vistumbler

Vistumbler patří mezi další užitečné freewarové nástroje pro mapování a zobrazení dostupných bezdrátových sítí v okolí počítače. Nabízí skenování v reálném čase, jenž je možné zastavit a výsledky zpracovat.

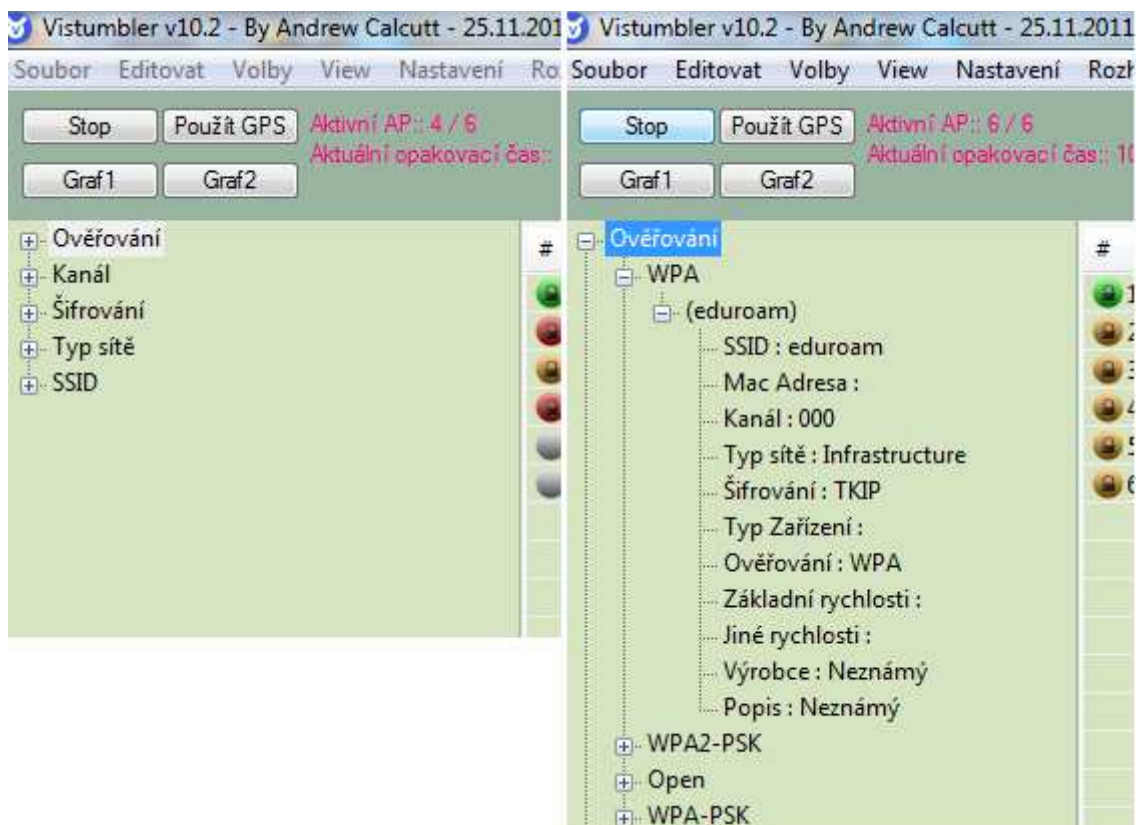
Po zapnutí programu se zobrazí uživatelsky přijatelné prostředí. Nedojde k automatickému skenování WiFi sítí bez vědomí uživatele. Při spuštění detekování sítí v okolí počítače se postupně zobrazují APs a informace o nich. Na obrazovce se vypíše jejich SSID, síla signálu, ověřování a šifrování.

#	Aktivita	Mac A...	SSID	Signál	High Signal	Kanál	Ověřování	Šifrování	Typ sítě
1	Aktivní		eduroam	100%	100%	0	WPA	TKIP	Infrastructure
2	Aktivní		51-616	26%	32%	0	WPA2-PSK	AES	Infrastructure
3	Aktivní		A9F1BDF1DAB1N...	34%	36%	0	Open	WEP	Ad Hoc
4	Aktivní			4%	36%	0	WPA-PSK	TKIP	Infrastructure
5	Aktivní		512U51	34%	40%	0	WPA2-PSK	AES	Infrastructure
6	Neakti...		512U51 - host	0%	42%	0	WPA2-PSK	AES	Infrastructure

Obrázek 19: Vistumbler - Dostupné WiFi sítě

Nevýhodou programu Vistumbler je, že se nedá zjistit použitý kanál a MAC adresa sítě. Mezi pozitiva patří možnost zvolení češtiny, zvuková signalizace nalezení nového AP nebo síly signálu, možnost vyobrazení pouze určitých sloupců a další možnosti nastavení vzhledu prostředí programu.

Software poskytuje i postranní panel filtrování a možnost zobrazení dvou různých grafů síly signálu.



Obrázek 20: Vistumbler – Filtrování

4.1.4 InSSIDer

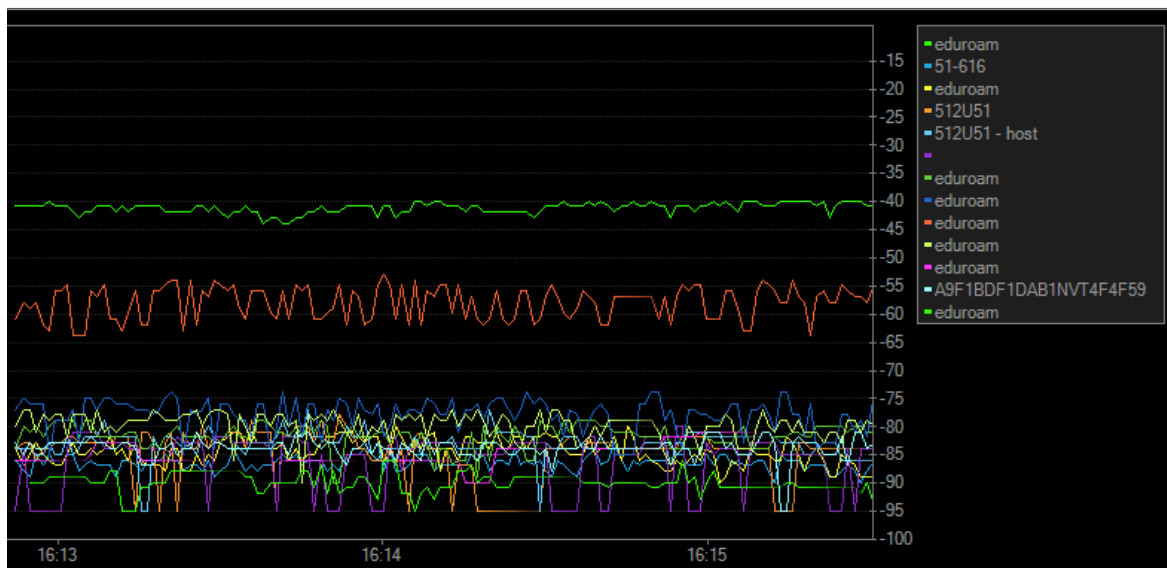
Software inSSIDer patří mezi nejčastěji využívaný program pro detailní vyhledávání dostupných WiFi sítí v okolí počítače. Hned po spuštění program zobrazí základní informace o skenovaných WiFi sítích jako SSID, MAC adresa, RSSI, použitý kanál, typ zařízení, zabezpečení, maximální rychlost, atd. Každá síť má přidělenou barvu, díky které je snadné propojení získaných dat s grafy. Detekování sítí v reálném čase je možné zastavit a výsledky zhodnotit.

✓	MAC Address	SSID	RSSI	Channel	Vendor	Security	Max Rate	Network Type
✓	00:14:F2:27:36:C0	eduroam	-48	1	Cisco Systems	WPA-TKIP	54	Infrastructure
✓	00:1E:7A:A9:38:70	eduroam	-94	1	Cisco Systems	WPA-TKIP	54	Infrastructure
✓	00:14:F2:27:37:A0	eduroam	-82	1	Cisco Systems	WPA-TKIP	54	Infrastructure
✓	00:22:75:E7:1F:E3	51-616	-84	1 + 5	Belkin International, Inc.	WPA2-Personal	300	Infrastructure
✓	00:14:F2:27:36:20	eduroam	-62	5	Cisco Systems	WPA-TKIP	54	Infrastructure
✓	00:22:15:0E:7D:56		-83	6	ASUSTek COMPUTER I...	WPA-Personal	54	Infrastructure
✓	00:3A:98:40:F3:E0	eduroam	-78	9	Cisco Systems	WPA-TKIP	54	Infrastructure
✓	00:3A:98:40:F2:E0	eduroam	-79	9	Cisco Systems	WPA-TKIP	54	Infrastructure
✓	0E:D3:CD:CA:17:17	A9F1BDF1DAB1NVT4...	-85	10		WEP	11	Adhoc
✓	00:1D:7E:4C:59:BB	Kancl	-91	11	Cisco-Linksys, LLC	WPA-Personal	54	Infrastructure
✓	96:84:0D:D8:9A:A3	512U51 - host	-83	11		WPA2-Personal	216	Infrastructure
✓	90:84:0D:D8:9A:A3	512U51	-83	11	Apple, Inc	WPA2-Personal	216	Infrastructure
✓	00:14:F2:27:3C:C0	eduroam	-73	13	Cisco Systems	WPA-TKIP	54	Infrastructure
✓	00:14:F2:27:37:E0	eduroam	-81	13	Cisco Systems	WPA-TKIP	54	Infrastructure

Obrázek 21: InSSIDer – Dostupné WiFi sítě

Prostředí programu je uživatelsky příjemné, barevné vyobrazení dostupných sítí na černém pozadí je pestré a díky tomu umožňuje lehkou manipulaci se softwarem. V horní části programu se nachází filtr, díky kterému budou skenovány pouze sítě s určitým parametrem.

Software inSSIDer vykreslí časový průběh RSSI všech zjištěných WiFi sítí v jednom grafu a graf RSSI s návazností na použitý kanál v pásmu 2,4 GHz a zvláště v pásmu 5 GHz.



Obrázek 22: InSSIDer – Časový graf RSSI



Obrázek 23: InSSIDer – Pásmo 2,4 GHz

4.1.5 NetSurveyor

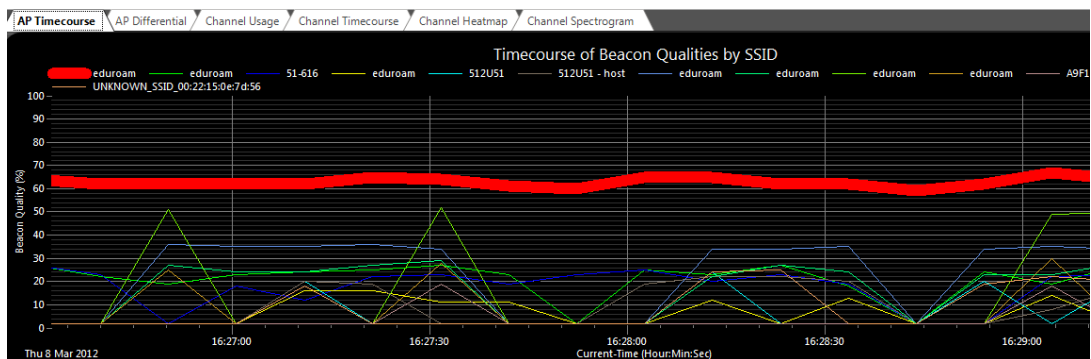
Software NetSurveyor slouží k detekci bezdrátových sítí, jež jsou založeny na standardu 802.11. WiFi APs jsou skenovány v reálném čase, které je možné stopnout a získaná data konvertovat do praktických Portable Document Format (dále jen PDF) formátů. Soubor PDF obsahuje záložku s informacemi o dostupných WiFi sítích - SSID, MAC adresa, kanál, RSSI, a zda je použito zabezpečení – a dále záložky s různými grafy a diagnostickými přehledy. Jedná se o časový průběh síly signálu, zaznamenaný rozdíl mezi

průměrným a aktuálním signálem, dále o přehled a tepelnou mapu použitých kanálů a spektrogram.

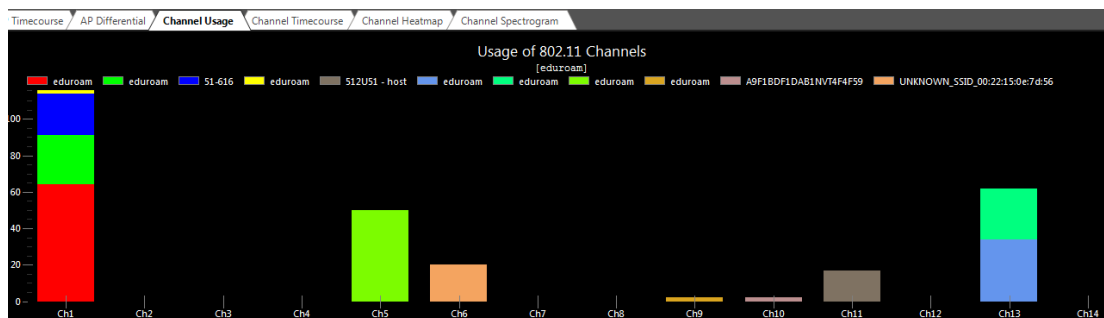
Visible	SSID	BSSID (MAC)	Channel	Beacon...	Beacon Str...	Beacon Q...	Signal Quality	Radio Type
<input checked="" type="checkbox"/>	eduroam	00:14:f2:27:36:c0	1	-50	10	64	Excellent	OFDM24
<input checked="" type="checkbox"/>	eduroam	00:14:f2:27:37:a0	1	-80	,01	27	Low	OFDM24
<input checked="" type="checkbox"/>	51-616	00:22:75:e7:1f:e3	1	-83	,005	23	Very Low	Unknown
<input checked="" type="checkbox"/>	eduroam	00:1e:7a:a9:38:70	1	-100	,0001	2	No Signal	OFDM24
<input checked="" type="checkbox"/>	eduroam	00:14:f2:27:36:20	5	-61	,7943	50	Very Good	OFDM24
<input checked="" type="checkbox"/>	UNKNOWN_SSID...	00:22:15:0e:7d:56	6	-85	,0032	20	Very Low	OFDM24
<input checked="" type="checkbox"/>	eduroam	00:3a:98:40:f3:e0	9	-100	,0001	2	No Signal	OFDM24
<input checked="" type="checkbox"/>	A9F1BDF1DAB1N...	0e:d3:cd:ca:17:17	10	-100	,0001	2	No Signal	Unknown
<input checked="" type="checkbox"/>	512U51	90:84:0d:d8:9a:a3	11	-86	,0025	19	Very Low	Unknown
<input checked="" type="checkbox"/>	512U51 - host	96:84:0d:d8:9a:a3	11	-88	,0016	17	Very Low	Unknown
<input checked="" type="checkbox"/>	eduroam	00:14:f2:27:3c:c0	13	-74	,0398	34	Low	OFDM24
<input checked="" type="checkbox"/>	eduroam	00:14:f2:27:37:e0	13	-79	,0126	28	Low	OFDM24

Obrázek 24: NetSurveyor – Dostupné WiFi sítě

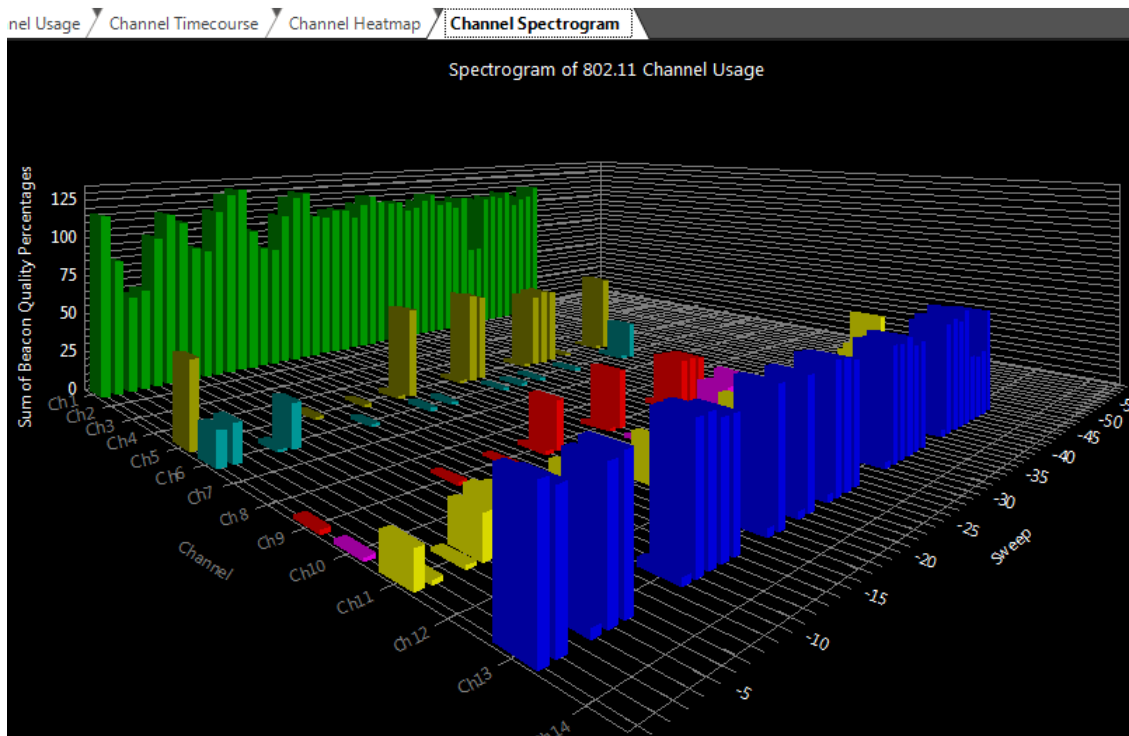
NetSurveyor je nejpřijatelnější program v grafických zobrazeních dostupných WiFi sítí. V získaných datech schází typ použitého zabezpečení. Je viditelné pouze, je-li síť šifrována, což snižuje kvalitu programu.



Obrázek 25: NetSurveyor – Časový průběh kvality signálu



Obrázek 26: NetSurveyor – Použité kanály

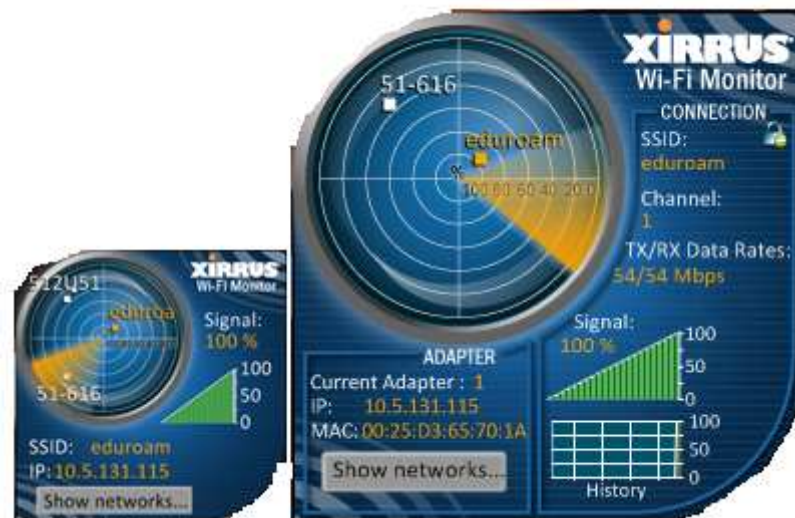


Obrázek 27: NetSurveyor – Spektrogram

Práce se softwarem je velmi snadná, získaná data lze lehce a přehledně zobrazit a barevné prostředí programu patří k jeho velkým přednostem.

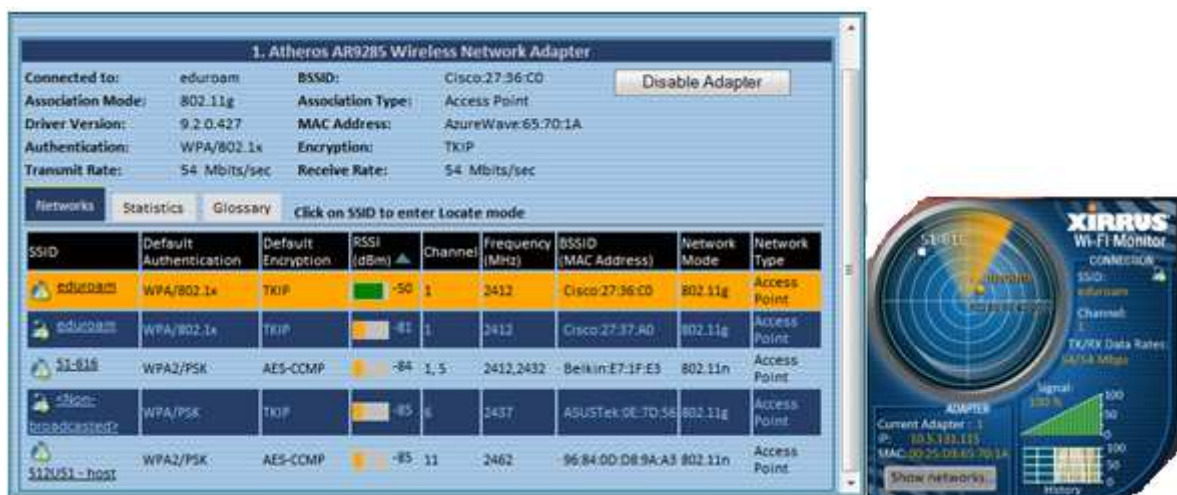
4.1.6 XiRRUS Wi-Fi Monitor

XiRRUS Wi-Fi Monitor je nástroj k nepřetržitému monitorování aktivních dostupných WiFi sítí. Jedná se o miniaplikaci vyobrazenou na ploše počítače, která svým vzhledem připomíná radar. Ve zmenšené verzi poskytuje informace o WiFi síti, ke které jsem právě připojena jako její SSID, kanál, síla signálu a její historii průběhu, dále pak MAC adresu a IP adresu síťového adaptéru.



Obrázek 28: XiRRUS Wi-Fi Monitor – Miniaplikace na ploše

Při rozkliknutí miniaplikace se zobrazí detailnější informace o síťové kartě a dále pak data o dostupných WiFi sítích v okolí počítače – SSID, zabezpečení, šifrování, RSSI v dBm, použitý kanál, frekvence, MAC adresa, režim a typ sítě. Program umožňuje i zvolení jiného síťového adaptéru k měření.



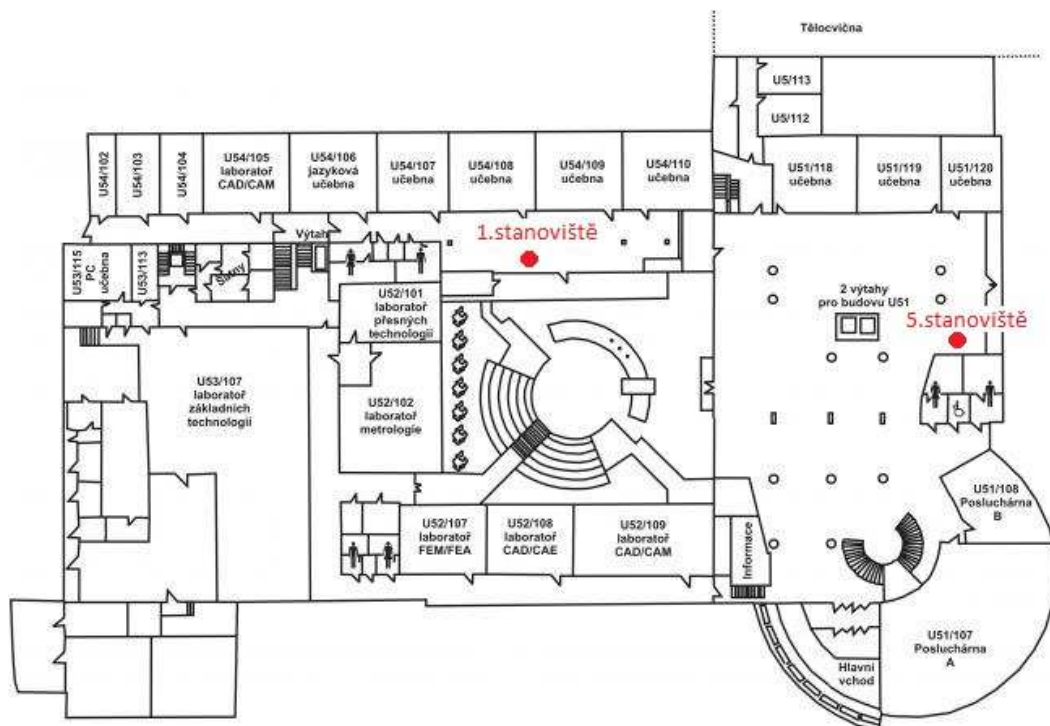
Obrázek 29: XiRRUS Wi-Fi Monitor – Dostupné WiFi sítě

Software neposkytuje žádné grafické vykreslení časových průběhů. Není možné skenování WiFi sítí zastavit a výsledky měření zpracovat v daném čase. V záložce glosář se nachází seznam všech odborných termínů týkajících se bezdrátových sítí a jejich definice.

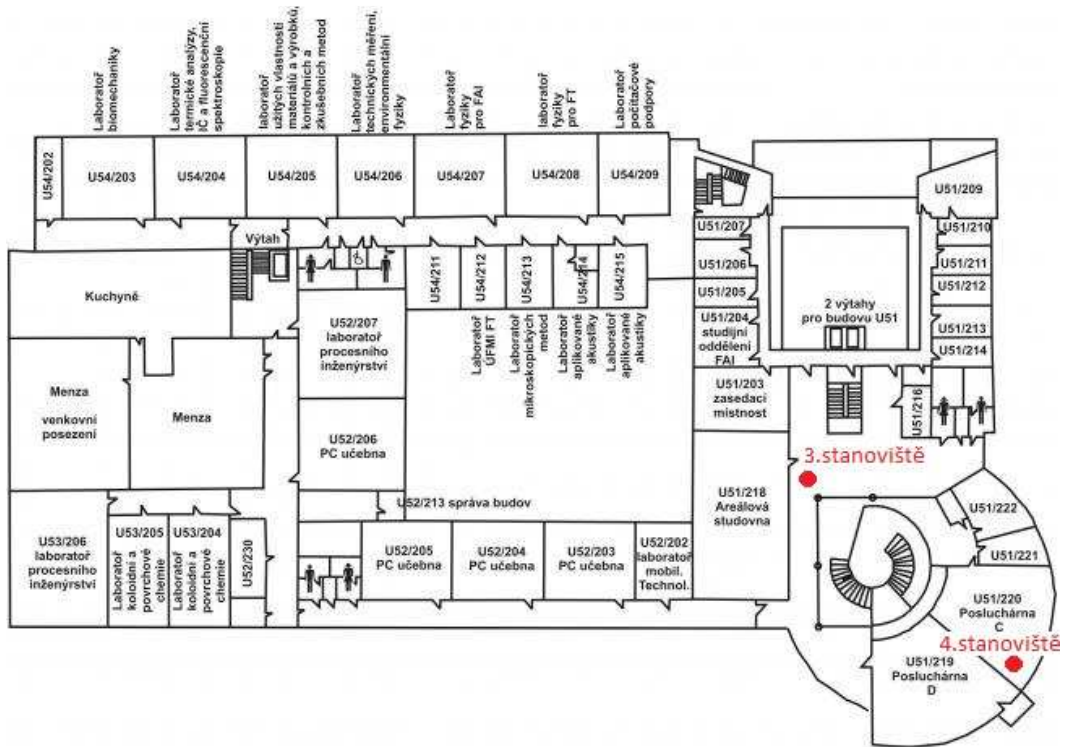
4.2 Metodika měření WiFi sítí jednotlivými softwary na vybraných místech budovy U5

Měření WiFi sítí nainstalovanými programy probíhá ve všední dny v čase 15:30 – 19 hod na budově U5 FAI UTB. Časové rozpětí jsem zvolila z hlediska vyšší pravděpodobnosti připojení většího počtu uživatelů v okolních domácnostech.

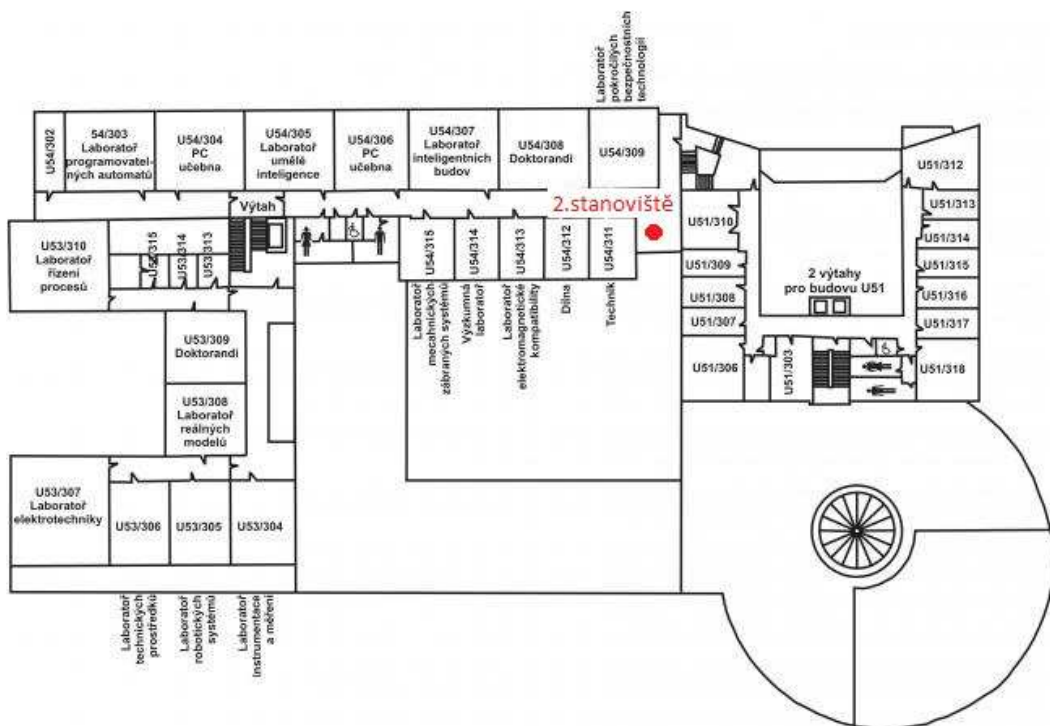
Místní WiFi síť s názvem eduroam má na budově U5 FAI UTB několik APs se svými specifickými MAC adresami, ke kterým se dá připojit pouze v určitých místech budovy. Při mapování WiFi sítí dochází k neustálému přemostování mého uživatelského účtu mezi jednotlivými APs sítě eduroam, jenž probíhá na základě získání lepší kvality signálu od jiného AP. K rušení WiFi sítě dochází taktéž díky výskytu více sítí na jednom kanále o stejné frekvenci.



Obrázek 30: Body měření v prvním patře budovy U5 FAI UTB [21]



Obrázek 31: Body měření v druhém patře budovy U5 FAI UTB [21]



Obrázek 32: Body měření ve třetím patře budovy U5 FAI UTB [21]

4.2.1 Zhodnocení výsledků z měřených stanovišť

Stanoviště prvního měření jsem zvolila v přízemí budovy U5 FAI UTB před učebnou U54/108, kde se nacházejí stoly a studenti se zde pravidelně připojují k Internetu na svém počítači. Výsledky ze všech měření nainstalovanými softwary jsem vkládala do sešitu Excel, který je první přílohou diplomové práce. Ke každému stanovišti uvádím souhrnnou tabulku, jež se zaměřuje na počet detekovaných sítí a typy použitého zabezpečení.

Na prvním stanovišti dle softwaru NetSurveyor jsem připojena k WiFi síti eduroam s MAC adresou 00:14:f2:27:3c:c0 a vynikající kvalitou signálu 61%, jež používá kanál 13.

Počet sítí	Šifrování
5 (3x eduroam)	Ano (4)
	Žádné (1)

Tabulka 3: NetSurveyor – První stanoviště

Program inSSIDer detekuje stejně jako program NetSurveyor pět WiFi sítí. NetSurveyor zachytává tři sítě eduroam a inSSIDer čtyři. Jinak podávají stejné výsledky měření s tím rozdílem, že inSSIDer poskytuje informace o použitém typu zařízení (Cisco Systems) a dále o zabezpečení. Místní síť eduroam používá WPA protokol se šifrovacím klíčem TKIP.

Počet sítí	Zabezpečení	
	Typ	Počet sítí
5 (4x eduroam)	WPA-TKIP	4
	WPA-Personal	1

Tabulka 4: InSSIDer – První stanoviště

Program Vistumbler na žádném ze stanovišť nedetekuje více sítí eduroam a to z toho důvodu, že nepodporuje zobrazení MAC adresy. Nedokáže jednotlivé WiFi APs sítě eduroam od sebe odlišit. Zachytává o jednu WiFi síť navíc oproti předešlým softwarům. Jde o síť s SSID 51-616, jejíž současný signál je nulový a je zabezpečena WPA2 protokolem a blokovou šifrou AES.

Počet sítí	Ověřování (šifrování)	
	Typ	Počet
4 (1x eduroam)	WPA (TKIP)	2
	WPA2-PSK (AES)	1
	Žádné (žádné)	1

Tabulka 5: Vistumbler – První stanoviště

Software WirelessMon zobrazuje stejné dostupné WiFi sítě v okolí počítače jako program inSSIDer, pouze zachytává o jednu síť eduroam méně. O WiFi síti eduroam, ke které jsem stále připojena, zjišťuji další informaci a to její maximální RSSI (-40 dBm) a standard dle IEEE (IEEE 802.11g).

Počet sítí	Zabezpečení	
	Typ	Počet sítí
4 (3x eduroam)	WPA-TKIP	4

Tabulka 6: WirelessMon – První stanoviště

Software XiRRUS Wi-Fi Monitor detekuje stejný počet sítí jako program WirelessMon a to i se stejnými výsledky. Vyobrazuje navíc použití autentizace 802.1x, což znamená, že umožňuje kvalitnější přihlašování uživatelů. O síti eduroam zjišťuji poslední dostupnou informaci a to střední frekvenční kmitočet, který je 2472 MHz.

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
4 (3x eduroam)	WPA/802.1x (TKIP)	3
	WPA/PSK (TKIP)	1

Tabulka 7: XiRRUS Wi-Fi Monitor – První stanoviště

Druhé stanoviště jsem volila ve třetím patře budovy U5 FAI UTB. Využila jsem k měření prostor se stoly u učebny U54/309. Připojila jsem se k AP místní síti eduroam s MAC adresou 00:14:f2:27:37:a0, jenž používá kanál 1. Kvalita signálu dle softwaru NetSurveyor je velmi dobrá (48%) a hodnota středního kmitočtu je 2412 MHz.

Počet sítí	Šifrování
9 (7x eduroam)	Ano (8)
	Žádné (1)

Tabulka 8: NetSurveyor – Druhé stanoviště

Počet sítí	Zabezpečení	
	Typ	Počet sítí
8 (6x eduroam)	WPA-TKIP	6
	WPA2-Personal	1
	Žádné	1

Tabulka 9: InSSIDer – Druhé stanoviště

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
3 (1x eduroam)	WPA (TKIP)	1
	WPA2-PSK (TKIP)	1
	Žádné (žádné)	1

Tabulka 10: Vistumbler – Druhé stanoviště

Počet sítí	Zabezpečení	
	Typ	Počet sítí
6 (4x eduroam)	WPA-TKIP	4
	WPA2	1
	žádné	1

Tabulka 11: WirelessMon – Druhé stanoviště

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
3 (1x eduroam)	WPA/802.1x (TKIP)	1
	WPA2/PSK (TKIP)	1
	Žádné (žádné)	1

Tabulka 12: XiRRUS Wi-Fi Monitor – Druhé stanoviště

Třetí měření probíhalo v druhém patře U51 u počítačové učebny, kde se studenti nejčastěji připojují k WiFi síti eduroam, proto by zde kvalita signálu měla být excelentní a nemělo by docházet k rušení. Zde jsem se připojila k místní síti eduroam s MAC adresou 00:14:f2:27:36:c0, jejíž kvalita signálu je velmi nízká a to pouhých 22%. WiFi síť využívá k šíření signálu kanál 1.

U počítačové učebny byla detekována i Ad-hoc síť vysílající své SSID A9F1BDF1DAB1NVT4F4F59 s MAC adresou 0e:d3:cd:ca:17:17. Síť je nakonfigurována na prázdném kanálu 10, zabezpečena protokolem WEP a její signál 48% dle softwaru NetSurveyor je velmi dobrý. Typ WiFi sítě využívá standard IEEE 802.11b. Zařízení, jenž sestavilo WiFi síť, je pro softwaru neznámé. Tato síť je zachycena všemi softwary s výjimkou programu XiRRUS Wi-Fi Monitor.

Počet sítí	Šifrování
11 (7x eduroam)	Ano (11)
	Žádné (0)

Tabulka 13: NetSurveyor – Třetí stanoviště

Počet sítí	Zabezpečení	
	Typ	Počet sítí
10 (7x eduroam)	WPA-TKIP	7
	WPA2-Personal	1
	WPA-Personal	1
	WEP	1

Tabulka 14: InSSIDer – Třetí stanoviště

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
7 (1x eduroam)	WPA (TKIP)	2
	WPA2-PSK (AES)	4
	Žádné (WEP)	1

Tabulka 15: Vistumbler – Třetí stanoviště

Počet sítí	Zabezpečení	
	Typ	Počet sítí
9 (6x eduroam)	WPA-TKIP	7
	WPA2	1
	WEP	1

Tabulka 16: WirelessMon – Třetí stanoviště

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
1 (1x eduroam)	WPA/802.1x (TKIP)	1

Tabulka 17: XiRRUS Wi-Fi Monitor – Třetí stanoviště

Ke čtvrtému měření jsem využila přednáškovou místnost U51/220, která se nachází ve druhém patře budovy U5 FAI UTB. V učebně bylo zachyceno nejméně WiFi sítí. Připojila jsem k místní síti eduroam s MAC adresou 00:14:f2:27:36:20. Síť využívá ke komunikaci kanál 5 se středním kmitočtem 2432 MHz, ale signál WiFi sítě byl velmi nízký. Při měření předposledním programem WirelessMon a i následným XiRRUS Wi-Fi Monitor došlo k přemostění na síť eduroam s MAC adresou 00:3A:98:40:F2:50. Je nakonfigurována na kanálu 9 a frekvence středního kmitočtu je 2452 MHz.

Počet sítí	Šifrování
3 (2x eduroam)	Ano (3)
	Žádné (0)

Tabulka 18: NetSurveyor – Čtvrté stanoviště

Počet sítí	Zabezpečení	
	Typ	Počet sítí
5 (2x eduroam)	WPA-TKIP	2
	WPA2-Personal	1
	WPA-Personal	1
	WEP	1

Tabulka 19: InSSIDer – Čtvrté stanoviště

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
4 (1x eduroam)	WPA (TKIP)	2
	WPA2-PSK (AES)	1
	Žádné (WEP)	1

Tabulka 20: Vistumbler – Čtvrté stanoviště

Počet sítí	Zabezpečení	
	Typ	Počet sítí
3 (1x eduroam)	WPA-TKIP	1
	WPA2	1
	WEP	1

Tabulka 21: WirelessMon – Čtvrté stanoviště

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
6 (2x eduroam)	WPA/802.1x (TKIP)	2
	WPA2/PSK (AES-CCMP)	1
	WPA/PSK (TKIP)	2
	Žádné (WEP)	1

Tabulka 22: XiRRUS Wi-Fi Monitor – Čtvrté stanoviště

Posledním pátým stanovištěm měření jsou stoly u kopírovacího zařízení v hale U51. Zde byl detekován největší počet sítí. Při měření prvními dvěma programy (NetSurveyor, inSSIDer) jsem byla připojena k WiFi síti eduroam s MAC adresou 00:14:f2:27:36:c0. Kvalita signálu dle softwaru NetSurveyor byla vynikající s hodnotou 64% a síť využívala kanál 1. WiFi síť ale byla na stanovišti měření nestálá a došlo k přepojení na jiný WiFi AP. Jde o síť eduroam s MAC adresou 00:14:F2:27:37:A0 běžící taktéž na kanálu 1.

Na stanovišti byla zachycena síť nevysílající své SSID, ale ostatní informace byly viditelné. Její MAC adresa je 00:22:15:0e:7d:56. WiFi síť využívá ke komunikaci kanál 6 se středním kmitočtem 2437 MHz. Kvalita signálu neznámé sítě je 20%, tzn. velmi nízká.

Síť je zabezpečena protokolem WPA a šifrovacími klíči TKIP. Zařízení AP je ASUSTek COMPUTER. Jedná se infrastrukturní síť využívající standard IEEE 802.11g.

Počet sítí	Šifrování
12 (7x eduroam)	Ano (12)
	Žádné (0)

Tabulka 23: NetSurveyor – Páté stanoviště

Počet sítí	Zabezpečení	
	Typ	Počet sítí
14 (8x eduroam)	WPA-TKIP	9
	WPA2-Personal	4
	WEP	1

Tabulka 24: InSSIDer – Páté stanoviště

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
6 (1x eduroam)	WPA (TKIP)	2
	WPA2-PSK (AES)	3
	Žádné (WEP)	1

Tabulka 25: Vistumbler – Páté stanoviště

Počet sítí	Zabezpečení	
	Typ	Počet sítí
11 (6x eduroam)	WPA-TKIP	7
	WPA2	3
	WEP	1

Tabulka 26: WirelessMon – Páté stanoviště

Počet sítí	Ověřování (šifrování)	
	Typ	Počet sítí
5 (2x eduroam)	WPA/802.1x (TKIP)	2
	WPA2/PSK (AES-CCMP)	2
	WPA/PSK (TKIP)	1

Tabulka 27: XiRRUS Wi-Fi Monitor – Páté stanoviště

5 SPEKTRÁLNÍ ANALYZÁTOR WI-SPY 2.4I

Spektrální analyzátor Wi-Spy 2.4i je cenově nejpřijatelnější software pro každého síťáře. Základní model, jenž lze pořídit do 2 500,-, je ideální volba pro mapování WiFi sítí v okolí počítače.

Výrobce Wi-Spy je společnost MetaGeek a i freewareového softwaru inSSIDer, který je využit k detekování sítí na budově U5 FAI UTB. MetaGeek dodává na trh různé typy spektrálních analyzátorů pro frekvenční pásma 900 MHz, 2,4 GHz, 5 GHz a speciální příslušenství k nim jako antény, zesilovače. Cena spektrálního analyzátoru s Universal Serial Bus (dále jen USB) rozhraním pro pásma 2,4 GHz a zároveň i pro 5 GHz se pohybuje kolem 14 000,-. Top model Wi-Spy DBX by byl ideální volbou pro skenování WiFi a GSM sítí v dosti zarušených místech jako sídliště, centra měst, budovy s kancelářskými prostory, obchodní komplexy, atd.

Wi-Spy 2.4i je k dostání s USB rozhraním, díky kterému je možné ho pohodlně připojit k počítači. Je vyvinut pro vyhledání volného frekvenčního pásma, k odstranění problémů s WiFi sítěmi a umožňuje práci v reálném čase, ale i ze záznamu. Zachytává veškerou bezdrátovou aktivitu jako WiFi sítě, bluetooth, bezdrátové telefony, mikrovlnné trouby a jiná zařízení pracující ve frekvenčním pásmu 2,4 GHz.



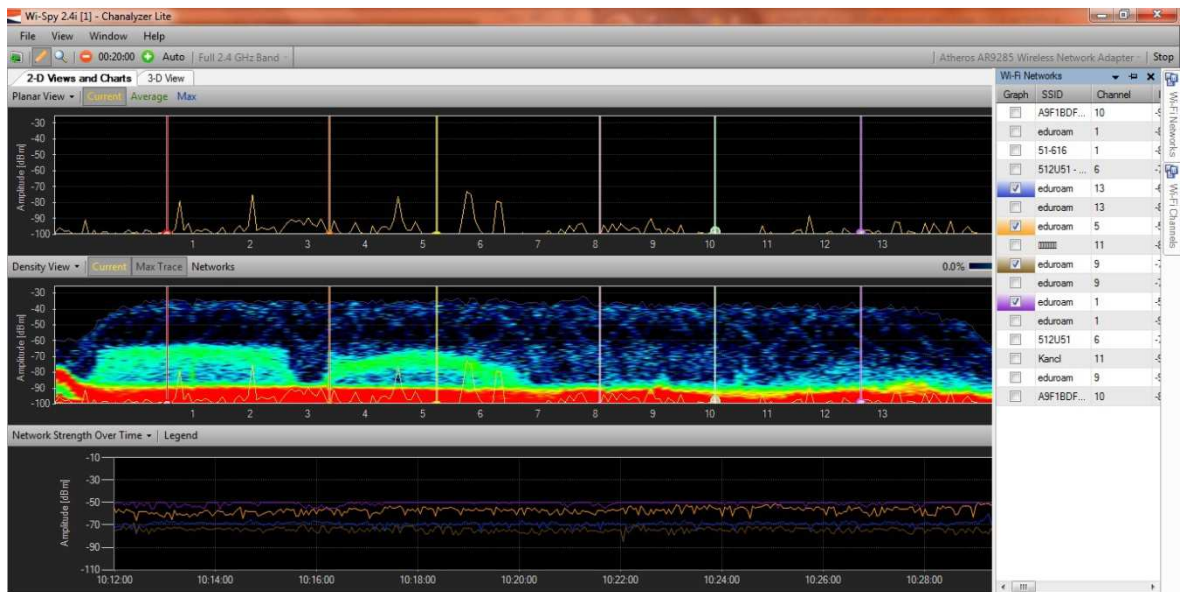
Obrázek 33: Wi-Spy 2.4i

Pro práci se spektrálním analyzátozem Wi-Spy 2.4i jsem musela doinstalovat software Chanalyzer Lite, jehož fungování je podmíněno přítomností Wi-Spy v počítači přes USB. Po spuštění programu dojde k mapování WiFi sítí a vypsání dostupných informací na pravou část obrazovky. Jedná o data jako SSID, použitý kanál, RSSI a grafické zobrazení jeho síly, čas prvního detekování sítě, typ zařízení, zabezpečení, MAC adresa, maximální rychlost a typ sítě.

Graph	SSID	Channel	RSSI	Time	Vendor	Privacy	MAC Address
<input type="checkbox"/>	A9F1BDF...	10	-98	09:39:07		WEP	a2:5e:2a:9d:d
<input type="checkbox"/>	eduroam	1	-83	10:10:55	Cisco Syst...	WPA-TKIP	00:14:f2:27:37
<input type="checkbox"/>	51-616	1	-82	10:10:55	Belkin Int...	RSNA-CC...	00:22:75:e7:1f
<input type="checkbox"/>	512U51 - ...	6	-76	10:10:55		RSNA-CC...	96:84:0d:d8:9
<input checked="" type="checkbox"/>	eduroam	13	-72	10:10:55	Cisco Syst...	WPA-TKIP	00:14:f2:27:3c
<input type="checkbox"/>	eduroam	13	-82	10:10:55	Cisco Syst...	WPA-TKIP	00:14:f2:27:37
<input checked="" type="checkbox"/>	eduroam	5	-54	10:10:55	Cisco Syst...	WPA-TKIP	00:14:f2:27:36
<input type="checkbox"/>		6	-78	10:10:55	ASUSTek...	WPA-TKIP	00:22:15:0e:7
<input checked="" type="checkbox"/>	eduroam	9	-74	10:10:55		WPA-TKIP	00:3a:98:40:f2
<input type="checkbox"/>	eduroam	9	-76	10:10:49		WPA-TKIP	00:3a:98:40:f2
<input checked="" type="checkbox"/>	eduroam	1	-50	10:10:55	Cisco Syst...	WPA-TKIP	00:14:f2:27:36
<input type="checkbox"/>	eduroam	1	-92	10:10:55	Cisco Syst...	WPA-TKIP	00:1e:7a:a9:3
<input type="checkbox"/>	512U51	6	-98	10:10:55		RSNA-CC...	90:84:0d:d8:9
<input type="checkbox"/>	Kancl	11	-91	10:06:52	Cisco-Link...	WPA-TKIP	00:1d:7e:4c:5
<input type="checkbox"/>	eduroam	9	-91	09:18:51		WPA-TKIP	00:3a:98:40:f2
<input type="checkbox"/>	A9F1BDF...	10	-82	10:09:40		WEP	82:5e:3c:f2:81

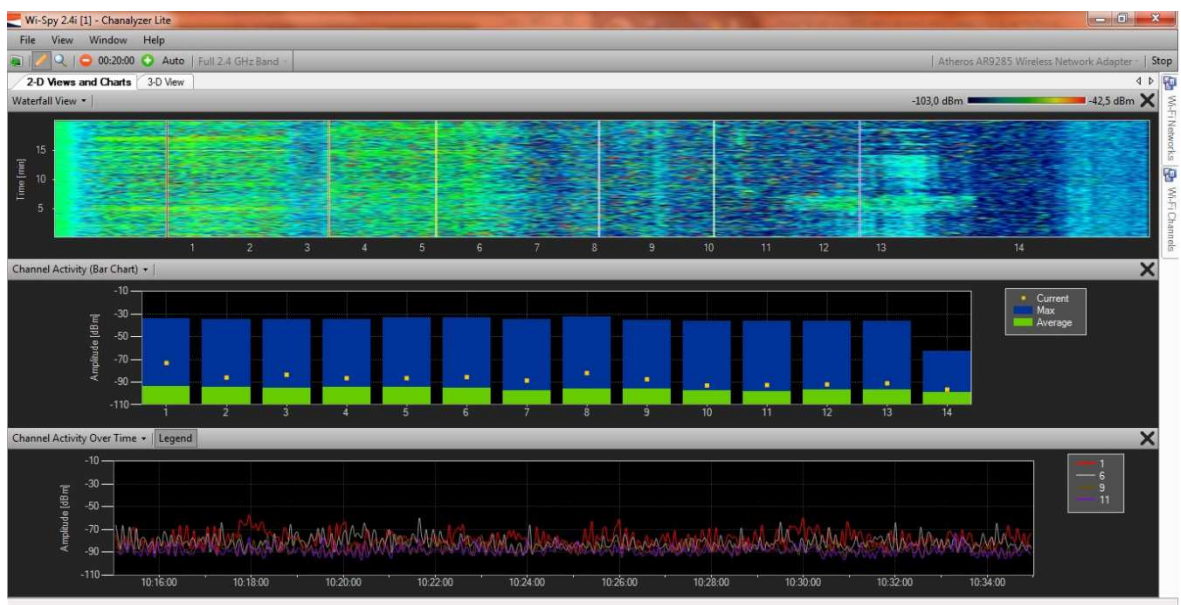
Obrázek 34: Wi-Spy 2.4i – Dostupné WiFi sítě

Umožňuje zobrazení až čtyř ze šesti dostupných 2D grafů v jednom okně obrazovky. Je možné vykreslit jenom mnou zvolené sítě. U vykreslení hodnoty amplitudy se nachází záložky průměrné, aktuální anebo maximální, což umožňuje zrušení či zobrazení daných hodnot. Graf hustoty zobrazuje zarušení na jednotlivých kanálech. Posledním vyobrazením je síla signálu WiFi sítě v reálném čase.



Obrázek 35: Wi-Spy 2.4i – Grafické vyobrazení I

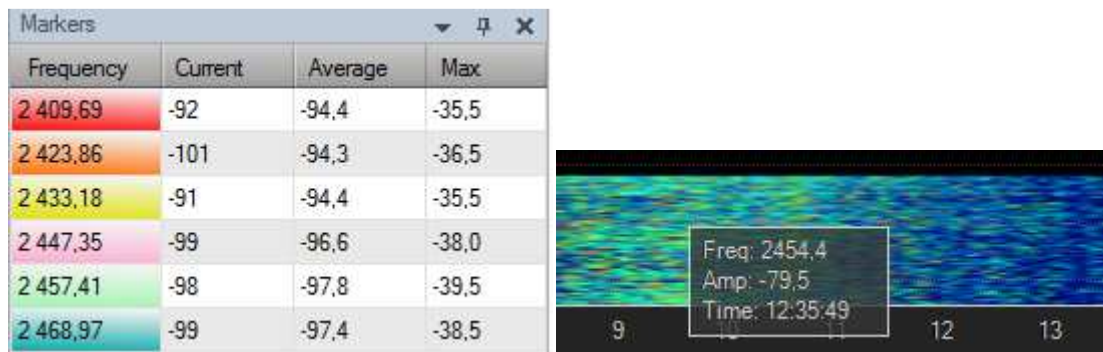
Dalšími typy grafů jsou nastalé změny amplitudy frekvence v čase, aktivita WiFi sítí na daných kanálech (průměrná, maximální a aktuální hodnota) a aktivita kanálu v reálném čase.



Obrázek 36: Wi-Spy 2.4i – Grafické vyobrazení II

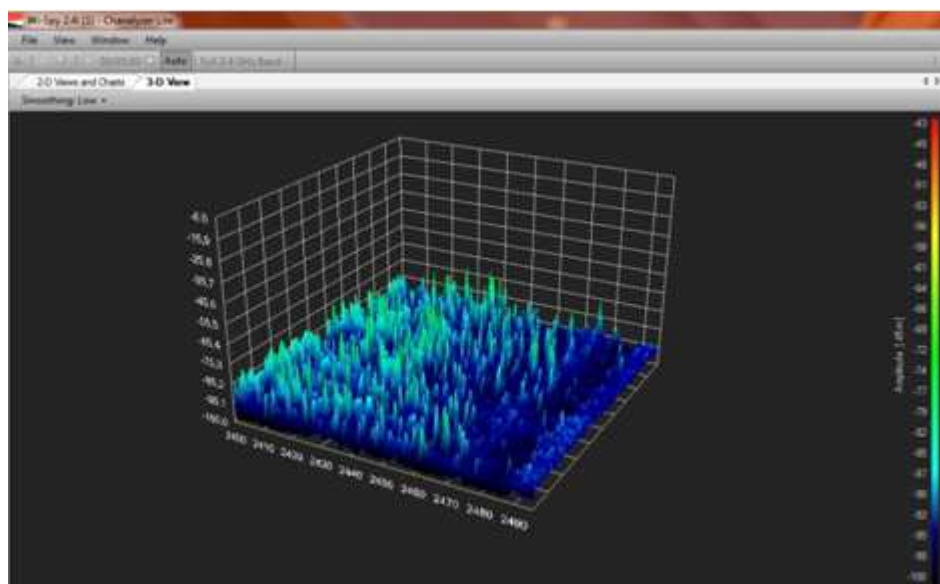
V levém horním rohu softwaru se nachází funkce „Marker“ a „Inspector“. Při procházení jednotlivých grafů s aktivní funkcí „Inspector“ se zobrazují aktuální hodnoty v daných

místech (např. frekvence, amplituda, čas, atd.). Naopak úloha „Marker“ umožňuje v grafech označovat určitá místa, frekvence, o kterých chci získat bližší informace. Data se zaznamenávají a vypíší se do speciální tabulky, kterou lze zobrazit. Je viditelná současná frekvence a k ní odpovídající průměrná, aktuální a maximální amplituda.



Obrázek 37: Wi-Spy 2.4i – Tabulka „Markers“ a funkce „Inspector“

V zobrazení 3D se vykreslují jednotlivé frekvence v závislosti na čase. Na pravé straně programu se nachází škála barevného provedení, a tak je možné lépe zjistit, kde je hodnota amplitudy frekvence nejvyšší. Amplitudy frekvence na stanovišti měření jsou téměř ve stejném barevném provedení, což napovídá, že WiFi síť, ke které jsem právě připojena, nepřináší silnější signál než okolní WiFi APs. Dochází k přemostování mého uživatelského účtu.



Obrázek 38: Wi-Spy 2.4i - 3D pohled

Výsledky z místa měření jsou verifikovány pomocí spektrálního analyzátoru Wi-Spy 2.4i a jsou zobrazeny v grafech. Mnoho WiFi AP běží na totožném kanálu, a tak je způsobeno jeho vysoké zarušení. Amplituda signálu se pohybuje ve velkém rozmezí, což snižuje kvalitu přijímaného signálu a způsobuje neustálé rušení.

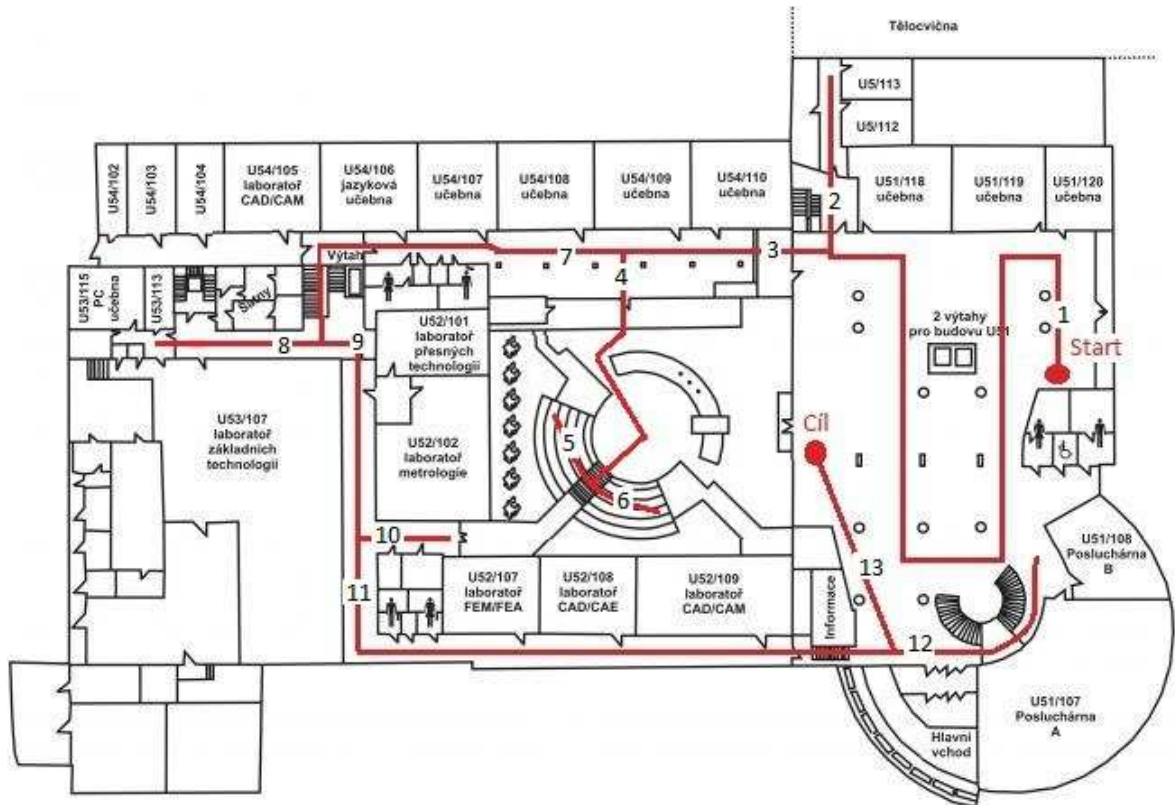
6 DETAILNÍ MAPOVÁNÍ WIFI SÍTĚ EDUROAM NA BUDOVĚ U5 PROGRAMEM INSSIDER

K mapování WiFi sítí byl využit software inSSIDer a metoda warstrolling neboli detekování sítí za chůze. Warstrolling patří mezi tzv. „War“ činnosti. Jedná se o metody hledání sítí, kterých existuje celá řada, např. wardriving (za jízdy v autě), warboating (za jízdy na lodi), warflying (za letu). [22]

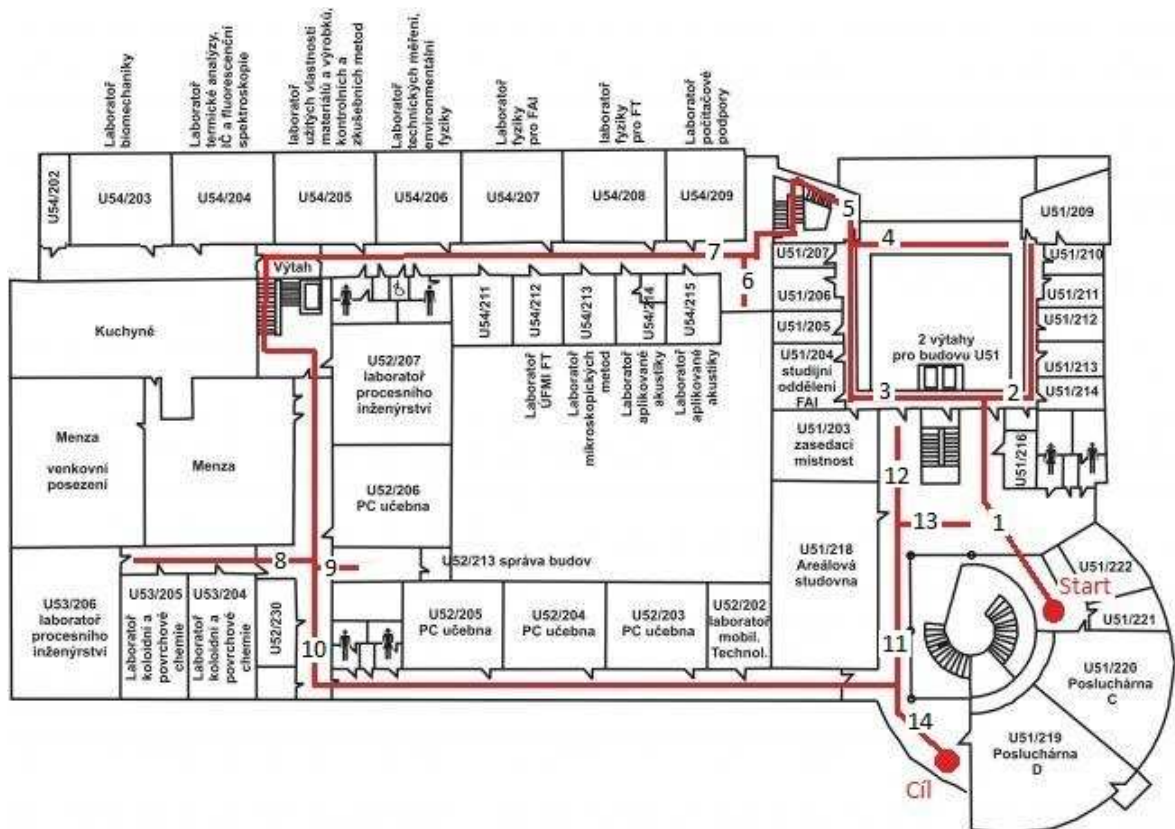
6.1 Metodika měření dat

Měření WiFi sítí na budově U5 FAI UTB jsem prováděla ve všední dny v odpoledním čase od 14 do 19 hod. Budovu U5 jsem rozdělila na čtyři základní etapy měření. Jedná se o 1., 2. a 3. podlaží a samostatně patra 8. - 4. v části budovy U51. Úseky byly členěny ještě na kratší části, a to z důvodu lepší orientace na plánu a řadou odboček z hlavní trasy. WiFi sítě byly celkem detekovány na 318 bodech. Stanoviště měření byly od sebe na trase vzdáleny v rozmezí od 1,5 do 3 metrů.

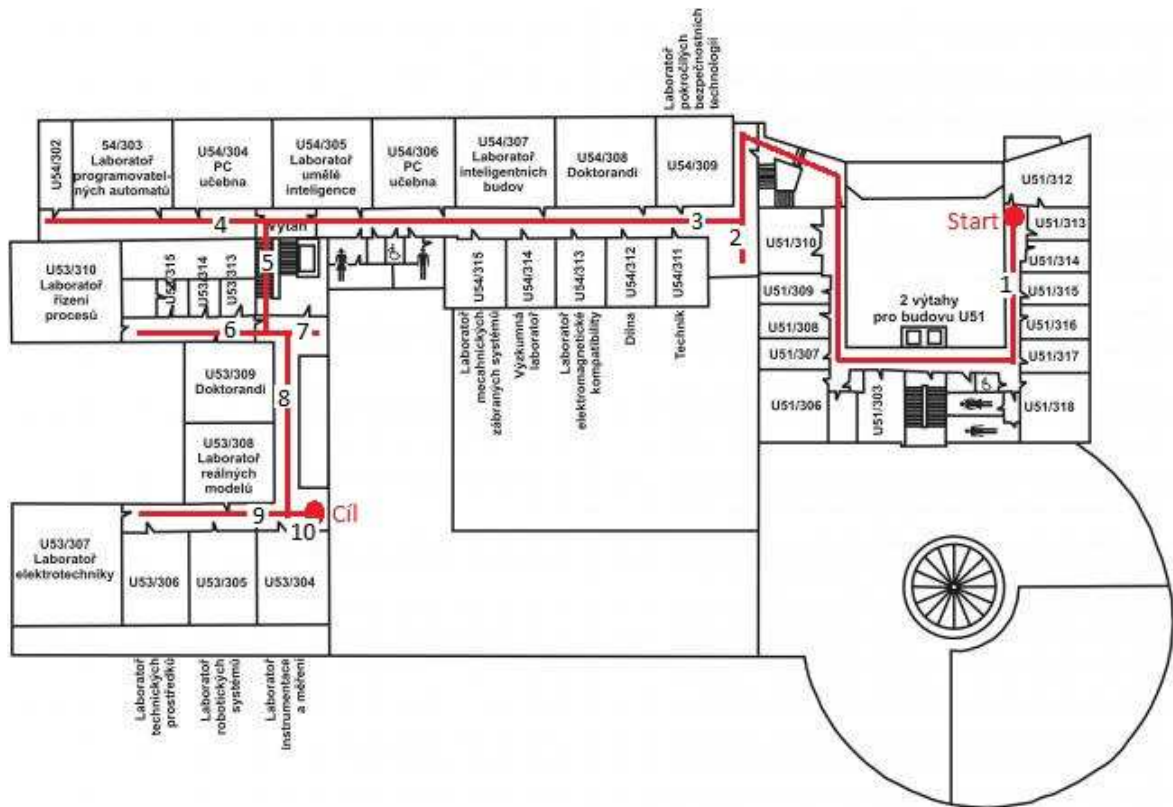
V softwaru inSSIDer jsem zahájila mapování dostupných WiFi sítí v okolí počítače tlačítkem „Start“. Hledání sítí na stanovištích trvalo 10 sekund, poté bylo detekování zastaveno tlačítkem „Stop“ a všechny podrobné výsledky byly vloženy do sešitu Excel, jenž je druhou přílohou diplomové práce.



Obrázek 39: Trasa měření v prvním patře budovy U5 FAI UTB [21]



Obrázek 40: Trasa měření v druhém patře budovy U5 FAI UTB [21]



Obrázek 41: Trasa měření ve třetím patře budovy U5 FAI UTB [21]

6.2 Sumarizace a zhodnocení získaných dat

Při průzkumu zabezpečení WiFi sítí na chodbách budovy U5 FAI UTB bylo celkem zachyceno 22 sítí včetně školní sítě eduroam na 318 stanovištích. Byly detekovány WiFi APs, které jsou většinou nainstalovány v kancelářích či laboratořích na budově U5 a cizí APs vyskytující se v okolí, jejichž výkon pokrývá měřený prostor. Bylo zjištěno, že školní místní síť eduroam má 12 WiFi APs s různými MAC adresami, jež vysílají na různých kanálech (1, 5, 9, 13).

O detekovaných sítích poskytuje software inSSIDer potřebná data jako MAC adresa, SSID, RSSI, kanál a zabezpečení a méně podstatné informace jako zařízení, maximální rychlost a typ sítě.

Během měření jsem celkově připojena k 11 WiFi APs sítě eduroam. Přemostování probíhá automaticky, většinou na základě získání lepšího signálu z jiného AP. Na budově U5 existují i místa, kde školní síť eduroam nebyla vůbec detekována. Jedná se konkrétně o šest stanovišť osmého úseku na první trase měření (část budovy - U52 směrem k rozvodně). V celém prvním patře U52 je kvalita signálu školní sítě velmi nízká. Většinou zde nejsem

připojena k žádné síti (38 stanovišť). Na budově U5 je ještě dalších jedenáct bodů, kde jsem se nemohla připojit k žádné síti:

- 40. - 41. stanoviště, 45. stanoviště: venkovní atrium,
- 173. - 174. stanoviště u správy budov,
- 245. - 246. stanoviště u učebny U53/310,
- 293. - 294. stanoviště v mezipatře mezi 5. a 6. patrem
- 307. - 308. stanoviště ve 4. patře úplně vlevo.

Na mnohých bodech měření byla zjištěna nestálost signálu a s tím souvisí omezený přístup neboli nemožnost připojení na Internet (hodnota RSSI od -80 až do -95 dBm). Jde celkem o 53 stanovišť. Místa se nachází:

- na úseku směrem k tělocvičně,
- na místech venkovního atria,
- na schodech a v mezipatrech,
- u vstupu do haly U51: za informacemi, za schody, u přednáškové místnosti U51/107.

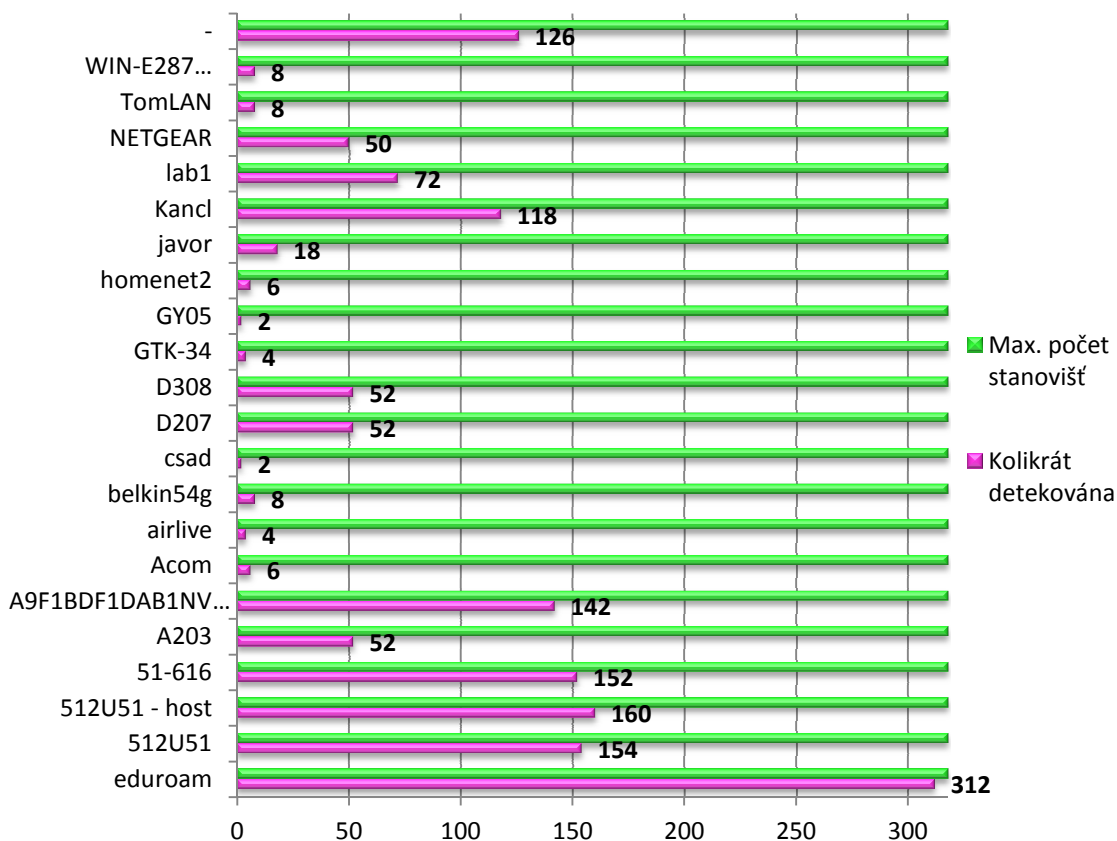
Ve 2. patře U54 a ve 4. patře U51 zleva je signál hodně nestálý.

Signál WiFi sítí eduroam je nejsilnější u AP. Hodnota RSSI se zde pohybuje kolem hodnoty -45 dBm. FAI UTB má logem označené místa, které jsou nejvhodnější k připojení studentů k WiFi síti. Nachází se v hale U51, před počítačovou učebnou, u učebny U53/307, v osmém patře U51, atd. Kvalita signálu na určených místech je dostačující (hodnota RSSI je okolo -60 dBm).

Soukromé WiFi sítě, jež byly zachyceny na blízkých stanovištích na trase, se ve větší míře vyskytovaly pouze kolem cílového místa (kancelář, laboratoř) a jejich signál byl velmi nízký až nulový. RSSI se pohybuje v rozmezí od -80 až do -95 dBm. Byly detekovány softwarem maximálně 10krát. WiFi sítě, zaznamenané 50krát a více, se vyskytovaly převážně ve vstupní hale U51 a na patrech.

SSID WiFi síť	Zabezpečení	Kolikrát byla zachycena
eduroam	WPA-TKIP	312
512U51	WPA2	154
512U51 - host	WPA2	160
51-616	WPA2	152
A203	WPA	52
A9F1BDF1DAB1NVT4F4F59	WEP	142
Acom	WPA	6
airlive	WEP	4
belkin54g	WEP	8
csad	WEP	2
D207	WPA	52
D308	WPA2	52
GTK-34	WEP	4
GY05	WEP	2
homenet2	WPA2	6
javor	WPA2	18
Kancl	WPA	118
lab1	WPA	72
NETGEAR	-	50
TomLAN	WPA2	8
WIN-E287...	WPA2	8
-	WPA	126

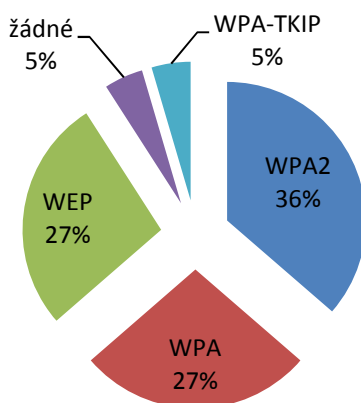
Tabulka 28: Zachycené WiFi sítě



Obrázek 42: Graf zachycených WiFi sítí

Téměř všechny zachycené WiFi APs jsou zabezpečeny jedním z bezpečnostních protokolů, kromě sítě NETGEAR (5%), která nepoužívá žádný typ šifrování a na některých měřeních stanovištích má signál postačující k připojení.

Zabezpečení WiFi sítí



Obrázek 43: Graf zabezpečení WiFi sítí

Protokol WEP, jímž je zabezpečeno šest WiFi sítí (27%), je stejně využíván jako WPA protokol (27%), i když byly v minulosti již oba prolomeny. WEP lze překonat za necelých šest minut. Na základě prolomení WPA byl vyvinut bezpečnostní protokol WPA2, který poskytuje kvalitnější zabezpečení WiFi sítí. Při měření bylo zjištěno, že protokol WPA2 je využíván v osmi WiFi sítích (36%).

Školní síť eduroam jako jediná (5%) využívá zabezpečení WPA-TKIP, což znamená zajištění bezpečnostním protokolem WPA s použitím šifrovacích klíčů TKIP, jenž jsou známy jen připojícím se klientským stanicím.

ZÁVĚR

V diplomové práci byla objasněna problematika WiFi sítí, které spadají do kategorie bezdrátových WLAN sítí. Technologie WiFi sítí je standardizována normou IEEE 802.11 a k přenosu elektromagnetického signálu využívá pásmo 2,4 GHz, jenž v sobě zahrnuje maximálně 14 kanálů s odlišným středním kmitočtem. Signál WiFi sítě se nejčastěji šíří ve vnitřním lokálním prostředí, ale není vyloučen i přenos dat ve vnějším prostoru za praktickování všesměrovým, sektorovým či směrovým antén a to do vzdálenosti až 30 kilometrů. Zde je potřeba přímé vizuální a rádiové viditelnosti.

Důležitou částí diplomové práce bylo zabezpečení WiFi sítí. Uživatelé, aby chránili svá tajná data před potencionálními pachateli, musí mít na svém počítači aktivní firewall. Dále je nutné blokovat vysílání SSID do prostoru a s tím souvisí i správné zvolení antény pokrývající jen požadovaný prostor. Nedílnou součástí zabezpečení je autentizace a šifrování. Prakticky nejvyužívanější a dostatečně kvalitní je bezpečnostní protokol WPA se šifrovacími klíči TKIP, jenž jsou známy jen připojující se klientské stanici. Typem autentizace a šifrování WPA-TKIP jsou zabezpečeny i místní WiFi sítě eduroam.

Praktická část byla zaměřena na testování dostupných programů pro měření kvality signálu WiFi sítí v okolí počítače. Prakticky jsem odzkoušela pět softwarů na pěti stanovištích budovy U5. Programy detekovaly v místech měření různý počet WiFi sítí. Software WirelessMon zobrazuje nejvíce dat o bezdrátových sítích a NetSurveyor poskytuje nejlepší diagnostické přehledy. Program XiRRUS Wi-Fi Monitor jako jediný umožňuje miniaplikaci na ploše pro nepřetržité mapování aktivních WiFi sítí. Vistumbler nepodává informace o MAC adresách a o použitém zabezpečení a nelze jej tedy považovat za kvalitní software k detekování bezdrátových sítí. Pátým testovaným softwarem byl inSSIDer, jenž vyobrazoval dostatečný počet informací, výsledky měření byly lehce zpracovatelné, a proto byl vybrán k mapování školní sítě eduroam na budově U5 FAI UTB.

Spektrální analyzátor Wi-Spy 2.4i od výrobce MetaGeek je cenově nepřijatelnějším nástrojem k mapování WiFi a GSM sítí. Budova U5 FAI UTB se nachází v hustě osídlené oblasti, kde se vyskytuje mnoho zařízení pracujících v pásmu 2,4 GHz jako bluetooth, bezdrátové telefony, mikrovlnné trouby, aj., které Wi-Spy 2.4i může detekovat. Vhodnou volbou pro vyhledávání WiFi sítí v zarušených místech je spektrální analyzátor pro pásma 2,4 GHz a zároveň pro 5 GHz, jehož cena se pohybuje kolem 14 000,-.

V dalším kroku praktické části bylo provedeno detekování signálu školní WiFi sítě eduroam na budově U5. Zjistila jsem, že školní WiFi síť má 12 APs, které pokrývají jednotlivé části budovy U5. Signál na 102 stanovištích z celkového počtu 318 bodů měření je velmi nízký až nulový a není tak zde možnost připojení k Internetu. Byly dokonce detekovány i místa, kde školní síť eduroam nebyla vůbec zachycena. Nejhůře pokryto WiFi signálem, jehož hodnota RSSI se průměrně pohybuje od -80 až do -85 dBm, je první patro části U52. Naopak signál je nejsilnější v blízkosti WiFi APs (RSSI okolo -45 dBm). V částech budovy U5, kde se studenti nejběžněji připojují ke školní síti eduroam, se hodnota RSSI pohybuje od -59 do -61 dBm, ale v některých místech je kvalita signálu nestálá a dochází tak k rušení a přemostování na jiný kvalitnější WiFi AP.

WiFi síť nachází také uplatnění v průmyslu komerční bezpečnosti. Je integrována do různých technologií a nahrazuje dosavadní metalické vedení. Využívají se v radiofrekvenčním pásmu k online komunikaci, předávání veškerých informací v reálném čase, k řízení činností, k lokalizaci PDA nebo notebooků vybavených WiFi.

Hlavním cílem práce bylo praktické seznámení se softwary k měření dostupných signálu WiFi sítí a detailní mapování kvality signálu školní sítě eduroam. Přínos práce spatřuji v jejím možném využití pro zkvalitnění pokrytí signálu WiFi sítí eduroam na budově U5 FAI UTB.

CONCLUSION

In the dissertation were explained issues of WiFi networks that fall into the category of wireless WLAN networks. Technology of WiFi networks is standardized by IEEE 802.11 standard and for transfer of electromagnetic signal uses the 2.4 GHz band which includes 14 channels maximum with diverse middle frequency. Signal of WiFi network is most often spread in an internal local environment; the data transfer in an external environment is not excluded though and that is done by the means of omnidirectional, sector, or directional antennas within the perimeter of 30 kilometres. There is the need of visual and radio visibility.

An important part of the dissertation was WiFi networks securing. Users need to have an active firewall on their computers in order to protect their confidential data from potential offenders. Furthermore, blocking of SSID transmission into an area is needed with which is connected the good choice of an antenna, covering only the required space. Authentication and encryption is part and parcel of securing. The most used and of sufficient quality is a security protocol WPA with cipher keys TKIP that only client's station knows. The WPA-TKIP type of authentication and encryption is also used for the local WiFi network eduroam.

The practical part was focused on testing of available programmes for quality measurement of WiFi signal within computer vicinity. I put five software products in practice at five posts at U5 building. Programmes detected various number of WiFi networks in areas of the measurement. Software WirelessMon displays the most information about wireless networks while NetSurveyor provides the best diagnostic view. Programme XiRRUS Wi-Fi Monitor as the only one enables the use of a mini-application on the screen for constant mapping of active WiFi networks. Vistumbler does not serve information about MAC addresses, nor about used securement and therefore cannot be considered as a quality product for detection of wireless networks. The fifth software product which I tested was inSSIDer; this one showed sufficient pieces of information, the results of measurement were easily processible, and as such was chosen for mapping of the school network eduroam at U5 FAI UTB building.

Spectral analyser Wi-Spy 2.4i by MetaGeek is at the most affordable price tool for mapping WiFi and GSM network. U5 FAI UTB building is located in densely populated area, where lot of devices work in 2.4 GHz band, for example Bluetooth, wireless phones,

microwave ovens etc., which Wi-Spy 2.4i can detect. Suitable choice for WiFi network searching within interfering areas is spectral analyser for 2.4 GHz bands and 5 GHz at the same time; its price is about 14 000CZK.

The next step in the practical part was the detection of signal of the school WiFi network eduroam at the U5 building. I found out that the school WiFi network has 12 APs that cover individual parts of U5 building. The signal at 102 posts, out of the total 318 measured places, is from very low to zero; therefore there is not the possibility of connection to Internet. There were even places where the school network eduroam was not detected at all. The lowest WiFi signal, where RSSI value is approximately between -80 and -85 dBm, is the first floor of U52. The strongest signal, on the other hand, is in the vicinity of WiFi APs (with RSSI about -45 dBm). In the places where students connect the most commonly to the school network eduroam, the RSSI value is between -59 and -61 dBm; in some places, however, is the signal quality not stable and therefore interference occurs there as well as bridging to a higher quality WiFi AP.

WiFi network is being used also in the industry of commercial security. It is integrated into various technologies and replaces existing metallic lines. They are being used for online communication in radio frequency band, transferring all information in real time, for activity management, for localization of PDA or notebooks equipped with WiFi.

The main goal of this dissertation was practical familiarization with software products for measurement of the availability of WiFi signal and detailed mapping of signal quality of school network eduroam. I see the contribution of this dissertation in its possible use for improvement of signal coverage of WiFi network eduroam at U5 FAI UTB building.

SEZNAM POUŽITÉ LITERATURY

- [1] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 4. aktualizované a rozšířené vydání. Brno: Computer Press, a.s., 2008. ISBN 978-80-251-2073-6.
- [2] BARTÁČEK, Jiří. Stránky o elektronice a počítačích. *Bezdrátové sítě*. [online]. 24. červenec 2011 [cit. 2011-11-27]. Dostupné z: <http://www.barts.cz/index.php/pocitace/site/29-bezdratovesite>
- [3] Wi-Fi. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 11. 9. 2010, last modified on 19. 11. 2011 [cit. 2011-11-27]. Dostupné z: <http://cs.wikipedia.org/wiki/Wi-Fi>.
- [4] KYSELA, Jiří. Bezdrátový Internet a technologie Wi-Fi v České republice. *Bezdrátový Internet a technologie Wi-Fi v České republice - Internet pro všechny* [online]. 14. duben 2010 [cit. 2011-11-29]. Dostupné z: <http://www.internetprovsechny.cz/bezdratovy-internet-a-technologie-wi-fi-v-ceske-republice/>
- [5] IVANKA, Ján a Marek ČANDÍK. Konfigurace a zabezpečení WiFi sítí. In: *Security magazín*. Praha: Familymedia, 2007, 4 - 8. ISSN 1210 - 8723.
- [6] ZANDL, Patrick. *Bezdrátové sítě WiFi : Praktický průvodce*. Brno: Computer Press, a.s., 2003. ISBN 80-7226-632-2.
- [7] BARKEN, Lee. Jak zabezpečit bezdrátovou síť Wi-Fi. Brno: Computer Press, a.s., 2004. ISBN 80-251-0346-3.
- [8] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Brno: CP Books, a.s., 2005. ISBN 80-251-0791-4.
- [9] KUCHARŤ, Martin. Jak zapojíme síť: WiFi bez tajemství. *Inflow: Svět hardware* [online]. 7. 10. 2009 [cit. 2012-02-01]. ISSN 1213-0818. Dostupné z: http://www.svethardware.cz/art_doc-6E26F87B6685C3F2C12570A600456195.html
- [10] KORUC, Zbyněk. Bezdrátové sítě dle standardu IEEE 802.11 (WiFi). In: *W-sin* [online]. 2006 [cit. 2012-02-01]. Dostupné z: <http://w-sin.cz/docs/wifi-teorie.pdf>

- [11] IVANKA, Ján a Petr NAVRÁTIL. Standardizace WiFi sítí a jejich využití v průmyslu komerční bezpečnosti. In: *Security magazín*. Praha: Familymedia, 2009, 25 - 31. ISSN 1210 – 8723.
- [12] SEIDL, David. Praktické zkušenosti s provozem WiFi Access Pointu pod OS GNU/Linux. In: *VŠB-TU Ostrava* [online]. 2005 [cit. 2012-02-01]. Dostupné z: http://ols.vsb.cz/2005-12-15/wifi/wifi_na_linuxu.pdf
- [13] GREGR, Filip et al. Návrh a realizace datových spojení pomocí bezdrátové sítě Wi-Fi. In: *Střední škola informatiky a spojů, Brno* [online]. 2010 [cit. 2012-02-02]. Dostupné z: http://www.sosinformatikybrno.cz/src/downloads/Navrh_a_realizace_datovych_spojovani_pomoci_bezdratove_site_Wi-Fi.pdf
- [14] XIRRUS. *Xirrus Wi-Fi Monitor Gadgets 1.2* [software]. [přístup 17. únor 2012]. Dostupné z: <http://www.slunecnice.cz/sw/xirrus-wi-fi-monitor-gadgets/>. Požadavky na systém: PC Windows Vista 32bit/Vista 64bit/7.
- [15] NUTS ABOUT NETS LLC. *NetSurveyor* [software]. [přístup 17. únor 2012]. Dostupné z: http://www.stahuj.centrum.cz/internet_a_site/monitoring_site/netsurveyor/. Požadavky na systém: PC Windows 2000/XP.
- [16] ANDRES CALCUTT. *Vistumbler* [software]. [přístup 17. únor 2012]. Dostupné z: http://www.stahuj.centrum.cz/internet_a_site/monitoring_site/vistumbler/. Požadavky na systém: PC Windows Vista.
- [17] PASSMARK SOFTWARE. *WirelessMon* [software]. [přístup 17. únor 2012]. Dostupné z: http://www.stahuj.centrum.cz/internet_a_site/monitoring_site/wirelessmon/. Požadavky na systém: PC Windows XP/Vista/Vista 64bit/2003 Server/2008 Server/7/7 64bit.
- [18] METAGEEK, LLC. *InSSIDer 2.0.7.0126* [software]. [přístup 17. únor 2012]. Dostupné z: <http://www.slunecnice.cz/sw/inSSIDer/>. Požadavky na systém: PC Windows Vista 32bit/ Vista 64bit/XP/7.
- [19] Eduroam.cz. *Www.terena.nl* [online]. 9. 3. 2006 [cit. 2012-02-21]. Dostupné z: <http://www.eduroam.cz/doku.php?id=cs:start>

- [20] Používání sítě Wi-Fi na FAI. *Univerzita Tomáše Bati ve Zlíně: Fakulta aplikované informatiky* [online]. © 2000-2012 [cit. 2012-03-04]. Dostupné z: http://web.fai.utb.cz/?id=0_0_9_3_0_1&lang=cs&type=0
- [21] Dislokace budovy U5. *Univerzita Tomáše Bati ve Zlíně: Fakulta aplikované informatiky* [online]. © 2000-2012 [cit. 2012-03-04]. Dostupné z: http://web.fai.utb.cz/?id=0_0_8&lang=cs&type=0
- [22] ŘEHÁK, Jan. Warchalking a bezpečnost WiFi sítě. *HW.cz.* [online]. 1997 - 2012 [cit. 2012-03-31]. Dostupné z: http://www.hw.cz/ethernet/wifi/wifi_warchalking.html
- [23] METAGEEK, LLC. *Chanalyzer Lite* [software]. [přístup 11. dubna 2012]. Dostupné z: <http://www.metageek.net/products/chanalyzer-lite/>. Požadavky na systém: Windows XP SP3, Vista, Windows.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

WiFi	Wireless Fidelity
IEEE	The Institute of Electrical and Electronic Engineers
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard
EAP	Extensible Authentication Protocol
GSM	Global System for Mobile Communications
UMTS	Universal Mobile Telecommunications System
CDMA	Code Division Multiple Access
SSID	Service Set Identifier
RSSI	Received Signal Strength Indication
FAI UTB	Fakulta aplikované informatiky Univerzity Tomáše Bati
IP	Internetový protokol
PDF	Portable Document Format
MAC	Media Access Control
VPN	Virtual Private Network
DoS	Denial of Service
AP/APs	Access Point/Access Points
ASCII	American Standard Code for Information Interchange

WiMAX	Worldwide Interoperability for Microwave Access
PDA	Personal Digital Assistant
IrDa	Infrared Data Association
ADSL	Asymmetric Digital Subscriber Line
EDGE	Enhanced Data Rates For Global Evolution
RADIUS	Remote Authentication Dial In User Service
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
GHz/MHz	Gigahertz, Megahertz; jednotka frekvence
Mbps, Mbits	Megabit za sekundu; jednotka přenosové rychlosti
dBi	Decibel na isotop; jednotka ziskovosti
dBm	Decibel nad miliwattem; jednotka RSSI
USB	Universal Serial Bus

SEZNAM OBRÁZKŮ

Obrázek 1: Vzdálenosti bezdrátových sítí [4].....	11
Obrázek 2: Režimy viditelnosti ve Fresnelově zóně	13
Obrázek 3: Šíření signálu v rámci buněk [4]	14
Obrázek 4: Struktura sítě Ad-hoc [2].....	15
Obrázek 5: Infrastrukturní síť [2]	15
Obrázek 6: Všesměrové antény [4].....	21
Obrázek 7: Vyzařovací diagram všesměrové antény a) v horizontálním směru a b) ve vertikálním směru [12]	21
Obrázek 8: Sektorové antény [9]	21
Obrázek 9: Vyzařovací diagram sektorové antény [12]	22
Obrázek 10: Směrové antény [2]	22
Obrázek 11: Vyzařovací diagram směrové antény [12]	23
Obrázek 12: Yagi anténa [9].....	23
Obrázek 13: Princip vícecestného šíření signálu [13]	25
Obrázek 14: WiFi síť eduroam v prvním patře budovy U5 FAI UTB [20]	27
Obrázek 15: WiFi síť eduroam ve druhém patře budovy U5 FAI UTB [20]	28
Obrázek 16: WirelessMon - Informace o WiFi síti	29
Obrázek 17: WirelessMon - Použité kanály měřených WiFi sítí	30
Obrázek 18: WirelessMon - Dostupné WiFi sítě.....	30
Obrázek 19: Vistumbler - Dostupné WiFi sítě	31
Obrázek 20: Vistumbler – Filtrování	31
Obrázek 21: InSSIDer – Dostupné WiFi sítě.....	32
Obrázek 22: InSSIDer – Časový graf RSSI.....	33
Obrázek 23: InSSIDer – Pásmo 2,4 GHz	33
Obrázek 24: NetSurveyor – Dostupné WiFi sítě	34
Obrázek 25: NetSurveyor – Časový průběh kvality signálu.....	34
Obrázek 26: NetSurveyor – Použité kanály.....	34
Obrázek 27: NetSurveyor – Spektrogram.....	35
Obrázek 28: XiRRUS Wi-Fi Monitor – Miniaplikace na ploše	36
Obrázek 29: XiRRUS Wi-Fi Monitor – Dostupné WiFi sítě.....	36
Obrázek 30: Body měření v prvním patře budovy U5 FAI UTB [21]	37
Obrázek 31: Body měření v druhém patře budovy U5 FAI UTB [21].....	38

Obrázek 32: Body měření ve třetím patře budovy U5 FAI UTB [21].....	38
Obrázek 33: Wi-Spy 2.4i	47
Obrázek 34: Wi-Spy 2.4i – Dostupné WiFi sítě	48
Obrázek 35: Wi-Spy 2.4i – Grafické vyobrazení I	49
Obrázek 36: Wi-Spy 2.4i – Grafické vyobrazení II.....	49
Obrázek 37: Wi-Spy 2.4i – Tabulka „Markers“ a funkce „Inspector“	50
Obrázek 38: Wi-Spy 2.4i - 3D pohled	50
Obrázek 39: Trasa měření v prvním patře budovy U5 FAI UTB [21]	53
Obrázek 40: Trasa měření v druhém patře budovy U5 FAI UTB [21].....	53
Obrázek 41: Trasa měření ve třetím patře budovy U5 FAI UTB [21]	54
Obrázek 42: Graf zachycených WiFi sítí.....	57
Obrázek 43: Graf zabezpečení WiFi sítí.....	57

SEZNAM TABULEK

Tabulka 1: Vlastnosti technologie WLAN [4].....	12
Tabulka 2: Kanály v pásmu 2,4 GHz využívané v Evropě [9].....	24
Tabulka 3: NetSurveyor – První stanoviště	39
Tabulka 4: InSSIDer – První stanoviště	39
Tabulka 5: Vistumbler – První stanoviště.....	40
Tabulka 6: WirelessMon – První stanoviště	40
Tabulka 7: XiRRUS Wi-Fi Monitor – První stanoviště	40
Tabulka 8: NetSurveyor – Druhé stanoviště.....	41
Tabulka 9: InSSIDer – Druhé stanoviště	41
Tabulka 10: Vistumbler – Druhé stanoviště	41
Tabulka 11: WirelessMon – Druhé stanoviště.....	41
Tabulka 12: XiRRUS Wi-Fi Monitor – Druhé stanoviště	41
Tabulka 13: NetSurveyor – Třetí stanoviště	42
Tabulka 14: InSSIDer – Třetí stanoviště	42
Tabulka 15: Vistumbler – Třetí stanoviště	42
Tabulka 16: WirelessMon – Třetí stanoviště.....	43
Tabulka 17: XiRRUS Wi-Fi Monitor – Třetí stanoviště	43
Tabulka 18: NetSurveyor – Čtvrté stanoviště.....	43
Tabulka 19: InSSIDer – Čtvrté stanoviště	43
Tabulka 20: Vistumbler – Čtvrté stanoviště	44
Tabulka 21: WirelessMon – Čtvrté stanoviště.....	44
Tabulka 22: XiRRUS Wi-Fi Monitor – Čtvrté stanoviště	44
Tabulka 23: NetSurveyor – Páté stanoviště.....	45
Tabulka 24: InSSIDer – Páté stanoviště	45
Tabulka 25: Vistumbler – Páté stanoviště	45
Tabulka 26: WirelessMon – Páté stanoviště.....	45
Tabulka 27: XiRRUS Wi-Fi Monitor – Páté stanoviště	46
Tabulka 28: Zachycené WiFi sítě	56

SEZNAM PŘÍLOH

PI: Výpis naměřených hodnot z prvního patra budovy U5 FAI UTB

PII: Výpis naměřených hodnot z druhého patra budovy U5 FAI UTB

PIII: Výpis naměřených hodnot z třetího patra budovy U5 FAI UTB

PIV: Výpis naměřených hodnot z 8. – 4. patra budovy U5 FAI UTB

PV: Výpis naměřených hodnot – školní síť eduroam

PVI: Výpis naměřených hodnot jednotlivými softwary na budově U5 FAI UTB

PVII: CD ROM, na kterém jsou uloženy podrobné výsledky z měření, práce s nimi a grafické zpracování ve dvou sešitech Excel s názvy Měření programy na exponovaných místech budovy U5.xlsx a Skenování WiFi sítí na budově U5.xlsx.