

# **Aplikační software pro monitoring WiFi sítí.**

Application software for monitoring WiFi networks.

Bc. Helena Spurná



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2010/2011

## ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Helena SPURNÁ**  
Osobní číslo: **A09458**  
Studijní program: **N 3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
  
Téma práce: **Aplikační software pro monitoring wifi sítí**

Zásady pro vypracování:

1. Seznamte se s oblastí a problematikou monitorování wifi sítí.
2. Uveďte charakteristiku několika programů pro monitorování wifi sítí.
3. Charakterizujte základní typy antén pro wifi sítě.
4. Provedte průzkum zabezpečení wifi sítí pomocí wardrivingu ve vybrané části sídliště Jižní svahy.
5. Vytvořte stručný manuál pro vyhledání volnějšího přenosového kanálu wifi sítě.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

1. BARKEN, Lee. Jak zabezpečit bezdrátovou síť Wi-Fi. Brno : Computer Press, a.s., 2004. 176 s.
2. IVANKA, Ján, ČANDÍK, Marek. Konfigurace a zabezpečení WiFi sítě. Security magazín. 2007, č. 14, s. 4-18.
3. HORÁK, Jaroslav; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4.aktualizované. Brno : Computer Press, a.s., 2008. 328 s.
4. KOHRE, Thomas. Stavíme si bezdrátovou síť Wi-Fi. Vyd. 1. Brno : Computer Press, a.s., 2004. 296 s.
5. HAŇKA, Ladislav. Teorie elektromagnetického pole. Praha : SNTL, 1982. 224 s.
6. BÁRTA, Jiří. Úvod do počítačových sítí. České Budějovice : Koop, 1995. 168 s.

Vedoucí diplomové práce:

Ing. Ján Ivanka

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

25. února 2011

Termín odevzdání diplomové práce:

27. května 2011

Ve Zlíně dne 25. února 2011

prof. Ing. Vladimír Vašek, CSc.  
děkan



doc. RNDr. Vojtěch Křesálek, CSc.  
ředitel ústavu

## **ABSTRAKT**

Diplomová práce seznamuje s oblastí, problematikou monitorování WiFi sítí. Stručně vysvětluje princip činnosti WiFi sítí a šíření elektromagnetických vln. Popisuje specifikace antén využívaných k WiFi připojení. Prezentuje několik druhů softwaru, které se používají pro monitoring WiFi sítí. Součástí diplomové práce je průzkum zabezpečení WiFi sítí, manuál k hledání volného pásma a odstraňování problémů s bezdrátovými sítěmi WiFi pomocí příslušného softwaru v lokalitě Jižní Svahy.

Klíčová slova: WiFi, monitoring, wardriving, signál, anténa

## **ABSTRACT**

The diploma thesis deals with the area and the question of WiFi monitoring. It shortly explains the principle of WiFi activity and spreading of electromagnetic waves. It describes the specifications of the antennas used for WiFi connection. It presents a few kinds of software which is used for WiFi monitoring. A part of the diploma thesis is an investigation of WiFi security, a manual for searching of free zones and removing of problems with WiFi using the relevant software in the area of Jižní Svahy.

Keywords: WiFi, monitoring, wardriving, signal, antenna

Ráda bych poděkovala vedoucímu diplomové práce panu Ing. Jánů Ivankovi za pomoc a rady při jejím zpracování. Dále bych ráda poděkovala rodině a přátelům, kteří mě podporovali ve studiu.

**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**

|  |           |
|--|-----------|
| <b>ÚVOD.....</b>   | <b>9</b>  |
| <b>I TEORETICKÁ ČÁST .....</b>                               | <b>10</b> |
| <b>1 PRINCIP ČINNOSTI WIFI SÍTÍ .....</b>                    | <b>11</b> |
| <b>2 SEZNÁMENÍ S RÁDIOVÝMI TECHNOLOGIEMI .....</b>           | <b>13</b> |
| 2.1 ELEKTROMAGNETISMUS .....                                 | 13        |
| 2.2 INDUKCE.....   | 13        |
| 2.3 VODIVOST .....   | 13        |
| 2.4 RÁDIOVÉ VLNY.....  | 13        |
| 2.4.1 Struktura vlny.....                                    | 14        |
| 2.5 MODULACE .....   | 14        |
| 2.5.1 Amplitudová modulace .....                             | 15        |
| 2.5.2 Frekvenční modulace .....                              | 15        |
| 2.5.3 Digitální modulace .....                               | 15        |
| 2.6 ÚTLUM .....  | 15        |
| <b>3 ZÁKLADNÍ TYPY A CHARAKTERISTIKA ANTÉN PRO WIFI.....</b> | <b>16</b> |
| 3.1 PRINCIP FUNKCE ANTÉN.....                                | 16        |
| 3.2 TYPY ANTÉN.....  | 16        |
| 3.2.1 Směrové antény .....                                   | 17        |
| 3.2.2 Sektorové antény .....                                 | 17        |
| 3.2.3 Všesměrové antény.....                                 | 18        |
| <b>4 MONITORING WIFI SÍTÍ.....</b>                           | <b>19</b> |
| 4.1 OTEVŘENÉ A UZAVŘENÉ SÍTĚ .....                           | 19        |
| 4.2 LEGISLATIVA PRO MONITORING WiFi SÍTÍ.....                | 20        |
| 4.3 WARDRIVING .....   | 20        |
| 4.4 WARCHALKING .....  | 21        |
| <b>5 SOFTWARE PRO MONITORING WIFI SÍTÍ.....</b>              | <b>23</b> |
| 5.1 NETSTUMBLER 0.4.0 .....                                  | 23        |
| 5.2 NETSURVEYOR 2.0.....                                     | 24        |
| 5.3 XIRRUS WiFi INSPECTOR.....                               | 25        |
| 5.4 VISTUMBLER 9.8 .....                                     | 26        |
| 5.5 INSSIDER.....  | 27        |
| 5.6 WIRESHARK .....  | 28        |
| 5.7 EASY WiFi RADAR 1.05 .....                               | 30        |
| <b>II PRAKTICKÁ ČÁST .....</b>                               | <b>31</b> |
| <b>6 PRŮZKUM ZABEZPEČENÍ WIFI SÍTÍ WARDRIVINGEM</b>          |           |

|  |           |
|--|-----------|
| <b>V LOKALITĚ JIŽNÍ SVAHY .....</b>                                    | <b>32</b> |
| 6.1 POUŽITÉ PROSTŘEDKY .....   | 32        |
| 6.2 MAPA JEDNOTLIVÝCH STANOVIŠŤ .....                                  | 33        |
| 6.3 DATA NAMĚŘENÁ V JEDNOTLIVÝCH STANOVIŠTÍCH .....                    | 33        |
| 6.4 VYHODNOCENÍ NAMĚŘENÝCH DAT.....                                    | 40        |
| <b>7 MANUÁL K HLEDÁNÍ VOLNĚJŠÍHO PŘENOSOVÉHO KANÁLU.....</b>           | <b>42</b> |
| 7.1 Wi-SPY 2.4I.....   | 42        |
| 7.2 NÁSTROJE (PRVKY) PROGRAMU CHANALYZER LITE .....                    | 43        |
| 7.2.1 Planar zobrazení (Planar view) .....                             | 43        |
| 7.2.2 Density zobrazení (Density view) .....                           | 44        |
| 7.2.3 Waterfall zobrazení (Waterfall view).....                        | 44        |
| 7.2.4 WiFi sítě (WiFi networks) .....                                  | 44        |
| 7.2.5 WiFi kanály (WiFi Channels) .....                                | 45        |
| 7.2.6 Síla sítě (Network Strength).....                                | 45        |
| 7.2.7 Aktivita kanálu v čase (Channel activity over time) .....        | 46        |
| 7.2.8 Aktivita WiFi sítí na kanálech (Channel activity bar graph)..... | 46        |
| 7.2.9 3D zobrazení .....   | 46        |
| 7.3 VLASTNÍ HLEDÁNÍ VOLNĚJŠÍHO PŘENOSOVÉHO KANÁLU WiFi SÍTĚ.....       | 47        |
| 7.3.1 Analýza WiFi sítě.....   | 48        |
| 7.3.2 Nástroje pro testování „datové“ propustnosti sítě.....           | 48        |
| 7.3.3 Nové nastavení WiFi kanálu .....                                 | 51        |
| 7.3.4 Ověření změn .....   | 52        |
| <b>ZÁVĚR .....</b>   | <b>54</b> |
| <b>ZÁVĚR V ANGLIČTINĚ .....</b>  | <b>56</b> |
| <b>SEZNAM POUŽITÉ LITERATURY .....</b>                                 | <b>58</b> |
| <b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK .....</b>                        | <b>60</b> |
| <b>SEZNAM OBRÁZKŮ .....</b>  | <b>61</b> |
| <b>SEZNAM TABULEK.....</b>   | <b>63</b> |



## ÚVOD

V posledních letech došlo k nárůstu využívání bezdrátových systémů. Příčinou byla poptávka po lepší konektivitě do sítě internet. K hlavním výhodám bezdrátového připojení patří cena, mobilita, vysoká univerzálnost. Největší nevýhodou je přenosové medium – vzduch. K přenosu rádiového signálu se používají elektromagnetické vlny.

Uživatelé počítačů se mohou setkat s nebezpečím různého druhu, v podobě virů i internetovými útoky. Ztráta informací může být pro společnosti závažným problémem. Vedoucí pracovníci v úřadech, společnostech si uvědomují, že je nutné provést opatření pro ochranu informací. Mnoho výrobců bezdrátových zařízení nechává z výroby vypnuté šifrování. A uživatelé, kteří nemají znalosti k problematice WiFi, šifrování opomenou nastavit.

Wardriving je technika vyhledávání bezdrátových sítí z automobilu. Warchalking je zjišťování dostupných bezdrátových sítí člověkem, který se pohybuje po vlastních nohou. Člověk potřebuje pouze notebook, síťovou kartu, anténu a software, aby mohl vyhledat bezdrátové sítě v okolí. Někteří lidé se snaží nejen najít bezdrátovou síť, ale i získat přístup k souborům nebo poškozovat systémy.

K získání informací, o dostupných bezdrátových sítích, se používá příslušný software. Do softwaru není třeba investovat. Několik typů aplikačního softwaru pro monitoring WiFi sítí je volně dostupný na internetu. Software se liší vizualizací a funkcemi, které poskytuje. Udává například informace o názvu sítě, síle signálu, zabezpečení sítě, umístění routeru.

Diplomová práce je rozdělena na teoretickou a praktickou část. Součástí teoretické části je seznámení s problematikou monitorování WiFi sítí a šíření elektromagnetických vln. Práce prezentuje několik programů, které se využívají pro monitoring WiFi sítí a jsou volně dostupné. Podle odhadů je více jak 60% firemních sítí otevřených anonymnímu přístupu. Proto součástí praktické části je průzkum zabezpečení WiFi sítí na sídlišti Jižní Svahy. K monitorování WiFi je využit jeden z programů, který je prezentován v teoretické části. Pro řešení problémů s WiFi sítěmi je v praktické části odzkoušen Wi-Spy 2.4i spektrální analyzátor, který se používá i k vyhledávání volnějšího kmitočtového pásma.

## **I. TEORETICKÁ ČÁST**

## 1 PRINCIP ČINNOSTI WIFI SÍTÍ

Wireless Fidelity (dále jen WiFi) je standard pro lokální bezdrátové sítě a vychází ze specifikace The Institute of Electrical and Electronics Engineers (dále jen IEEE) 802.11. Využívá bezlicenční pásmo (2,4 GHz a 5 GHz), důsledkem toho je silné zarušení příslušného frekvenčního spektra.

WiFi sítě používají dvě topologie k uspořádání komponent v síti. U první topologie se zařízení připojují k jednomu centrálnímu prvku, který je označen jako Access Point (dále jen AP) pomocí bezdrátových Peripheral Component Interconnect (slot na základní desce) WiFi karet či přímo a častěji pomocí routerů (směrovač), které jsou k počítači připojeny klasickou metalickou sítí. V ideálním případě by na sebe centrální prvek a druhá z komunikujících stran měli vidět, protože s jakoukoliv překážkou se síla signálu poměrně znatelně snižuje.[7]

Druhou možností je použití topologie „ad-hoc“ (jednotlivý uživatelé spolu komunikují přímo), kdy žádné AP není nutno použít. To se vyplatí jak z pohledu finančních nákladů, tak díky jednoduchosti zapojení. Stinnou stránku však představuje z pochopitelných důvodů nutnost vzájemné viditelnosti všech zařízení (v případě sítí s AP komunikuje klient pouze s tímto síťovým prvkem, zde nikoliv). A to u větších prostor, které je třeba pokrýt, možné není. Typ připojení je uváděn pod zkratkou Independent Basic Service Set (nezávislý základní soubor služeb).[7]

Síťová WiFi karta může být také jednoduše nahrazena nejrůznějšími Universal Serial Bus klíči (dále jen USB, způsob připojení periférií k počítači), které svou práci odvádějí v menších prostorách velmi dobře. Lepší USB klíče dokonce umožňují připojit pro zvýšení dosahu signálu a jeho zkvalitnění některou z externích antén.[7]

Při užívání bezdrátové sítě je důležité si uvědomit, že signál se šíří vzduchem. Signál proniká i mimo prostor uživatele. Bezdrátovou komunikaci je možné zabezpečit šifrovacími protokoly. V současné době se používají protokoly Wired Equivalent Privacy (dále jen WEP), WiFi Protected Access (dále jen WPA), WiFi Protected Access 2 (dále jen WPA 2). Při monitoringu WiFi sítí, příslušný software vypisuje informace o bezdrátových sítích i o typu šifrování.

**Konfigurace přímého připojení**

PC



PC

**Bezdrátová komunikace****Rekonfigurace přímého připojení  
na bezdrátový router**

PC



PC



PC

**Bezdrátová komunikace****Konfigurace s AP a routerem**

PC

Obr. 1: Topologie uspořádání komponent v síti

## 2 SEZNÁMENÍ S RÁDIOVÝMI TECHNOLOGIEMI

V současné době možnost šířit signál z bodu X do bodu Y bez použití kabelů je jednoduché. Více jak 100 let jsou staré vědecké znalosti, na jejichž principu pracují zařízení pro bezdrátové připojení. Využití elektromagnetických vln pro vysílání a přijímání signálu má svůj začátek v objevu elektromagnetismu. Účelem této kapitoly je seznámit se rádiovými technologiemi, popsat základní charakteristiku rádiové vlny a vztahy mezi veličinami rádiové vlny.

### 2.1 Elektromagnetismus

Hans Christian Oersted objevil úzký vztah mezi elektřinou a magnetismem. Dokázal, že průchodem elektrického proudu se vodič zahřívá.

### 2.2 Indukce

Michael Faraday objevil zákon elektromagnetické indukce – magnetické pole vytváří ve vodiči elektrický proud. Faraday navinul dlouhý drát na papírovou trubici a dovnitř trubice vsouval a vysouval magnet. Průchod magnetického pole „indukoval“ ve vodiči elektrický proud.[8]

### 2.3 Vodivost

Samuel Morse prováděl pokusy s bezdrátovým šířením signálu. Na protějšcích březích vodního kanálu ponořil do vody velké kovové desky s připojenými vodiči. Zjistil, že elektrický proud se šíří i vodou. [8]

### 2.4 Rádiové vlny

Heinrich Rudolph Hertz provedl experiment, kterým ukázal, že elektrický proud se v podobě elektromagnetických vln může šířit vzduchem rychlostí světla. Italský inženýr Guglielmo Marconi sestrojil bezdrátový telegraf, kterým přenesl kódovanou zprávu v Morseově abecedě přes průliv La Manche. Reginald Fessenden prostřednictvím elektromagnetických vln přenesl přímou řeč. V roce 1920 byly běžnou součástí automobilů rádiové přijímače. V roce 1997 vydalo IEEE standard 802.11, který vedl k masovému rozšíření bezdrátových přenosů dat.[8]

### 2.4.1 Struktura vlny

Pomocí vln se vysvětluje šíření světla, zvuku i rádiového signálu. Jednotlivé komponenty vlny pouze kmitají nahoru a dolů, vlna jako celek však cestuje materiálem a šíří se z jednoho místa na druhé.[8]

| Veličina               | Popis  |
|------------------------|--|
| Hřeben                 | Nejvyšší bod vlny  |
| Údolí                  | Nejnižší bod vlny  |
| Amplituda $\alpha$     | Popisuje výšku vlny měřenou ke střední úrovni  |
| Vlnová délka $\lambda$ | Horizontální vzdálenost mezi dvěma identickými body vlny (např. vzdálenost mezi dvěma hřebeny nebo dvěma údolími)      |
| Perioda $\tau$         | Čas potřebný na proběhnutí jednoho cyklu vlny v sekundách. Pokud vlně trvá cyklus 3 sekundy, má periodu 3              |
| Frekvence $f$          | Počet vln za jednotku času, měřeno jako počet cyklů za sekundu. Vlna provede 100 cyklů za sekundu, má frekvenci 100 Hz |
| Rychlost $v$           | Rychlost šíření vlny v jednotkách vzdálenosti za jednotku času   |

Tabulka 1: Základní charakteristika rádiové vlny[8]

|                           |  |
|---------------------------|--|
| $\omega = \lambda / \tau$ | Rychlost je rovna vlnové délce dělena periodou     |
| $\phi = v / \lambda$      | Frekvence je rovna rychlosti dělena vlnovou délkou |
| $\omega = \lambda * f$    | Rychlost je rovna vlnové délce násobené frekvencí  |
| $\phi = 1 / \tau$         | Frekvence je převrácená hodnota periody            |

Tabulka 2: Základní vztahy mezi veličinami rádiové vlny[8]

## 2.5 Modulace

Modulace je proces přidání informací ze signálové vlny na nosnou vlnu s cílem zlepšit celkovou kvalitu přenosu.[8] Modulace umožňuje současný přenos. Bez modulace by se musel přijímat a vysílat signál velkými anténami. Na počátku procesu je signál, který

je přidán k nosné vlně. Nosná vlna signál přenese a na druhé straně je zpráva přijata. Po odstranění nosné vlny dostaneme původní signál.

### **2.5.1 Amplitudová modulace**

Amplitudová modulace provádí manipulaci s amplitudou nosné vlny. Při modulaci signálu na nosnou vlnu mění amplitudu nosné vlny tak, že kopíruje průběh vlny signálové. Přijímač změny detekuje a rekonstruuje z nich signálovou vlnu. Frekvence nosné vlny se nemění. [8]

### **2.5.2 Frekvenční modulace**

U frekvenční modulace dochází k manipulaci s frekvencí nosné vlny. Amplituda nosné zůstává konstantní, mění se jen její frekvence. Hlavní výhodou frekvenční modulace oproti amplitudové modulaci je větší odolnost proti statickému rušení. [8]

### **2.5.3 Digitální modulace**

Modulace amplitudová a frekvenční se používají pro analogové přenosy, ale mnoho aplikací vyžaduje přenos digitálního signálu. Digitální signál se namoduluje na nosnou vlnu. Přijímač po přijetí odstraní nosnou vlnu a reprodukuje na původní digitální signál.

## **2.6 Útlum**

Základní zákonitostí šíření rádiového signálu je fakt, že čím jsme dále od jeho zdroje, tím je signál slabší. Čím je vzdálenost od AP větší, tím je pravděpodobnější, že datový přenos má menší rychlost.

### 3 ZÁKLADNÍ TYPY A CHARAKTERISTIKA ANTÉN PRO WIFI

Principem fungování bezdrátových sítí je pokrytí prostoru signálem. K tomu je zapotřebí odpovídající anténa. Antény slouží k vyzařování a zaostření energie do určitého směru. Antény nezesilují signál. Typ antény vyplývá z účelu, na kterou je použit. Např. na propojení dvou budov mezi sebou se použije směrová anténa. K pokrytí fotbalového hřiště použijeme všesměrovou anténu. Špatný výběr antény a pokrytí větší plochy signálem, dává prostor k provedení útoku na síť. Při monitoringu WiFi sítí využívají wardrivers signál cizích sítí. Mnozí uživatelé často netuší, že dosah signálu jejich sítě může být i mimo jejich prostory. Účelem kapitoly Základní typy a charakteristika antén pro WiFi je stručně objasnit princip funkce antén a ukázat vyzařovací diagramy používaných antén pro bezdrátové připojení.

#### 3.1 Princip funkce antén

Anténa posílá elektrický náboj tam a zpět vodičem. Elektrické pole vede k indukci magnetického pole, z něhož se následně indukuje elektrické pole, z toho magnetické – vlna se může šířit médiem (vzduchem). Vzniklý signál označujeme jako elektromagnetické pole. [8]

Antény mají řadu vlastností, z nichž se odvíjí jejich provozní a výkonnostní charakteristiky. Každá anténa je v důsledku své velikosti vhodná pro konkrétní frekvenci. Každá anténa formuje vyzařované pole do určitého směru. Vyzařovací obrazec se často vykresluje v několika směrech, aby se lépe zobrazovala oblast, kterou anténa pokrývá. Ke změření množství signálu, který anténa vysílá nebo přijímá, se používá poměrný systém. Zisk (v decibelech, dB) představuje poměr dvou výkonů (výstupní/vstupní). [8]

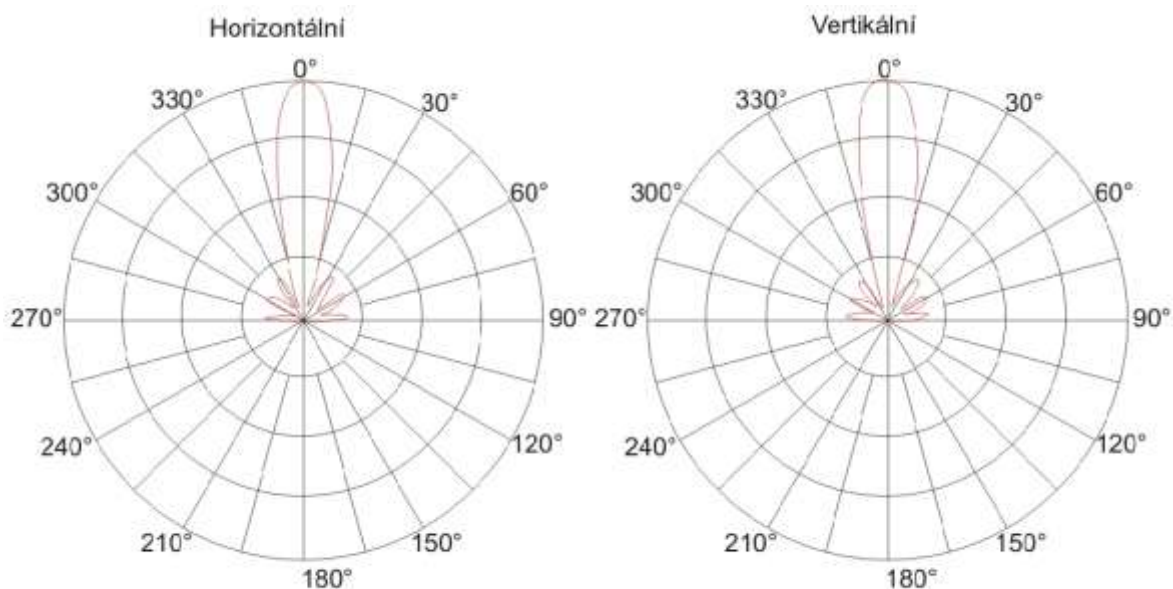
#### 3.2 Typy antén

Výběr antény se odvíjí od účelu, na který má být použita. Směrovost antény je schopnost antény vyzařovat elektromagnetické vlny v požadovaném směru. Z hlediska směrovosti dělíme antény na směrové, sektorové a všesměrové.



### 3.2.1 Směrové antény

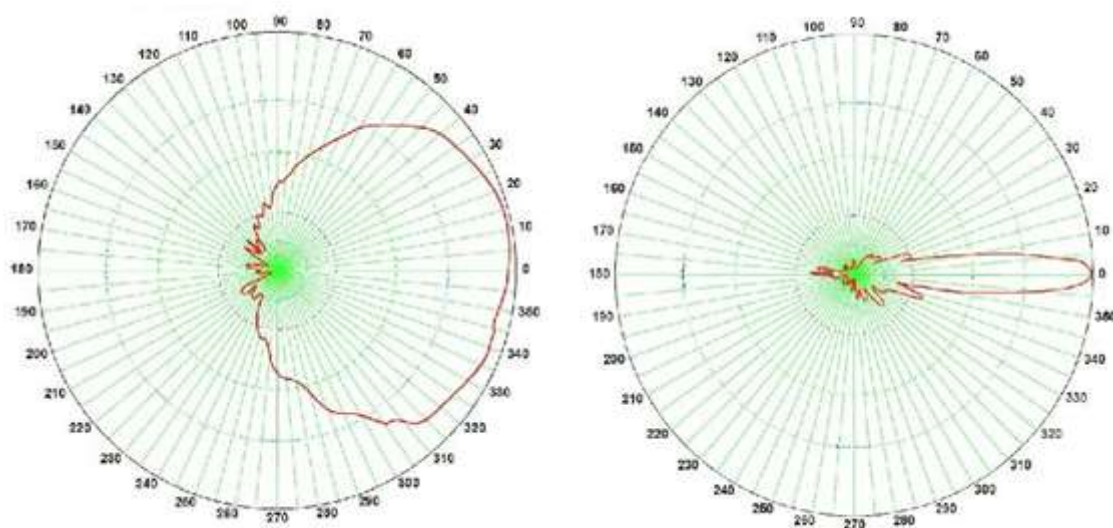
U směrových antén je vysílaný výkon soustředěn do úzkého prostorového úhlu. Slouží k propojení dvou bodů na delší vzdálenosti (1-3km). Používají se antény parabolické a tzv. Yagi antény.



Obr. 2: Vyzařovací diagram směrové antény v horizontální a vertikální rovině[19]

### 3.2.2 Sektorové antény

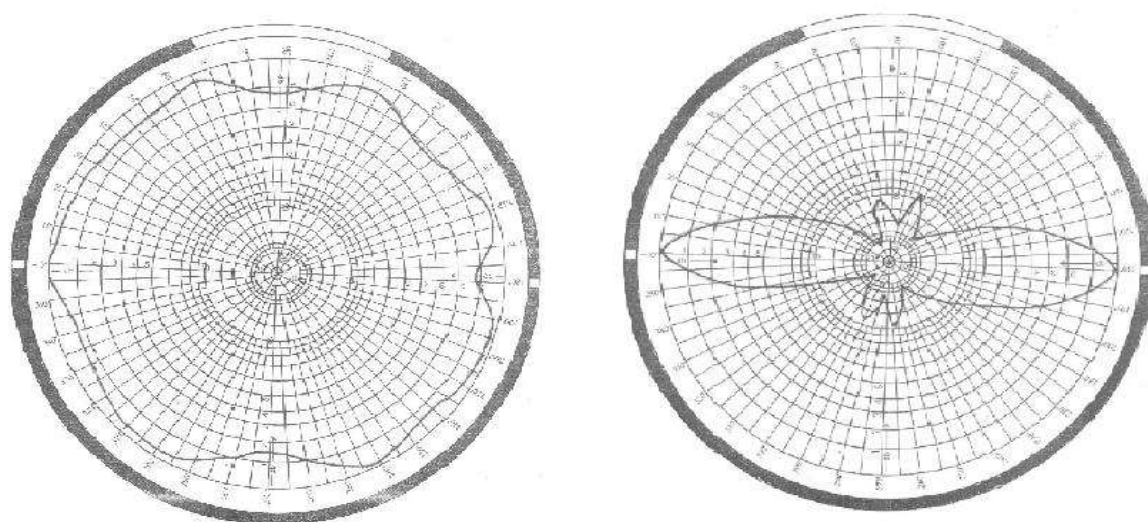
Sektorové antény pokrývají jen určitý úhel 30° do 180°. Využívají se v prostorách, kde stačí pokrýt signálem pouze omezený prostor.



Obr. 3: Vyzařovací diagram sektorové antény v horizontální (vlevo) a vertikální rovině(vpravo)[20]

### 3.2.3 Všesměrové antény

Všesměrové antény vysílají signál do všech stran, pokrývají úhel  $360^\circ$ . Přístupový bod připojuje klienty ze všech směrů nebo síť ad-hoc propojuje počítače v celém domě ze všech směrů.



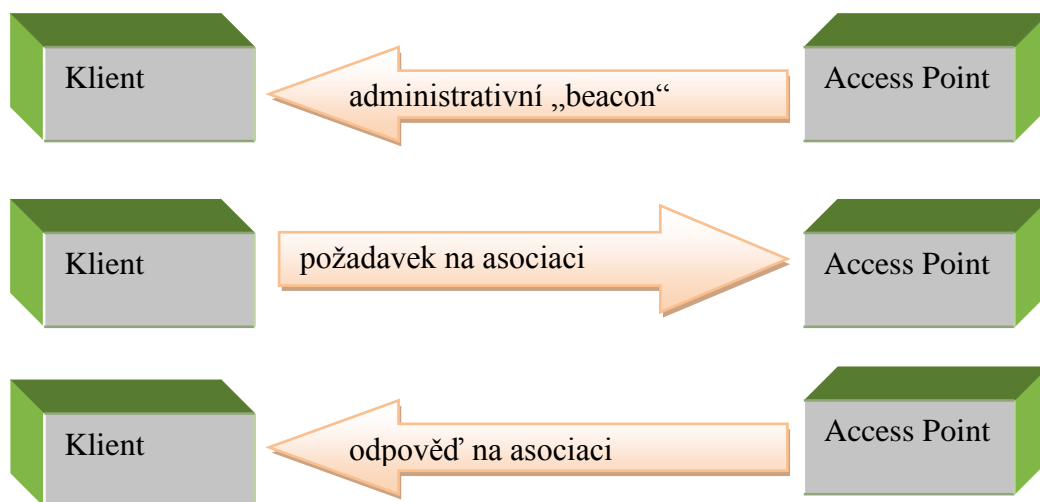
Obr. 4: Vyzařovací diagram všesměrové antény v horizontální a vertikální rovině[21]

## 4 MONITORING WIFI SÍTÍ

Monitoring představuje periodické či nárazové provádění testů, dotazů na síťové služby. Přípojky k internetu, které si lidé pořizují do svých objektů, jsou obvykle zakončovány bezdrátovými přístupovými body technologie WiFi. Mnoho lidí vlastní notebook a bezdrátové připojení umožňuje volnější pohyb. WiFi signál se řídí zákony fyziky, proto se může stát, že signál zasahuje třeba k sousedovi nebo do jiného veřejného prostoru. Kdokoli může zachytit signál a využít ho.

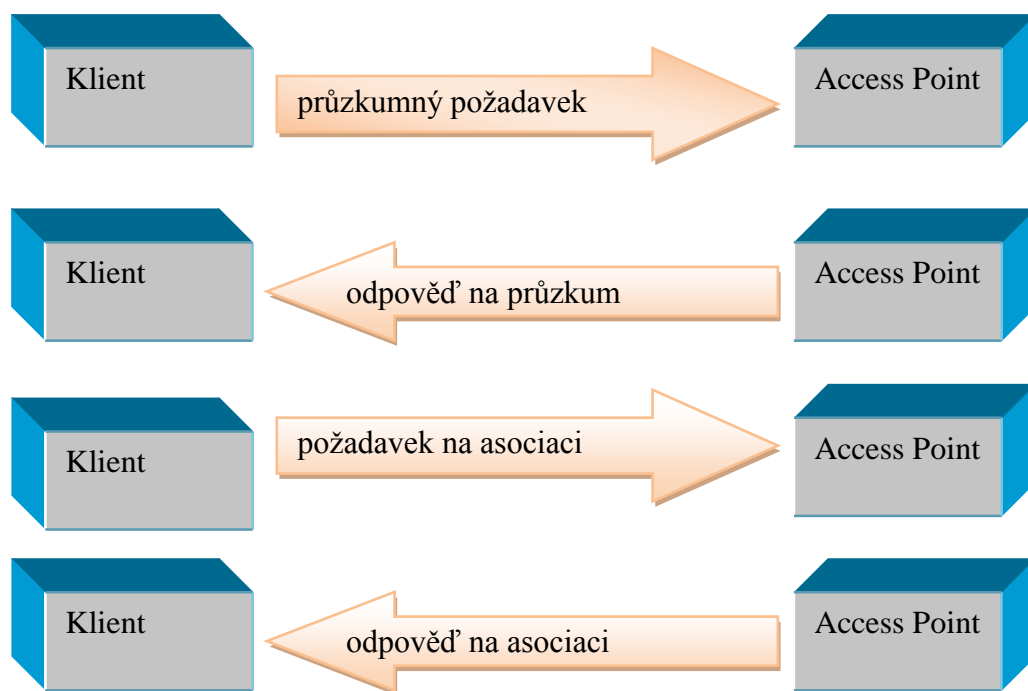
### 4.1 Otevřené a uzavřené sítě

V otevřené síti vysílá AP pravidelně administrativní rámce (beacons), ve kterých oznamuje své Service Set Identifier (dále jen SSID, název bezdrátové sítě) a další údaje (podporovaná rychlost, síla signálu). Klient vysílané rámce vidí, pošle požadavek na asociaci a AP mu odpoví asociační odpovědí.[5]



Obr. 5: Asociace v otevřené síti[5]

V uzavřené síti musí uživatel hodnotu SSID znát (někdo mu ji řekne). Klient nejprve pošle průzkumný požadavek, který obsahuje hodnotu SSID. AP požadavek přijme, a pokud se SSID shoduje s jeho vlastním, odešle odpověď na průzkum. Pokud se SSID neshoduje, AP průzkum ignoruje.[5]



Obr. 6: Asociace v uzavřené síti[5]

## 4.2 Legislativa pro monitoring WiFi sítí

Wardriving nelegálním není ve Spojených státech a ani v České republice. Wardriving (a ostatní „War“ činnosti) je pouze zjišťování volně dostupných informací aniž by síť byla jakkoliv využita či byly prováděny jakékoliv další aktivity na zjištěné síti. Dokonce není ani neautorizovaným přístupem.

Následné využívání "anonymně" přístupných sítí už ovšem nelegální ve většině států světa rozhodně je. A případný hacking prostřednictvím bezdrátových sítí je stejně nelegální jako hacking prostřednictvím sítí pevných.[22]

## 4.3 Wardriving

Wardriving je činnost, při které lidé vyhledávají dostupné bezdrátové sítě. Původně je lidé vyhledávali z jedoucího auto, proto vznikl název wardriving.

- Warstrolling – hledání sítí za pochodu na vlastních nohou
- Warboating – hledání sítí při plavbě na lodi
- Warflying – hledání sítí za letu

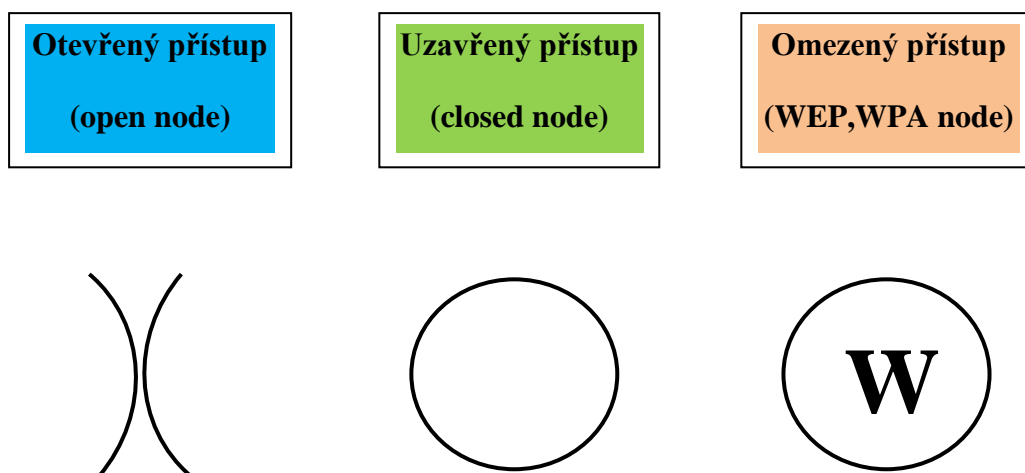
Výrobci standardně u zařízení pro bezdrátové připojení ponechávají vypnuté šifrování. Uživatelé nemusí mít znalosti, aby povolili šifrování bezdrátového přenosu nebo nastavili zabezpečení. Vyhledávání a zneužití takového připojení je jednoduchou záležitostí. Útoky typu wardriving však nemusí být jen neškodné. Útočníci mohou mít zlé úmysly a pokouší se o přístup k souborům s cílem poškodit systém. Zabezpečení bezdrátových sítí je naštěstí poměrně snadné a útočníky lze odradit pomocí několika jednoduchých úkonů.

Klasický wardriving je pasivní, využitý software pouze zaznamenává informace o dostupných WiFi sítích a kombinuje je s informací o poloze. V mnoha případech vytváří mapu pokrytí oblasti WiFi.

Aktivní wardriving je už trochu ošemetnější, vyžaduje připojení k přístupovému bodu a v některých zemích může být nelegální. Ve většině případů je, ale někde na hraně - v USA by například porušení zákona bylo teprve to, kdyby wardriver opravdu použil nějakou ze služeb přístupového bodu, nebo se jeho prostřednictvím připojil na místní síť či Internet.

#### **4.4 Warchalking**

Warchalking je činnost, při které se kreslením symbolů na chodníky a na zdi upozorňuje na přítomnost AP. Značky sdělují přítomnost otevřených a uzavřených AP, nastavení SSID, údaje o přenosové rychlosti nebo kontaktní údaje[5]. Warchalker je člověk, která má svůj laptop (pda, pc) s příslušným softwarem a hardwarem a hledá dostupné bezdrátové sítě. Při hledání se pohybuje pomocí vlastních nohou a má u sebe prostředky pro malování informativních symbolů. Získané informace poskytuje pro veřejnost a každý může využít zdarma sítě firem nebo jednotlivců k přístupu na internet. Nezabezpečené bezdrátové sítě využívají lidé i pro rozesílání spamů (nevyžádaná komerční pošta).



Obr. 7: Warchalking – ukázka symbolů[5]

Otevřený přístup – je uvedeno SSID a rychlost

Uzavřený přístup – je uvedeno SSID

Omezený přístup – je uvedeno SSID, kontaktní adresa a rychlost

## 5 SOFTWARE PRO MONITORING WIFI SÍTÍ

Při budování bezdrátových sítí je důležité dodržovat určité zásady. Jednou z nich je předcházení vzájemného rušení sítí v blízkém okolí. V oblastech, které jsou více obydlené je pravděpodobnost výskytu dalších WiFi sítí velmi velká.

Pro monitoring WiFi sítí se používá příslušný software. Základní vyhledávání dostupných sítí i jejich parametrů je zpravidla zabudováno i v podpůrných programech, které jsou součástí síťové karty nebo operačního systému. Využitím příslušného softwaru získáme více informací o dané WiFi síti. Obsahem kapitoly je popis několika nejznámějších programů pro detekci WiFi sítí a jejich stručný popis.

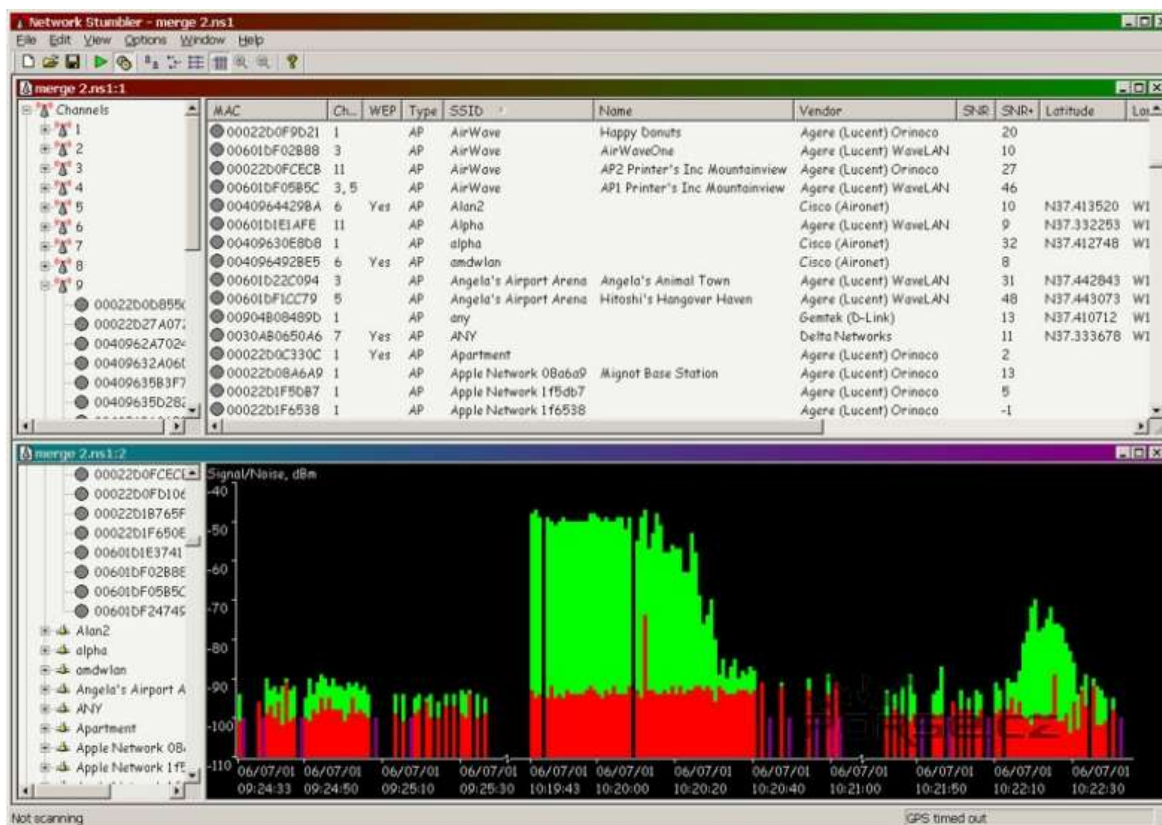
### 5.1 NetStumbler 0.4.0

Jednoduchý program pro sledování a detekci WiFi sítí. Podporuje bezdrátové karty 802.11b, 802.11g a 802.11a. Sledovat lze sílu signálu AP i jednotlivých počítačů – klientů. Výsledky se znázorňují jak číselně i graficky. Funkce ozvučení je přínosem při směřování antény. Program přehledně třídí dle rádiového kanálu, na kterém WiFi síť funguje nebo podle názvu SSID. Dává přehled o obsazenosti jednotlivých rádiových kanálů, tím umožňuje si vybrat volný rádiový kanál a zajistit si lepší dostupnost signálu. Zobrazuje Media Access Control (dále jen MAC) adresu adaptérů, rychlost, typ, výrobce, druh šifrovacího protokolu a spoustu dalších zajímavých a potřebných informací. Zajímavostí je Global Positioning System (dále jen GPS) modul, který pomáhá s lokalizací WiFi sítí, případně různých zdrojů rušení. Program je přehledný, snadně ovladatelný a je v češtině.

|                        |                 |
|------------------------|-----------------|
| <b>Velikost v (MB)</b> | <b>1,3</b>      |
| <b>Licence</b>         | <b>freeware</b> |
| <b>Lokalizace</b>      | <b>Čeština</b>  |
| <b>Operační systém</b> | <b>XP/Vista</b> |

Tabulka 3: Shrnutí specifikací programu NetStumbler





Obr. 8: Vizualizace programu NetStumbler[14]

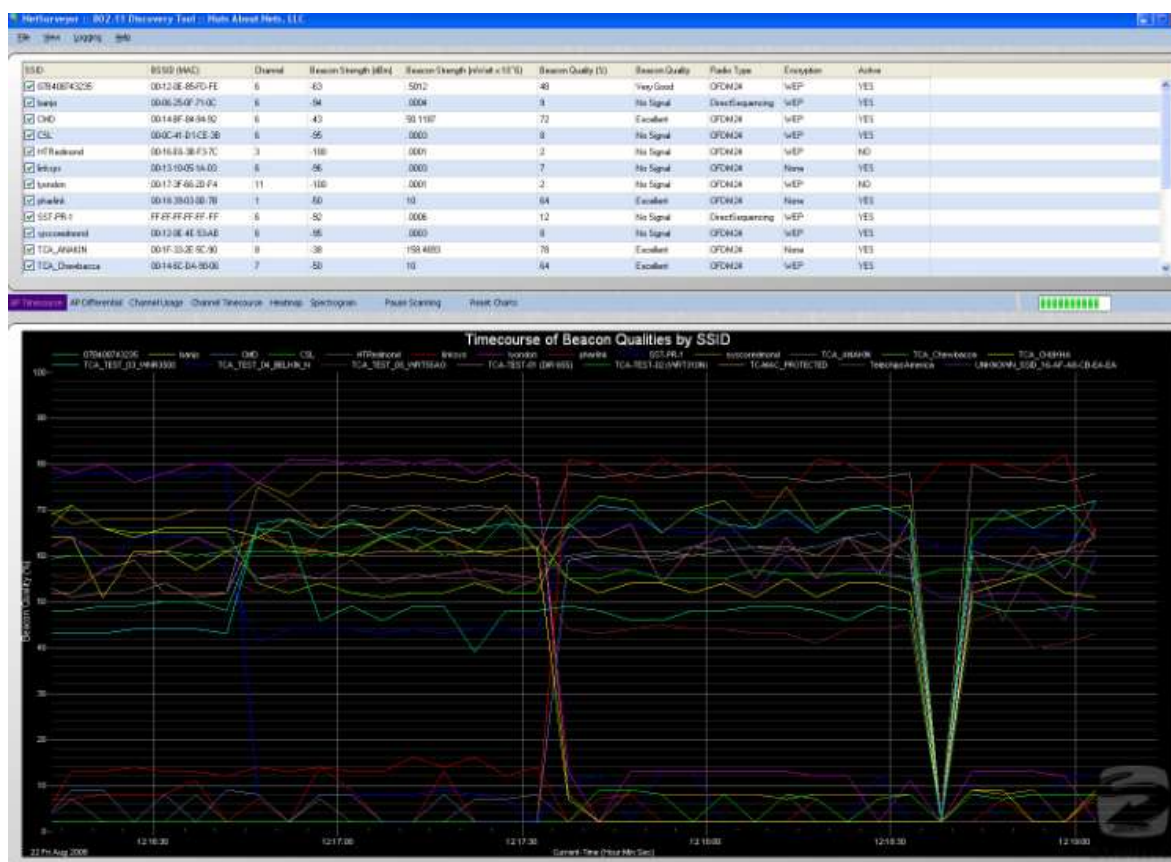
## 5.2 NetSurveyor 2.0

NetSurveyor je program pro monitoring bezdrátových sítí, které jsou založeny na standardu 802.11. Aplikace zjišťuje informace o všech bezdrátových sítích v reálném čase. Umožňuje najít přítomné sítě v okolí a podle toho postavit svou vlastní síť tak, aby nebyla rušena. NetSurveyor je pomůcka k vytvoření a nastavení parametrů vlastní sítě. Pro zobrazení dat jsou k dispozici diagnostické přehledy a grafy. Data je možné nahrávat v určitých intervalech a později přehrávat. Vygenerované zprávy se ukládají do formátu PDF.

|                        |   |
|------------------------|---|
| <b>Velikost v (MB)</b> | <b>8,07</b>                                   |
| <b>Licence</b>         | <b>freeware</b>                               |
| <b>Lokalizace</b>      | <b>Angličtina</b>                             |
| <b>Operační systém</b> | <b>Windows 2008/2000/XP/Vista 32/Vista 64</b> |

Tabulka 4: Tabulka shrnutí specifikací programu NetSurveyor





Obr. 9: Vizualizace programu NetSurveyor[14]

### 5.3 Xirrus WiFi Inspector

Xirrus WiFi Inspector je k dispozici v podobě samostatného programu nebo i miniaplikace pro nástrojovou lištu Windows Vista. Zajišťuje kompletní správu bezdrátových WiFi sítí. Vyhledává bezdrátové sítě v okolí a vypisuje přehled jejich parametrů (název sítě, adaptér, sílu signálu, zabezpečení sítě). Sílu signálu je možné sledovat pomocí grafu nebo na animovaném radaru.

|                        |                                     |
|------------------------|-------------------------------------|
| <b>Velikost v (MB)</b> | <b>22,09</b>                        |
| <b>Licence</b>         | <b>freeware</b>                     |
| <b>Lokalizace</b>      | <b>Angličtina</b>                   |
| <b>Systém</b>          | <b>Windows XP/Vista 32/Vista 64</b> |

Tabulka 5: Shrnutí specifikací programu Xirrus WiFi Inspector



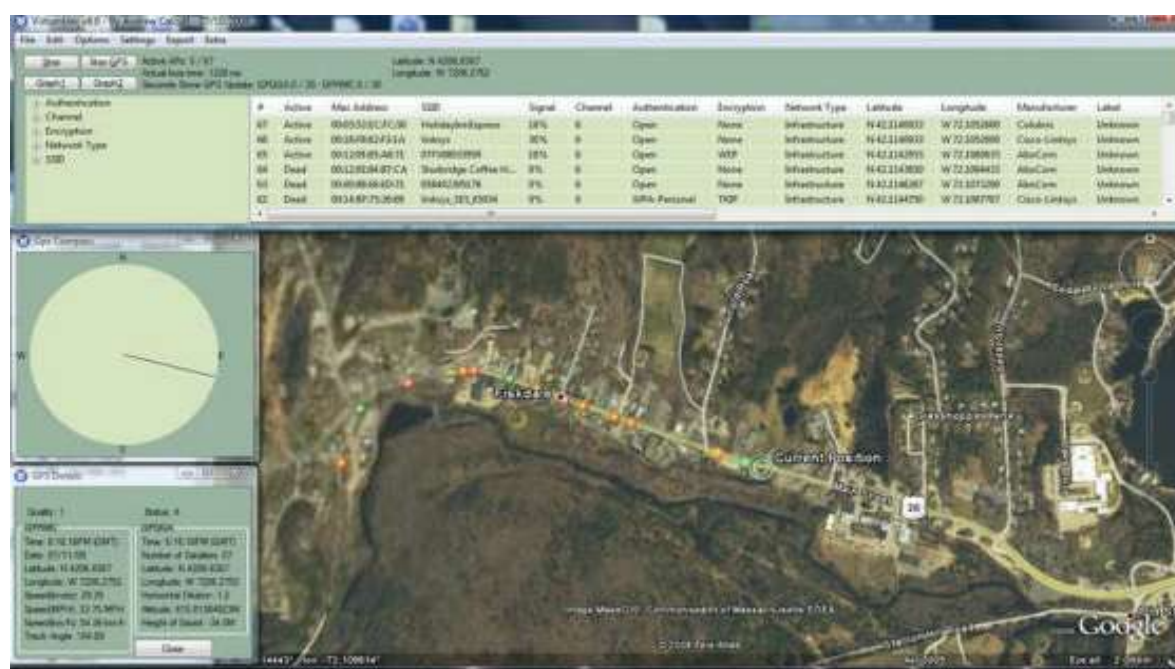
Obr. 10: Vizualizace programu Xirrus Wi-Fi Inspector [14]

## 5.4 Vistumbler 9.8

Vistumbler slouží k vyhledávání bezdrátových sítí ve Windows Vista a Windows 7. Přehledně zobrazuje dostupné bezdrátové WiFi sítě v reálném čase. Dokáže zjistit, na jakém rádiovém kanálu daná síť vysílá, její úroveň signálu, zabezpečení, SSID, MAC nebo AP. Program podporuje GPS moduly a dostupné AP je možné zobrazit v satelitní mapě aplikace Google Earth. Import i export vyhledaných AP je možný do souborů typu TXT, VS1 a VSZ. Vistumbler je dobrým pomocníkem při nastavování vlastní bezdrátové sítě.

|                        |                                |
|------------------------|--------------------------------|
| <b>Velikost v (MB)</b> | <b>2,72</b>                    |
| <b>Licence</b>         | <b>freeware</b>                |
| <b>Lokalizace</b>      | <b>Čeština</b>                 |
| <b>Systém</b>          | <b>Win 7/Vista 32/Vista 64</b> |

Tabulka 6: Shrnutí specifikací programu Vistumbler



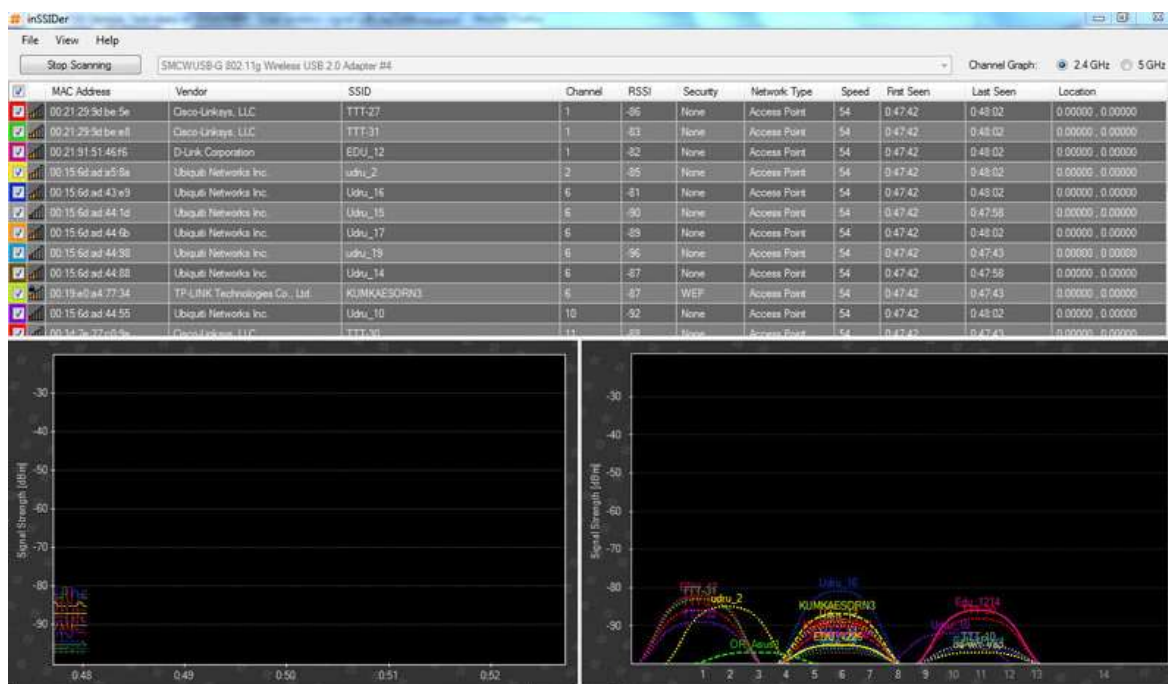
Obr. 11: Vizualizace programu Vistumbler[15]

## 5.5 InSSIDer

InSSIDer je volně dostupný WiFi síťový skener. Vyhledává informace o dostupných WiFi sítích v okolí. Graficky vykresluje sílu signálu v závislosti na zvoleném rádiovém kanálu. Zobrazuje časový průběh intenzity jednotlivých signálů. Při stavbě bezdrátové sítě je ideální zvolit nepoužívaný rádiový kanál. Program vypisuje informace o přenosových rychlostech, zabezpečení, síle signálu, překrývání sítí a umožňuje identifikovat volnější rádiový kanál. InSSIDer je vhodným pomocníkem pro zjištění optimálního místa pro připojení.

|                        |                         |
|------------------------|-------------------------|
| <b>Velikost v (MB)</b> | <b>1,56</b>             |
| <b>Licence</b>         | <b>freeware</b>         |
| <b>Lokalizace</b>      | <b>Čeština</b>          |
| <b>Systém</b>          | <b>Windows XP/Vista</b> |

Tabulka 7: Shrnutí specifikací programu InSSIDer



Obr. 12: Vizualizace programu InSSIDer[16]

## 5.6 Wireshark

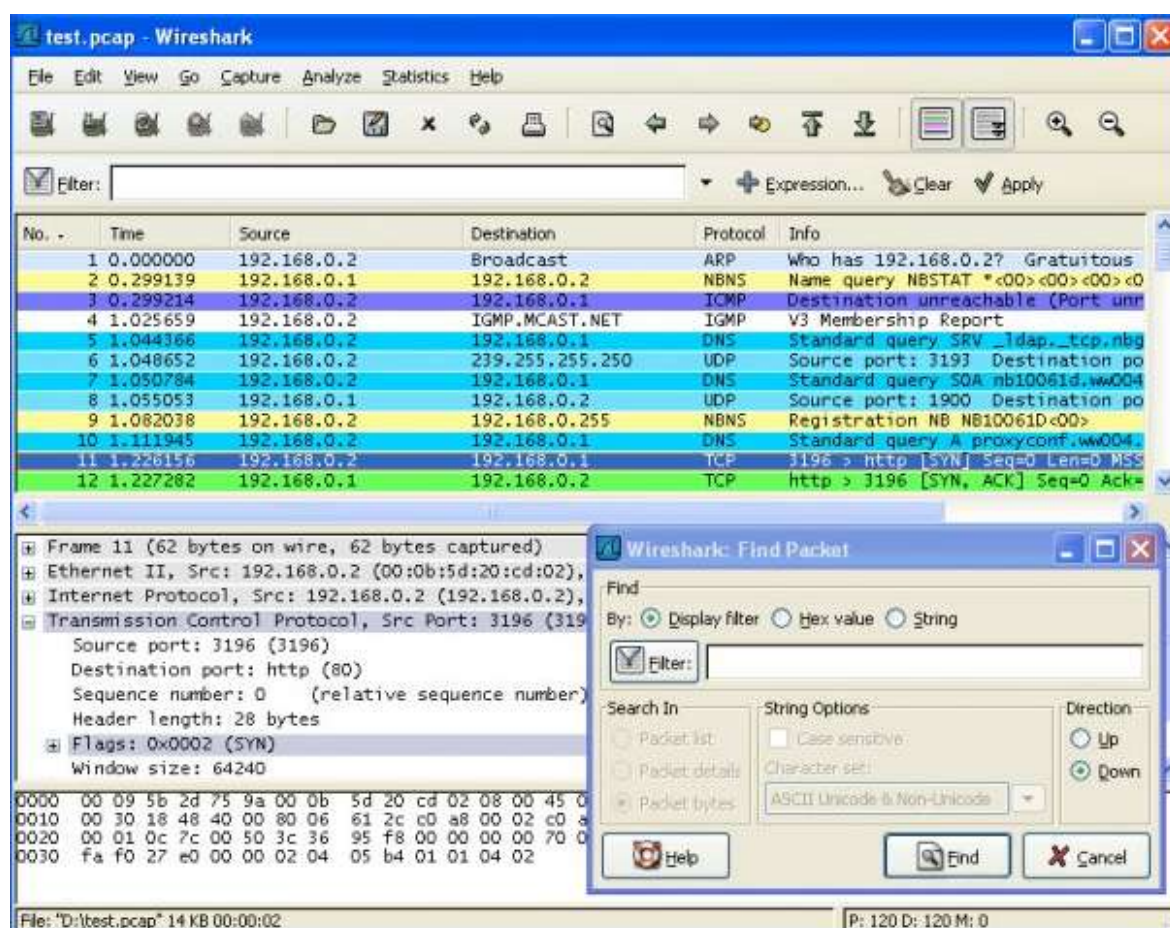
Wireshark je výkonný nástroj pro zachytávání komunikace, která prochází skrz síťová rozhraní počítače (Ethernet, The Institute of Electrical and Electronics Engineers 802.11, Bluetooth, USB, Token Ring a další). Podrobně analyzuje data protékající sítími nebo uložené na disku. Umožňuje snadno rozpoznat navázání spojení, ukládat komunikaci, která probíhá na síťové kartě, dekodovat paket a ukázat v původním zobrazení. Hlavními vlastnostmi je schopnost dešifrovat protokoly (Internet Protocol Security (dále jen IPSec), WiFi Protected Access, Wired Equivalent Privacy), vylepšené analyzování Voice over



Internet Protocol (dále jen VoIP) komunikací, možnost exportu dat. Výhodou je, že je šířen pod licencí GNU/GPL (GNU's Not Unix/General Public License, licence pro volný software).

|                        |   |
|------------------------|---|
| <b>Velikost v (MB)</b> | <b>18</b>                                   |
| <b>Licence</b>         | <b>freeware</b>                             |
| <b>Lokalizace</b>      | <b>Angličtina</b>                           |
| <b>Systém</b>          | <b>Windows 2000/2003/2008/XP/Vista/Win7</b> |

Tabulka 8: Shrnutí specifikací programu Wireshark



Obr. 13: Vizualizace programu Wireshark[17]

## 5.7 Easy WiFi Radar 1.05

Easy WiFi Radar je volně dostupný nástroj k hledání WiFi sítí v okolí. Vyhledává bezdrátové sítě, které následně zobrazuje na radaru. Úkolem programu je připojit se k internetu zadarmo. Na radaru označují červené body chráněné hotspoty. Zelené znamenají bezplatné připojení k internetu. Žlutá označuje to samé co zelená, ale se slabým signálem.

|                        |                        |
|------------------------|------------------------|
| <b>Velikost v (MB)</b> | <b>2,1</b>             |
| <b>Licence</b>         | <b>freeware</b>        |
| <b>Lokalizace</b>      | <b>Angličtina</b>      |
| <b>System</b>          | <b>Windows 2000/XP</b> |

Tabulka 9: Shrnutí specifikací programu Easy WiFi Radar



Obr. 14: Vizualizace programu Easy WiFi Radar[18]

## **II. PRAKTICKÁ ČÁST**

## **6 PRŮZKUM ZABEZPEČENÍ WIFI SÍTÍ WARDRIVINGEM V LOKALITĚ JIŽNÍ SVAHY**

V současné době jsou informace cenná nehmotná aktiva. Mnoho domácích uživatelů, kteří využívají bezdrátové připojení, si neuvědomují důležitost bezpečnosti informací, dat. Spousta sítí, tak zůstává nezabezpečena nebo zabezpečena nedostatečně. Uživatelé umožňují volný přístup ke svým aktivům.

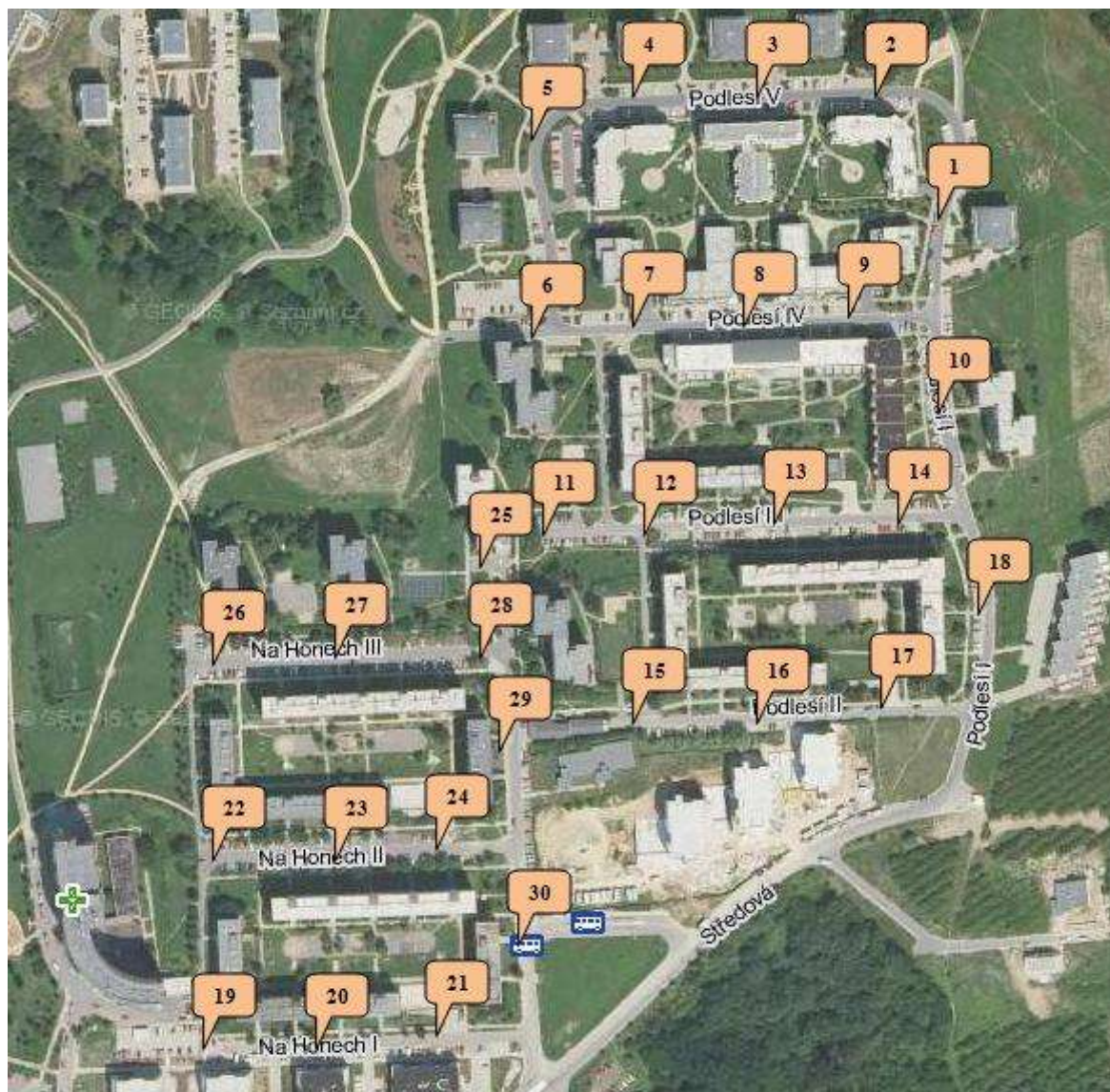
Monitoring WiFi sítí je proveden ve vymezené lokalitě na Jižních Svazích. Jižní Svahy je sídliště a pro wardrivery je to ideální místo pro hledání sítí nebo provedení útoku na síť. Výstupem průzkumu je vyhodnocení naměřených dat zabezpečení WiFi sítí v zadané lokalitě.

### **6.1 Použité prostředky**

V zadané lokalitě jsou vybrána stanoviště, ve kterých probíhalo monitorování sítí. Měření na jednotlivých stanovištích probíhalo v osobním automobilu. Rozmístění jednotlivých stanovišť je v závislosti na možnosti zastavení automobilu v místě, tak aby neohrožovalo provoz v dané lokalitě. K měření byl použit laptop, který podporuje standard 802.11b/g. Součástí je interní anténa typu Atheros AR5007EG. Má dosah 46 m v uzavřeném prostoru a 96 m ve volném prostranství. Software pro hledání sítí byl vybrán InSSIDer, který je pro monitoring volně dostupný (viz kapitola 5). Monitorovalo se ve dnech pondělí až čtvrtek mezi 19.00 a 22.00 hodinou. Časově rozpětí je stanoveno z hlediska větší pravděpodobnosti připojení uživatelů k síti. Podmínky byly stanoveny, aby odpovídali průměrnému člověku, který se pokusí o vyhledání sítě a případné připojení k síti.



## 6.2 Mapa jednotlivých stanovišť



Obr. 15: Mapa stanovišť pro monitoring WiFi sítí

## 6.3 Data naměřená v jednotlivých stanovištích

Tabulky zobrazují shrnutí dat z každého stanoviště, ve kterém bylo provedeno monitorování WiFi sítí. Tabulka prezentuje počet sítí zachycených na daném stanovišti při 1. a 2. měření a jejich typ šifrování. Součástí je procentuální podíl z celkového počtu sítí v každém stanovišti, viz. tab.10 až 39.

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 0             | 0              | 0            | 0              |
| WEP           | 4             | 30,8           | 3            | 37,5           |
| WPA-TKIP      | 5             | 38,4           | 4            | 50             |
| RSNA-CCMP     | 4             | 30,8           | 1            | 12,5           |
|               | $\Sigma = 13$ |                | $\Sigma = 8$ |                |

Tabulka 10: Souhrn dat ze stanoviště č. 1

| Typ šifrování | 1. měření    |                | 2. měření    |                |
|---------------|--------------|----------------|--------------|----------------|
|               | počet sítí   | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 1            | 20             | 0            | 0              |
| WEP           | 0            | 0              | 1            | 11,2           |
| WPA-TKIP      | 3            | 60             | 4            | 44,4           |
| RSNA-CCMP     | 1            | 20             | 4            | 44,4           |
|               | $\Sigma = 5$ |                | $\Sigma = 9$ |                |

Tabulka 11: Souhrn dat ze stanoviště č. 2

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 2             | 12,5           | 2             | 15,4           |
| WEP           | 2             | 12,5           | 4             | 30,8           |
| WPA-TKIP      | 3             | 18,8           | 2             | 15,4           |
| RSNA-CCMP     | 9             | 56,25          | 5             | 38,4           |
|               | $\Sigma = 16$ |                | $\Sigma = 13$ |                |

Tabulka 12: Souhrn dat ze stanoviště č. 3

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 2             | 9,1            | 0             | 0              |
| WEP           | 5             | 22,7           | 0             | 0              |
| WPA-TKIP      | 8             | 36,4           | 8             | 57,1           |
| RSNA-CCMP     | 7             | 31,8           | 6             | 42,9           |
|               | $\Sigma = 22$ |                | $\Sigma = 14$ |                |

Tabulka 13: Souhrn dat ze stanoviště č. 4

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 1             | 9,1            | 3             | 20             |
| WEP           | 3             | 27,3           | 4             | 26,7           |
| WPA-TKIP      | 4             | 36,3           | 3             | 20             |
| RSNA-CCMP     | 3             | 27,3           | 5             | 33,3           |
|               | $\Sigma = 11$ |                | $\Sigma = 15$ |                |

Tabulka 14: Souhrn dat ze stanoviště č. 5

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 3             | 15,8           | 1            | 12,5           |
| WEP           | 4             | 21,0           | 3            | 37,5           |
| WPA-TKIP      | 3             | 15,8           | 1            | 12,5           |
| RSNA-CCMP     | 9             | 47,4           | 3            | 37,5           |
|               | $\Sigma = 19$ |                | $\Sigma = 8$ |                |

Tabulka 15: Souhrn dat ze stanoviště č. 6

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 0             | 0              | 1            | 11,1           |
| WEP           | 2             | 20             | 2            | 22,3           |
| WPA-TKIP      | 4             | 40             | 3            | 33,3           |
| RSNA-CCMP     | 4             | 40             | 3            | 33,3           |
|               | $\Sigma = 10$ |                | $\Sigma = 9$ |                |

Tabulka 16: Souhrn dat ze stanoviště č. 7

| Typ šifrování | 1. měření    |                | 2. měření    |                |
|---------------|--------------|----------------|--------------|----------------|
|               | počet sítí   | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 1            | 11,2           | 2            | 22,2           |
| WEP           | 3            | 33,3           | 3            | 33,4           |
| WPA-TKIP      | 2            | 22,2           | 2            | 22,2           |
| RSNA-CCMP     | 3            | 33,3           | 2            | 22,2           |
|               | $\Sigma = 9$ |                | $\Sigma = 9$ |                |

Tabulka 17: Souhrn dat ze stanoviště č. 8

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 1             | 10             | 1            | 16,7           |
| WEP           | 5             | 50             | 5            | 83,3           |
| WPA-TKIP      | 2             | 20             | 0            | 0              |
| RSNA-CCMP     | 2             | 20             | 0            | 0              |
|               | $\Sigma = 10$ |                | $\Sigma = 6$ |                |

Tabulka 18: Souhrn dat ze stanoviště č. 9

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 2             | 7,7            | 1             | 6,25           |
| WEP           | 9             | 34,6           | 4             | 25             |
| WPA-TKIP      | 5             | 19,2           | 3             | 18,75          |
| RSNA-CCMP     | 10            | 38,5           | 8             | 50             |
|               | $\Sigma = 26$ |                | $\Sigma = 16$ |                |

Tabulka 19: Souhrn dat ze stanoviště č. 10

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 3             | 12,5           | 0            | 0              |
| WEP           | 5             | 20,8           | 0            | 0              |
| WPA-TKIP      | 7             | 29,2           | 0            | 0              |
| RSNA-CCMP     | 9             | 37,5           | 0            | 0              |
|               | $\Sigma = 24$ |                | $\Sigma = 0$ |                |

Tabulka 20: Souhrn dat ze stanoviště č. 11

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 1             | 9,1            | 2             | 5,6            |
| WEP           | 5             | 45,5           | 6             | 16,7           |
| WPA-TKIP      | 2             | 18,2           | 13            | 36,1           |
| RSNA-CCMP     | 3             | 27,2           | 15            | 41,6           |
|               | $\Sigma = 11$ |                | $\Sigma = 36$ |                |

Tabulka 21: Souhrn dat ze stanoviště č. 12

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 0             | 0              | 0            | 0              |
| WEP           | 3             | 30             | 0            | 0              |
| WPA-TKIP      | 3             | 30             | 2            | 22,2           |
| RSNA-CCMP     | 4             | 40             | 7            | 77,8           |
|               | $\Sigma = 10$ |                | $\Sigma = 9$ |                |

Tabulka 22: Souhrn dat ze stanoviště č. 13

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 1             | 8,3            | 0             | 0              |
| WEP           | 1             | 8,3            | 6             | 40             |
| WPA-TKIP      | 2             | 16,7           | 1             | 6,7            |
| RSNA-CCMP     | 8             | 66,6           | 8             | 53,3           |
|               | $\Sigma = 12$ |                | $\Sigma = 15$ |                |

Tabulka 23: Souhrn dat ze stanoviště č. 14

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 1             | 5,3            | 6             | 17,6           |
| WEP           | 5             | 26,3           | 11            | 32,4           |
| WPA-TKIP      | 5             | 26,3           | 6             | 17,6           |
| RSNA-CCMP     | 8             | 42,1           | 11            | 32,4           |
|               | $\Sigma = 19$ |                | $\Sigma = 34$ |                |

Tabulka 24: Souhrn dat ze stanoviště č. 15

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 0             | 0              | 0             | 0              |
| WEP           | 2             | 15,4           | 8             | 26,7           |
| WPA-TKIP      | 3             | 23,1           | 7             | 23,3           |
| RSNA-CCMP     | 8             | 61,5           | 15            | 50             |
|               | $\Sigma = 13$ |                | $\Sigma = 30$ |                |

Tabulka 25: Souhrn dat ze stanoviště č. 16

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 2             | 10             | 0            | 0              |
| WEP           | 7             | 35             | 4            | 66,6           |
| WPA-TKIP      | 3             | 15             | 1            | 16,7           |
| RSNA-CCMP     | 8             | 40             | 1            | 16,7           |
|               | $\Sigma = 20$ |                | $\Sigma = 6$ |                |

Tabulka 26: Souhrn dat ze stanoviště č. 17

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 4             | 18,2           | 0            | 0              |
| WEP           | 3             | 13,6           | 1            | 14,3           |
| WPA-TKIP      | 6             | 27,3           | 0            | 0              |
| RSNA-CCMP     | 9             | 40,9           | 6            | 85,7           |
|               | $\Sigma = 22$ |                | $\Sigma = 7$ |                |

Tabulka 27: Souhrn dat ze stanoviště č. 18

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 1             | 4,2            | 2             | 6,25           |
| WEP           | 14            | 58,3           | 17            | 53,1           |
| WPA-TKIP      | 3             | 12,5           | 2             | 6,25           |
| RSNA-CCMP     | 6             | 25             | 11            | 34,4           |
|               | $\Sigma = 24$ |                | $\Sigma = 32$ |                |

Tabulka 28: Souhrn dat ze stanoviště č. 19

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 2             | 11,8           | 2            | 33,3           |
| WEP           | 7             | 41,2           | 2            | 33,3           |
| WPA-TKIP      | 1             | 5,8            | 1            | 16,7           |
| RSNA-CCMP     | 7             | 41,2           | 1            | 16,7           |
|               | $\Sigma = 17$ |                | $\Sigma = 6$ |                |

Tabulka 29: Souhrn dat ze stanoviště č. 20

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 1             | 8,3            | 1             | 9,1            |
| WEP           | 6             | 50             | 1             | 9,1            |
| WPA-TKIP      | 2             | 16,7           | 4             | 36,4           |
| RSNA-CCMP     | 3             | 25             | 5             | 45,4           |
|               | $\Sigma = 12$ |                | $\Sigma = 11$ |                |

Tabulka 30: Souhrn dat ze stanoviště č. 21

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 3             | 8,1            | 1             | 3,6            |
| WEP           | 9             | 24,4           | 7             | 25             |
| WPA-TKIP      | 7             | 18,9           | 6             | 21,4           |
| RSNA-CCMP     | 18            | 48,6           | 14            | 50             |
|               | $\Sigma = 37$ |                | $\Sigma = 28$ |                |

Tabulka 31: Souhrn dat ze stanoviště č. 22

| Typ šifrování | 1. měření    |                | 2. měření    |                |
|---------------|--------------|----------------|--------------|----------------|
|               | počet sítí   | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 0            | 0              | 0            | 0              |
| WEP           | 1            | 16,7           | 0            | 0              |
| WPA-TKIP      | 0            | 0              | 0            | 0              |
| RSNA-CCMP     | 5            | 83,3           | 3            | 100            |
|               | $\Sigma = 6$ |                | $\Sigma = 3$ |                |

Tabulka 32: Souhrn dat ze stanoviště č. 23

| Typ šifrování | 1. měření    |                | 2. měření    |                |
|---------------|--------------|----------------|--------------|----------------|
|               | počet sítí   | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 0            | 0              | 1            | 25             |
| WEP           | 2            | 33,3           | 2            | 50             |
| WPA-TKIP      | 0            | 0              | 0            | 0              |
| RSNA-CCMP     | 4            | 66,7           | 1            | 25             |
|               | $\Sigma = 6$ |                | $\Sigma = 4$ |                |

Tabulka 33: Souhrn dat ze stanoviště č. 24

| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 1             | 4,5            | 3             | 10,7           |
| WEP           | 4             | 18,2           | 6             | 21,4           |
| WPA-TKIP      | 9             | 40,9           | 5             | 17,9           |
| RSNA-CCMP     | 8             | 36,4           | 14            | 50             |
|               | $\Sigma = 22$ |                | $\Sigma = 28$ |                |

Tabulka 34: Souhrn dat ze stanoviště č. 25



| Typ šifrování | 1. měření     |                | 2. měření     |                |
|---------------|---------------|----------------|---------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 9             | 27,3           | 4             | 21,1           |
| WEP           | 4             | 12,1           | 2             | 10,5           |
| WPA-TKIP      | 6             | 18,2           | 3             | 15,8           |
| RSNA-CCMP     | 14            | 42,4           | 10            | 52,6           |
|               | $\Sigma = 33$ |                | $\Sigma = 19$ |                |

Tabulka 35: Souhrn dat ze stanoviště č. 26

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 1             | 9,1            | 2            | 25             |
| WEP           | 3             | 27,3           | 2            | 25             |
| WPA-TKIP      | 2             | 18,2           | 2            | 25             |
| RSNA-CCMP     | 5             | 45,4           | 2            | 25             |
|               | $\Sigma = 11$ |                | $\Sigma = 8$ |                |

Tabulka 36: Souhrn dat ze stanoviště č. 27

| Typ šifrování | 1. měření     |                | 2. měření    |                |
|---------------|---------------|----------------|--------------|----------------|
|               | počet sítí    | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 2             | 20             | 3            | 50             |
| WEP           | 3             | 30             | 2            | 33,3           |
| WPA-TKIP      | 2             | 20             | 1            | 16,7           |
| RSNA-CCMP     | 3             | 30             | 0            | 0              |
|               | $\Sigma = 10$ |                | $\Sigma = 6$ |                |

Tabulka 37: Souhrn ze stanoviště č. 28

| Typ šifrování | 1. měření    |                | 2. měření    |                |
|---------------|--------------|----------------|--------------|----------------|
|               | počet sítí   | počet sítí v % | počet sítí   | počet sítí v % |
| ŽÁDNÉ         | 0            | 0              | 1            | 14,3           |
| WEP           | 3            | 60             | 2            | 28,6           |
| WPA-TKIP      | 1            | 20             | 1            | 14,3           |
| RSNA-CCMP     | 1            | 20             | 3            | 42,8           |
|               | $\Sigma = 5$ |                | $\Sigma = 7$ |                |

Tabulka 38: Souhrn dat ze stanoviště č. 29

| Typ šifrování | 1. měření    |                | 2. měření     |                |
|---------------|--------------|----------------|---------------|----------------|
|               | počet sítí   | počet sítí v % | počet sítí    | počet sítí v % |
| ŽÁDNÉ         | 2            | 28,6           | 2             | 10,6           |
| WEP           | 3            | 42,8           | 6             | 31,6           |
| WPA-TKIP      | 0            | 0              | 5             | 26,2           |
| RSNA-CCMP     | 2            | 28,6           | 6             | 31,6           |
|               | $\Sigma = 7$ |                | $\Sigma = 19$ |                |

Tabulka 39: Souhrn dat ze stanoviště č. 30

## 6.4 Vyhodnocení naměřených dat

Měření bylo umístěno na 30 stanovištích v zadané lokalitě. Získaná data wardrivingem byla exportována do souboru v excelu, který je přílohou diplomové práce. Protože dosah některých sítí zasahoval do více stanovišť, byla data upravena tak, že každá síť je pouze jednou, aby nedošlo ke zkreslení výsledku. Celkový počet monitorovaných sítí u 1. měření je 462 sítí, při opakovaném monitoringu bylo zachyceno 415 sítí. Grafy zobrazují procentuální zabezpečení WiFi sítí jednotlivými protokoly. Protože protokol WEP lze prolomit za necelých 6 minut, nepovažuje se v současné době za téměř žádnou ochranu pro WiFi síť. Ačkoliv byl protokol WPA prolomen zůstává stále kvalitní ochranou pro zabezpečení WiFi. WPA2 (RSNA-CCMP) zůstává nejbezpečnějším protokolem.

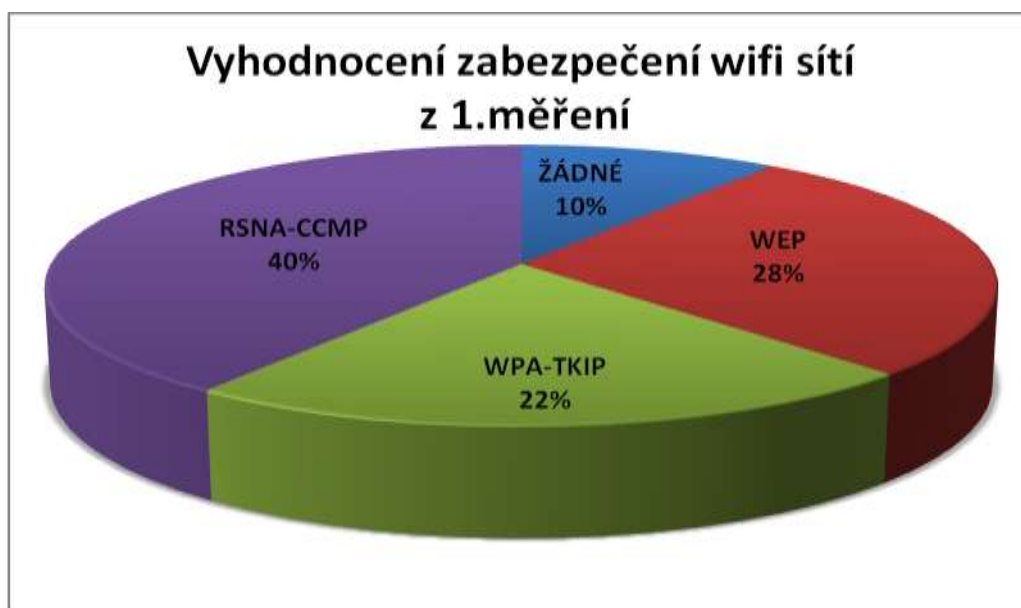
Průzkumem zabezpečení WiFi v zadané lokalitě na Jižních Svazích bylo zjištěno, že 37-38 % (zabezpečení Žádné + WEP) bezdrátových sítí je nezabezpečeno a jsou snadno přístupné narušitelům. 62-63 % (WPA + WPA2) bezdrátových sítí je zabezpečeno kvalitním šifrovacím protokolem.

V posledních letech bylo prezentováno, že více jak 60 % bezdrátových sítí je nekvalitně zabezpečeno. Na základě výsledku průzkumu, lze říci, že v současné době uživatelé bezdrátových sítí si více uvědomují důležitost ochrany informací a využívají kvalitní šifrovací protokoly při bezdrátovém připojení k síti.

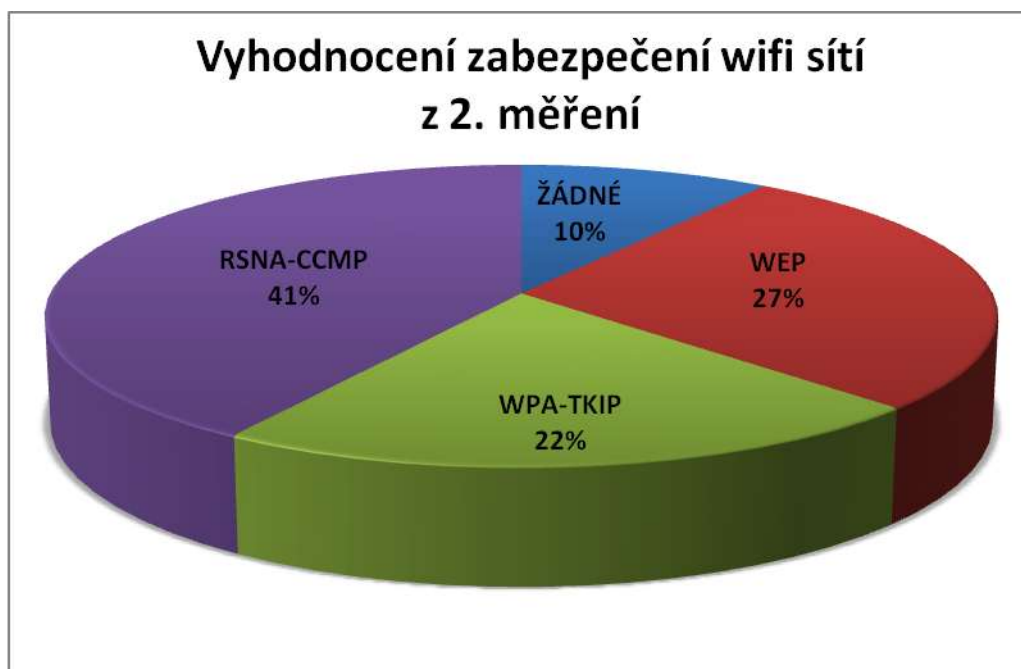
| Typ šifrování | 1. měření      |                | 2. měření      |                |
|---------------|----------------|----------------|----------------|----------------|
|               | počet sítí     | počet sítí v % | počet sítí     | počet sítí v % |
| ŽÁDNÉ         | 47             | 10,2           | 41             | 9,8            |
| WEP           | 127            | 27,5           | 114            | 27,5           |
| WPA-TKIP      | 103            | 22,3           | 90             | 21,7           |
| RSNA-CCMP     | 185            | 40             | 170            | 41             |
|               | $\Sigma = 462$ |                | $\Sigma = 415$ |                |

Tabulka 40: Shrnutí počtu monitorovaných sítí a jejich zabezpečení





Obr. 16: Graf vyhodnocení dat z 1. měření



Obr. 17: Graf vyhodnocení dat z 2. měření

## 7 MANUÁL K HLEDÁNÍ VOLNĚJŠÍHO PŘENOSOVÉHO KANÁLU

### 7.1 Wi-Spy 2.4i

Wi-Spy 2.4i je profesionální spektrální analyzátor pro WiFi 2.4 GHz s rozhraním USB a pracující v reálném čase i ze záznamu, se spoustou dalších možností. Zejména bezkonkurenční cenou je Wi-Spy ideální volbou pro každého síťáře. Wi-Spy je nástroj speciálně vyvinutý pro vyhledávání volného pásma a odstraňování problémů s bezdrátovými sítěmi WiFi/GSM. Chanalyzer Lite - funguje jen s příslušným zařízením, Chanalyzer Lite lze částečně použít s jakoukoliv kartou jako WiFi skener nebo jako volnou utilitu inSSIDer.[24]

V obchodních, kancelářských komplexech a v centrech měst je zarušení pásma 2,4 GHz největší. Pro analýzu okolí a řešení problémů je vhodný Wi-Spy 2.4i. Mapuje veškerou radiovou aktivitu nejen v podobě Wi-Fi, ale i bluetooth, bezdrátové telefony, mikrovlnky a jiná 2,4 GHz zařízení. Wi-Spy vše graficky zobrazuje na monitoru počítače, je kompatibilní s pc.



Obr. 18: Zapojení Wi-Spy přes USB do laptopu[23]

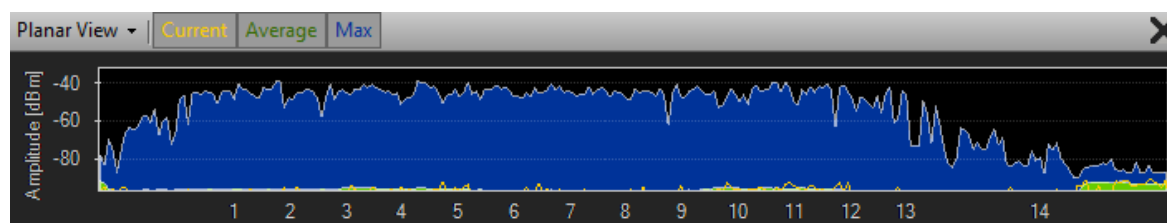
| Typ                  | Wi-Spy 2.4i        |
|----------------------|--------------------|
| Anténa               | jen interní        |
| Frekvenční rozsah    | 2.400 to 2.495 GHz |
| Frekvenční rozlišení | 373 KHz            |
| Šířka pásma filtru   | 429 KHz            |
| Rozsah amplitudy     | -102 to -6.5 dBm   |
| Rozlišení amplitudy  | 0.5 dBm            |
| Software             | Chanalyzer Lite    |

Tabulka 41: Specifikace Wi-Spy 2.4i

## 7.2 Nástroje (prvky) programu Chanalyzer Lite

### 7.2.1 Planar zobrazení (Planar view)

Žlutá čára představuje aktuální amplitudu, zelená je průměrná amplituda a modrá je maximální amplituda, které nastaly v době vybraného snímku. Kliknutím na tlačítka aktuální (current), průměrná (average) nebo maximální (max) amplituda přepínáme zobrazení odpovídající stopy. Pro sledování konkrétní frekvence je k dispozici nástroj Marker (ikona tužky v horní liště). Po umístění značky v dané frekvenci se v tabulce začne zobrazovat aktuální, průměrná a maximální amplituda u každé značky.



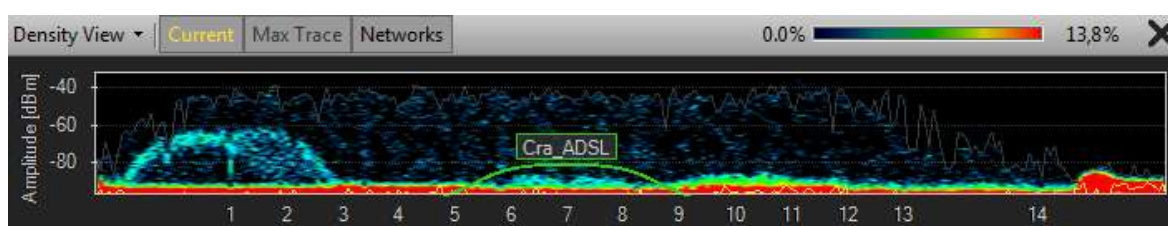
Obr. 19: Planar view

| Markers   |         |         |       |
|-----------|---------|---------|-------|
| Frequency | Current | Average | Max   |
| 2 449,58  | -99     | -98,6   | -46,0 |
| 2 462,26  | -99     | -97,4   | -44,5 |
| 2 462,26  | -99     | -97,4   | -44,5 |

Obr. 20: Markers

### 7.2.2 Density zobrazení (Density view)

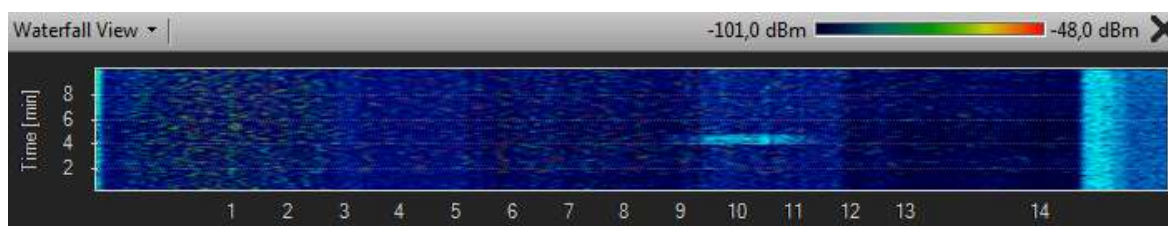
Density view je mapa hustoty aktivity bezdrátového vysílání. Nezobrazuje aktuální amplitudy každé frekvence, ale zobrazuje hustotu vysílání na dané frekvenci v daný čas. Barvy prezentují hustotu namísto amplitudy. Modrá znamená nízkou hustotu, červená vysokou. Čím více aktivity, tím více se objeví červené. V horní části je užitečná legenda, která zobrazuje, jak přehuštěné jsou body na základě jejich barvy. Pro charakteristiku konkrétního frekvenčního bodu je funkce „inspektor“, ikona je umístěna v horní liště v podobě tlačítka s lupou.



Obr. 21: Density view

### 7.2.3 Waterfall zobrazení (Waterfall view)

Zobrazuje změny v čase. Tmavě modrá barva zobrazuje nízké amplitudy a červená zobrazuje nejvyšší amplitudy. Např. když je síť aktivní nebo se mění přenosový kanál. Můžeme si odečíst hodnotu aktivity vybraného zařízení v našem bezdrátovém spektru.



Obr. 22: Waterfall view

### 7.2.4 WiFi síť (WiFi networks)

Tabulka zobrazuje informace o každém WiFi AP, stejně jako inSSIDer. Vybereme požadovanou WiFi kartu ze seznamu a klikneme na tlačítko Start (v pravém horním rohu programu) pro začátek scanování WiFi sítí. Pro zobrazení tabulky WiFi sítí klikneme na Window menu a označíme Wi-Fi Networks.



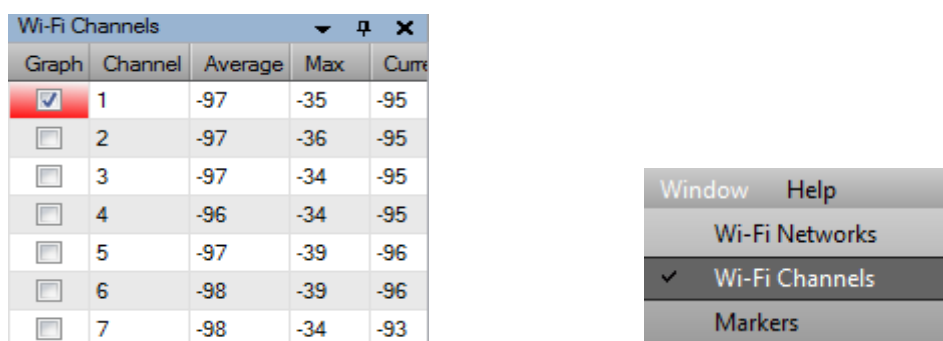
| Graph                               | SSID         | Channel | RSSI | Time     |
|-------------------------------------|--------------|---------|------|----------|
| <input checked="" type="checkbox"/> |              | 1       | -56  | 23:01:09 |
| <input checked="" type="checkbox"/> | 2P05         | 3       | -89  | 23:01:03 |
| <input checked="" type="checkbox"/> | CMMS_EU      | 6       | -87  | 23:01:09 |
| <input checked="" type="checkbox"/> | ADRIA_GRANDE | 6       | -97  | 22:50:47 |
| <input checked="" type="checkbox"/> | CMMS_EU      | 6       | -88  | 22:14:49 |
| <input checked="" type="checkbox"/> | Cra_ADSL     | 7       | -81  | 23:01:03 |

Window Help  
☒ Wi-Fi Networks  
☒ Wi-Fi Channels  
☒ Markers

Obr. 23: WiFi sítě (vlevo) a menu pro zobrazení WiFi sítí (vpravo)

### 7.2.5 WiFi kanály (Wi-Fi Channels)

Tabulka Wi-Fi Channels zobrazuje informace o vysílání WiFi sítí na jednotlivých kanálech. Informace jsou získány z Wi-Spy. Pro zobrazení tabulky vybereme volbu Window – Wi-Fi Channels.



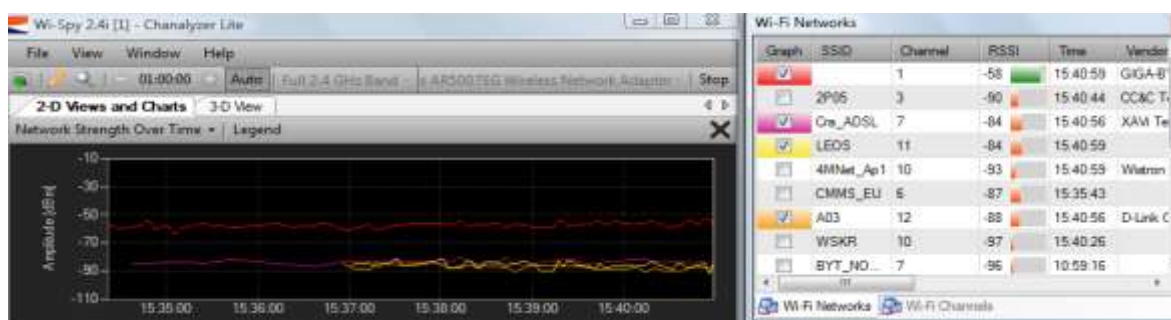
| Graph                               | Channel | Average | Max | Current |
|-------------------------------------|---------|---------|-----|---------|
| <input checked="" type="checkbox"/> | 1       | -97     | -35 | -95     |
| <input type="checkbox"/>            | 2       | -97     | -36 | -95     |
| <input type="checkbox"/>            | 3       | -97     | -34 | -95     |
| <input type="checkbox"/>            | 4       | -96     | -34 | -95     |
| <input type="checkbox"/>            | 5       | -97     | -39 | -96     |
| <input type="checkbox"/>            | 6       | -98     | -39 | -96     |
| <input type="checkbox"/>            | 7       | -98     | -34 | -93     |

Window Help  
 Wi-Fi Networks  
☒ Wi-Fi Channels  
 Markers

Obr. 24: WiFi kanály (vlevo) a menu pro zobrazení WiFi kanálů (vpravo)

### 7.2.6 Síla sítě (Network Strength)

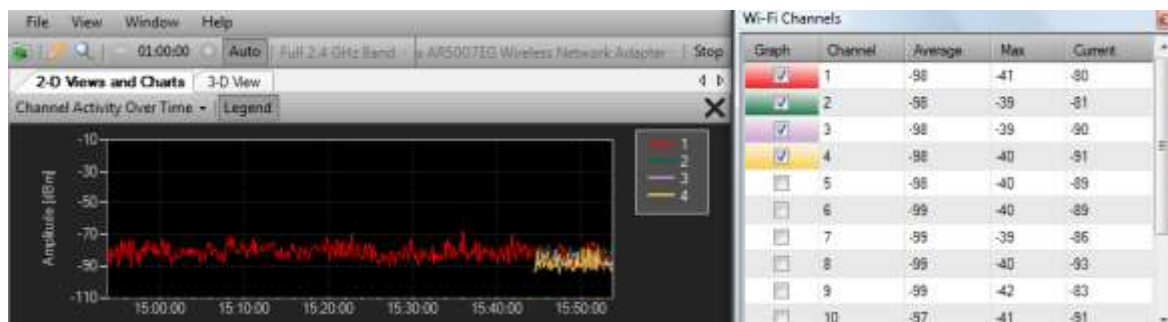
Použitím WiFi karty Chanalyzer Lite získává data o síle signálu každého AP v čase. Zobrazí se jen ty sítě, které jsou označené v tabulce WiFi sítí.



Obr. 25: Zobrazení síly sítě

### 7.2.7 Aktivita kanálu v čase (Channel activity over time)

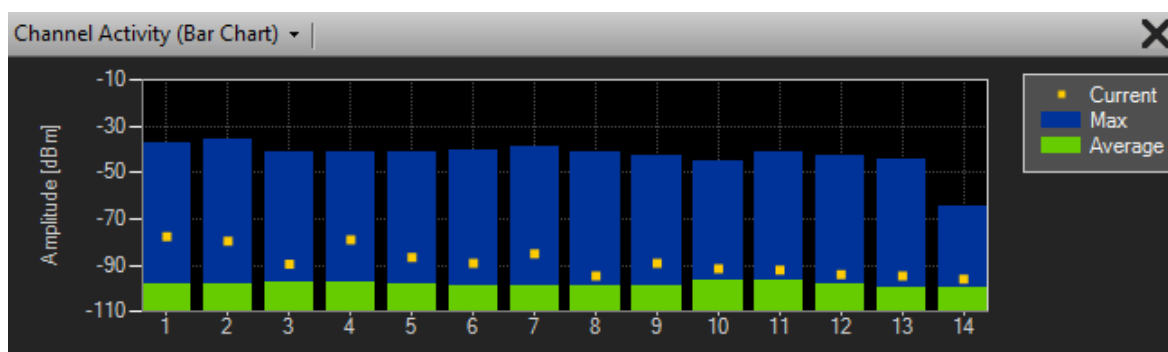
Chanalyzer Lite vypočítává aktivitu WiFi sítí v čase na každém WiFi kanále. Výběrem kanálu v tabulce WiFi Channels sledujeme aktivitu vybraných kanálů za určitý časový úsek. V případě dlouhodobých malých amplitud víme, že dané kanály jsou volné.



Obr. 26: Aktivita kanálu v čase

### 7.2.8 Aktivita WiFi sítí na kanálech (Channel activity bar graph)

Ukazuje průměrnou, maximální a aktuální aktivitu WiFi sítí na kanálech. Žluté čtverce pohybující se nahoru a dolů ukazují aktuální amplitudu na daném kanálu. Vysoké amplitudy ukazují velkou WiFi aktivitu. Čím nižší jsou průměrné a maximální hodnoty, tím lepší volba pro novou síť.



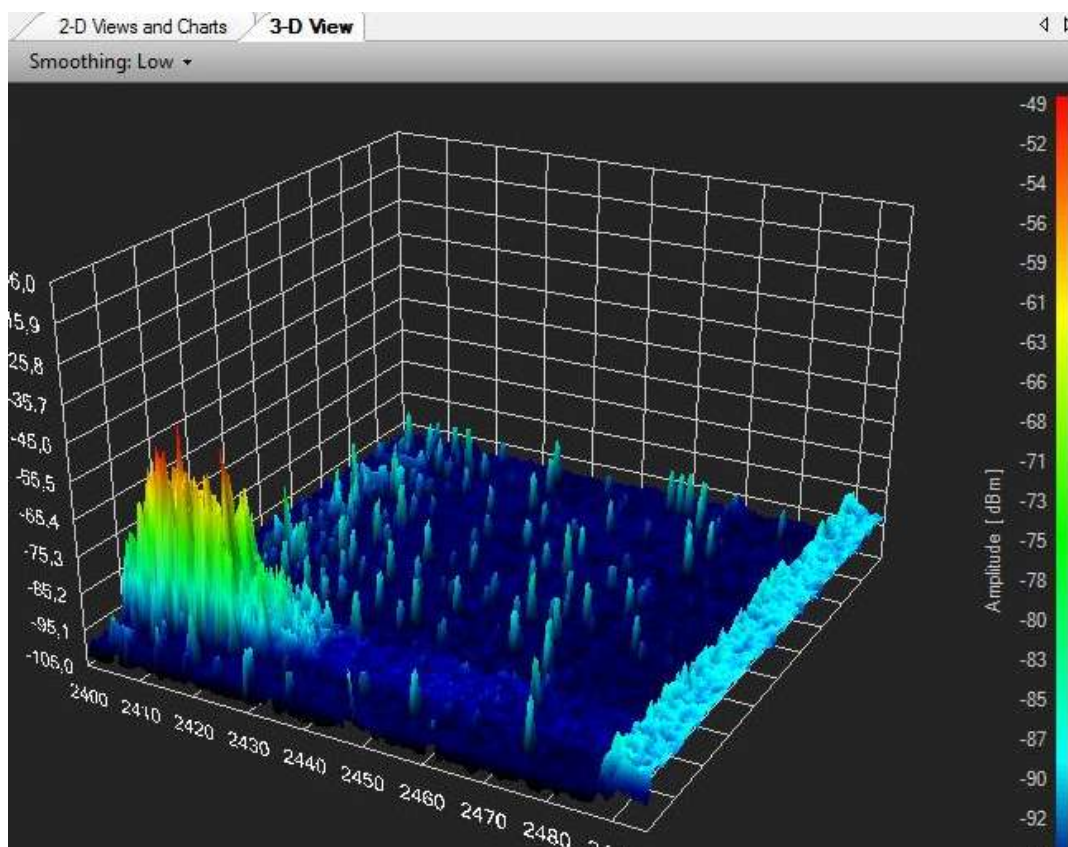
Obr. 27: Aktivita WiFi sítí na kanálech

### 7.2.9 3D zobrazení

3D zobrazení vykresluje amplitudu frekvence v čase (čas je na ose Z). Poskytuje přehled o WiFi aktivitě sítí, zatímco 2D model zobrazuje více o specifických frekvencích, kanálech. 3D zobrazení je možné otočit kliknutím a tažením nebo přiblížit a oddálit.



Možnost použití vyhlazovací volby v 3D pohledu pro blokaci šumu přístrojů, které často mění frekvenci.

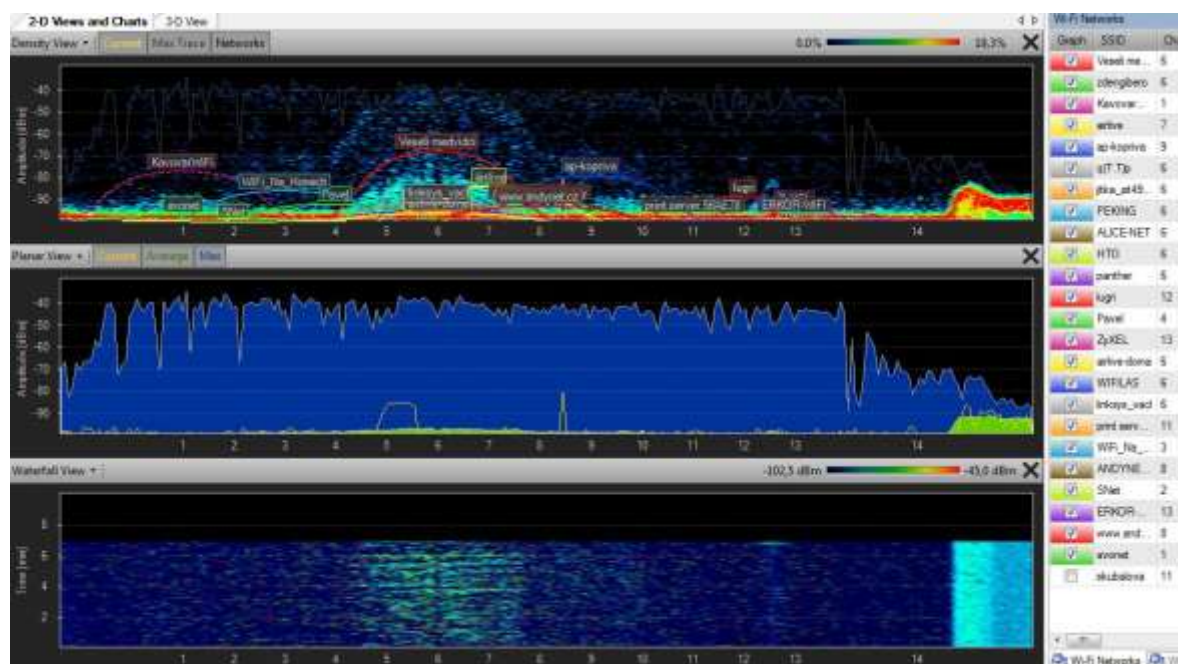


Obr. 28: 3D zobrazení aktivity WiFi sítě při spuštění programu iperf

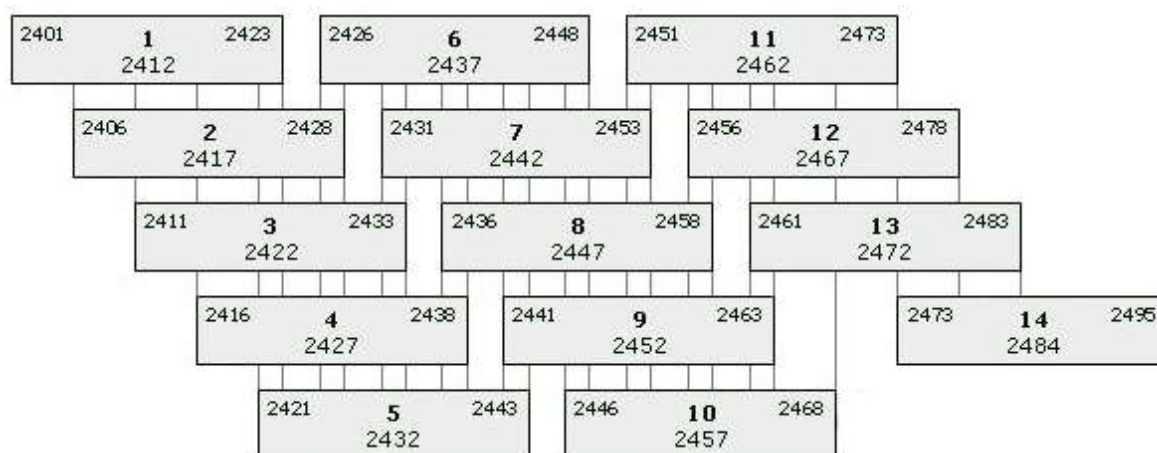
### 7.3 Vlastní hledání volnějšího přenosového kanálu WiFi sítě

Zapojením Wi-Spy do USB laptopu a spuštěním programu Chanalyzer Lite proběhla analýza okolních WiFi sítí. Bylo monitorováno 25 sítí v okolí. Naše síť Veselí Medvíci je na kanále 6. Celkově bylo nalezeno 25 WiFi sítí, které jsou vypsány na pravé straně obr. 29 i s nastaveným WiFi kanálem. Zároveň na kanále 6 je nastaveno další 10 sítí. Na obr. 29 je znázorněno, že na kanále 6 probíhá největší aktivita, a proto je využití kanálu 6 pro naši síť nevýhodné. Dalším důležitým prvkem při rozhodování je překrývání jednotlivých WiFi kanálů, které jsou zobrazeny na obr. 30. Abychom se vyhnuli nejvíce překrývaným WiFi kanálům a zároveň kanálům, na kterých je připojeno nejvíce sítí, rozhodla jsem se zvolit kanál 1.

### 7.3.1 Analýza WiFi sítě



Obr. 29: Analýza WiFi kanálů



Obr. 30: Překrývání WiFi kanálů[13]

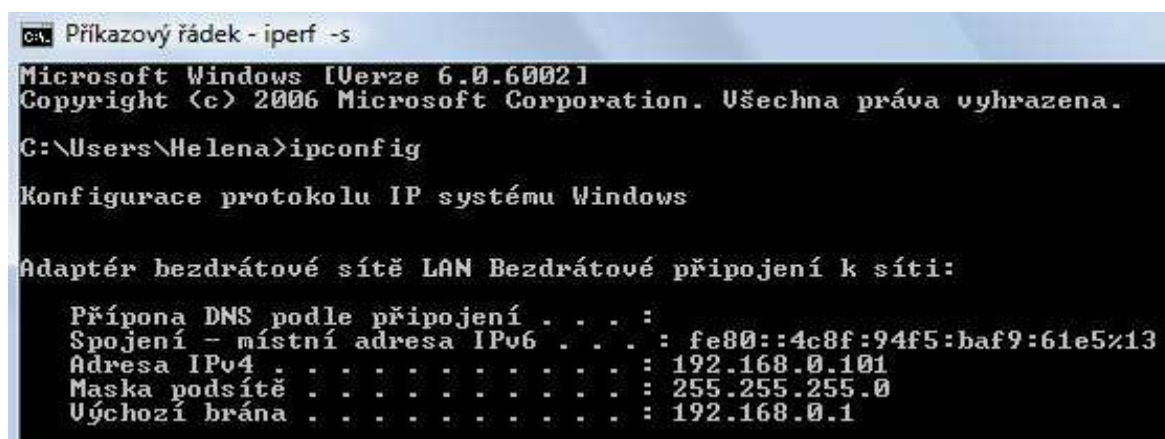
### 7.3.2 Nástroje pro testování „datové“ propustnosti sítě

Abychom si ověřili, že změna z 6. kanálu na kanál 1 způsobí pozitivní změnu v datové propustnosti, provedeme 3 testy před změnou kanálu a po změně kanálu v obousměrné komunikaci.



- Iperf je běžně užívaný pro testování sítí. Může vytvořit TCP i UDP proudy dat a testovat jimi propustnost dané sítě. Iperf je moderní nástroj na měření výkonu sítě napsaný v C++. Umožňuje uživateli užití různých parametrů, které mohou být použity pro testování sítě nebo pro optimalizaci výkonu sítě. Iperf má jak klientskou tak síťovou funkcionalitu. Může měřit propustnost mezi dvěma konci, náhodně nebo tam a zpět. Je to open source.[3]
- Printing Communications Association Port of Test Transmission Control Protocol (dále jen PCATTCP) - je program spustitelný z příkazové řádky, původně pro BSD systém, jehož první verze byla vynalezena v roce 1984. Tento nástroj slouží pro měření výkonu TCP a UDP mezi dvěma systémy. PCATTCP je jeho přímočarý port pro funkci pod operačními systémy Windows.

Měření datové propustnosti mezi 2 laptopy proběhlo třemi testy. Prvním krokem je spuštění příkazového řádku a spuštění příkazu „ipconfig“, u obou laptopů, který nám zobrazí výpis konfigurace protokolu IP systému Windows. Ve výpisu zjistíme adresu IPv4 obou laptopů.



```

ca. Příkazový řádek - iperf -s
Microsoft Windows [Verze 6.0.60021]
Copyright (c) 2006 Microsoft Corporation. Všechna práva vyhrazena.

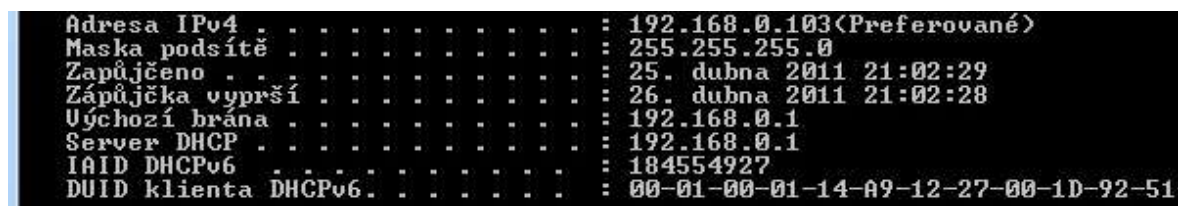
C:\Users\Helena>ipconfig

Konfigurace protokolu IP systému Windows

Adaptér bezdrátové sítě LAN Bezdrátové připojení k síti:

    Připojení DNS podle připojení . . . . . :
    Spojení - místní adresa IPv6 . . . . . : fe80::4c8f:94f5:baf9:61e5%13
    Adresa IPv4 . . . . . : 192.168.0.101
    Masky podsítě . . . . . : 255.255.255.0
    Účchází brána . . . . . : 192.168.0.1
  
```

Obr. 31: Výpis konfigurace laptopu č. 1



```

Adresa IPv4 . . . . . : 192.168.0.103 (Preferované)
Maska podsítě . . . . . : 255.255.255.0
Zapůjčeno . . . . . : 25. dubna 2011 21:02:29
Zapůjčka vyprší . . . . . : 26. dubna 2011 21:02:28
Účchází brána . . . . . : 192.168.0.1
Server DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 184554927
DUID klienta DHCPv6 . . . . . : 00-01-00-01-14-A9-12-27-00-1D-92-51
  
```

Obr. 32: Výpis konfigurace laptopu č. 2

- Měření pomocí programu Iperf:
  - na laptopu č. 1 spustíme příkazový řádek
  - z místa, kde je program Iperf uložen spustíme Iperf příkazem „iperf –s“
  - na laptopu č. 2 spustíme příkazový řádek a z místa kde je Iperf uložen pokračujeme příkazem „iperf –c 192.168.0.101“ (IPv4 laptopu č. 1)
  - měření zopakujeme v druhém směru – začneme spuštěním na laptopu č. 2 příkazem „iperf –s“
  - na laptopu č. 1 pokračujeme příkazem „iperf –c 192.168.0.103“ (IPv4 laptopu č. 2)

```
C:\Users\Helena\net>iperf -c 192.168.0.103
-----
Client connecting to 192.168.0.103, TCP port 5001
TCP window size: 8.00 KByte (default)
-----
[104] local 192.168.0.101 port 50969 connected with 192.168.0.103 port 5001
[ ID] Interval      Transfer    Bandwidth
[104] 0.0-10.0 sec  3.16 MBytes  2.65 Mbits/sec
```

Obr. 33: Naměřené hodnoty laptopu č. 1

```
C:\Users\Majkiii2\Downloads\net>iperf -c 192.168.0.101
-----
Client connecting to 192.168.0.101, TCP port 5001
TCP window size: 8.00 KByte (default)
-----
[124] local 192.168.0.103 port 49307 connected with 192.168.0.101 port 5001
[ ID] Interval      Transfer    Bandwidth
[124] 0.0-10.0 sec  6.44 MBytes  5.39 Mbits/sec
```

Obr. 34: Naměřené hodnoty laptopu č. 2

- Měření pomocí programu PCATTCP – měření probíhá stejně jako u programu Iperf v obou směrech. Rozdílem je spouštěcí příkaz, který je „pcattcp –r“ a příkaz u druhého laptopu je „pccattcp –t 192.168.0.101“.

```
C:\Users\Majkiii2\Downloads\net\PCATTCP>pcattcp -t 192.168.0.101
PCAUSA Test TCP Utility V2.01.01.14 <IPv4/IPv6>
  IP Version   : IPv4
Started TCP Transmit Test 0...
TCP Transmit Test
  Transmit     : TCPv4 0.0.0.0 -> 192.168.0.101:5001
  Buffer Size   : 8192; Alignment: 16384/0
  TCP_NODELAY   : DISABLED <0>
  Connect      : Connected to 192.168.0.101:5001
  Send Mode     : Send Pattern; Number of Buffers: 2048
  Statistics    : TCPv4 0.0.0.0 -> 192.168.0.101:5001
16777216 bytes in 28.688 real seconds = 571.11 KB/sec ***
numCalls: 2048; msec/call: 14.344; calls/sec: 71.388
```

Obr. 35: Výpis naměřených hodnot programem PCATTCP laptopu č. 1

```

C:\Users\Helena\net\PCATTCP>pcattcp -t 192.168.0.103
PCAUSA Test TCP Utility V2.01.01.14 <IPv4/IPv6>
IP Version : IPv4
Started TCP Transmit Test 0...
TCP Transmit Test
Transmit : TCPv4 0.0.0.0 -> 192.168.0.103:5001
Buffer Size : 8192; Alignment: 16384/0
TCP_NODELAY : DISABLED <0>
Connect : Connected to 192.168.0.103:5001
Send Mode : Send Pattern; Number of Buffers: 2048
Statistics : TCPv4 0.0.0.0 -> 192.168.0.103:5001
16777216 bytes in 21.449 real seconds = 763.86 KB/sec +++
numCalls: 2048; msec/call: 10.725; calls/sec: 95.482

```

Obr. 36: Výpis naměřených hodnot programem PCATTCP laptopu č. 2

- Měření času při přesunu souboru z jednoho laptopu na druhý. Oboustranně byl poslán soubor o velikosti 233MB. Přesun z laptopu č. 2 na č. 1 trval 7:56. Opačně byl časový interval 6:16.

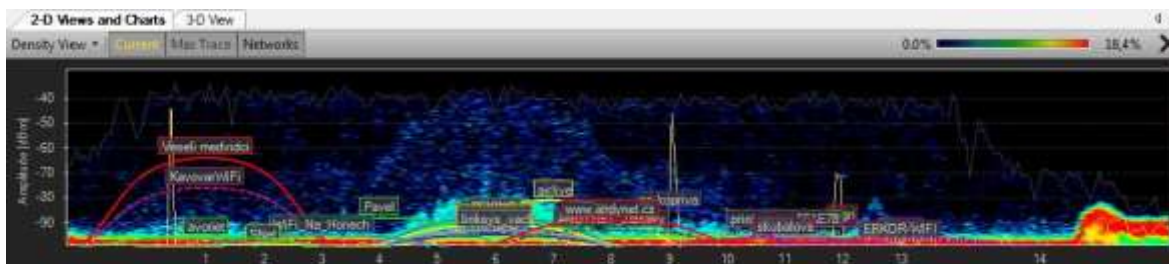
Rozdíly v protisměrném měření v rámci jednoho kanálu jsou způsobeny starší verzí WiFi přijímače v jednom z laptopů.

### 7.3.3 Nové nastavení WiFi kanálu

K spuštění nastavení routeru je potřeba znát IP adresu routeru. Na obr. 31 je výpis konfigurace protokolu IP systému Windows, kde je i IP adresa routeru – výchozí brána. Do výchozího prohlížeče (např. Google Chrome) zadáme číselnou adresu výchozí brány. V nastavení routeru změníme přenosový kanál z 6 na 1.



Obr. 37: Změna WiFi kanálu



Obr. 38: Zobrazení změny na WiFi kanál 1 pomocí Wi-Spy

### 7.3.4 Ověření změn

Po změně přenosového kanálu na kanál č. 1 proběhly 3 testy datové propustnosti znovu.

- Měření programem Iperf po změně na kanál 1. Měření se provádí stejně jako před změnou WiFi kanálu.

```
C:\Users\Helena\net>iperf -s
-----
Server listening on TCP port 5001
TCP window size: 8.00 KByte (default)
-----
[116] local 192.168.0.101 port 5001 connected with 192.168.0.103 port 49497
[ ID] Interval      Transfer    Bandwidth
[116] 0.0-10.0 sec  6.59 MBytes  5.52 Mbits/sec
```

Obr. 39: Měření programem Iperf po změně kanálu na laptopu č. 1

```
C:\Users\Helena\net>iperf -c 192.168.0.103
-----
Client connecting to 192.168.0.103, TCP port 5001
TCP window size: 8.00 KByte (default)
-----
[104] local 192.168.0.101 port 49355 connected with 192.168.0.103 port 5001
[ ID] Interval      Transfer    Bandwidth
[104] 0.0-10.0 sec  8.31 MBytes  6.97 Mbits/sec
```

Obr. 40: Měření programem Iperf po změně kanálu na laptopu č. 2

- Měření programem PCATTCP po změně na WiFi kanál 1. Měření se provádí stejně jako před změnou WiFi kanálu.

```
C:\Users\Helena\net\PCATTCP>pcattcp -r
PCAUSA Test TCP Utility V2.01.01.14 <IPv4/IPv6>
IP Version : IPv4
Started TCP Receive Test 0...
TCP Receive Test
Local Host : Helena-PC
*****
Listening...: On TCPv4 0.0.0.0:5001

Accept : TCPv4 0.0.0.0:5001 <- 192.168.0.103:49519
Buffer Size : 8192; Alignment: 16384/0
Receive Mode: Sinking <discarding> Data
Statistics : TCPv4 0.0.0.0:5001 <- 192.168.0.103:49519
16777216 bytes in 21.988 real seconds = 745.13 KB/sec +++
numCalls: 2052; msec/call: 10.973; calls/sec: 93.324
```

Obr. 41: Měření programem PCATTCP po změně kanálu na laptopu č. 1



```

C:\Users\Helena\net\PCATTCP>pcatttcp -t 192.168.0.103
PCAUSA Test TCP Utility 02.01.01.14 (IPv4/IPv6)
  IP Version   : IPv4
Started TCP Transmit Test 0...
TCP Transmit Test
  Transmit     : TCPv4 0.0.0.0 -> 192.168.0.103:5001
  Buffer Size  : 8192; Alignment: 16384/0
  TCP_NODELAY  : DISABLED (0)
  Connect     : Connected to 192.168.0.103:5001
  Send Mode    : Send Pattern; Number of Buffers: 2048
  Statistics   : TCPv4 0.0.0.0 -> 192.168.0.103:5001
16777216 bytes in 18.926 real seconds = 865.69 KB/sec +++
numCalls: 2048; msec/call: 9.463; calls/sec: 108.211

```

Obr. 42: Měření programem PCATTCP po změně kanálu na laptopu č. 2

- Měření času při přesunu souboru z jednoho laptopu na druhý. Oboustranně byl poslán soubor o velikosti 233MB. Přesun z laptopu č. 2 na č. 1 probíhal 5:39. Opačně byl čas přesunu 4:49.

|                     | Testy kanál 6 |           | Testy kanál 1 |           | Změna v % |           |
|---------------------|---------------|-----------|---------------|-----------|-----------|-----------|
| Typ testu           | Laptop 1.     | Laptop 2. | Laptop 1.     | Laptop 2. | Laptop 1. | Laptop 2. |
| Iperf (Mbps/sec)    | 2,65          | 5,39      | 5,52          | 6,97      | 108,30    | 29,31     |
| PCATTCP (KB/sec)    | 571,11        | 763,86    | 745,13        | 865,69    | 30,47     | 13,33     |
| Přenos dat (KB/sec) | 501,24        | 634,55    | 703,81        | 825,58    | 40,41     | 30,10     |

Tabulka 42: Shrnutí naměřených dat před změnou WiFi kanálu a po změně

V tabulce jsou vyplněny hodnoty naměřené při nastavení WiFi sítě na přenosovém kanálu 6 u všech tří testů. Zároveň jsou ke srovnání hodnoty naměřené po změně na přenosový kanál 1. Poslední část tabulky zobrazuje procentuální zlepšení datové propustnosti po změně přenosového kanálu. Změnou přenosového kanálu jsme dosáhli u všech tří testů lepších výsledků než v původním nastavení.

## ZÁVĚR

Bezdrátová komunikace je běžnou součástí moderního života, jak v soukromém životě, tak v práci. Rádiové sítě se snadno odposlouchávají a dávají prostor pro narušitele k provedení útoků na WiFi sítě, které se v současné době využívají i v průmyslu komerční bezpečnosti. U WiFi sítě je důležitá implementace bezpečnostních protokolů – zvolit nejvyšší možné šifrování, které bezdrátové zařízení poskytuje.

Teoretická část diplomové práce vysvětluje princip činnosti WiFi sítí a popisuje jednotlivé typy antén, které se používají pro bezdrátové připojení. Nesprávně zvoleným typem antény a jejím nastavením pro přenos signálu, můžeme dát útočníku větší příležitost pro provedení útoku na síť. Bezdrátovou síť je důležité udržet v prostoru, ve kterém ji potřebujeme.

V teoretické části je prezentováno několik programů pro monitorování WiFi sítí. Všechny programy jsou volně dostupné ke stažení z internetu. Jeden z prezentovaných programů (InSSIDer) byl vybrán do praktické části pro průzkum zabezpečení WiFi sítí v zadané oblasti sídliště Jižní Svahy.

Průzkum byl prováděn wardrivingem (činnost vyhledávání WiFi sítí z auta). Programem InSSIDer bylo na 30 stanovištích celkově monitorováno 837 WiFi sítí a shromážděny informace o jednotlivých sítích. Výsledkem průzkumu zabezpečení WiFi sítí v zadané oblasti bylo zjištěno, že přes 60 % WiFi sítí je zabezpečeno kvalitním šifrovacím protokolem. Oproti předešlým letům, si lidé více uvědomují důležitost ochrany osobních informací a dat.

V praktické části byl vytvořen návod k používání Wi-Spy 2.4i a popsány jednotlivé prvky. Wi-Spy je spektrální analyzátor pro WiFi 2,4 GHz a byl použit pro analýzu vlastní i okolních sítí. Vlastní WiFi síť byla analyzována na stávajícím kanále a následně změněna na volnější přenosový kanál. Pro verifikaci změny přenosového kanálu byly spuštěny 3 testy datové propustnosti. Všechny 3 testy prokázaly, že změnou přenosového kanálu bylo dosaženo větší datové propustnosti. Diplomová práce bude sloužit jako manuál pro hledání a ověřování volnějšího přenosového kanálu u bezdrátových sítí.

Využití bezdrátových sítí narůstá. Pásmo 2,4 GHz je zahlceno dalšími zařízeními, která mohou ovlivňovat bezdrátové připojení a snižovat datovou propustnost. Správným

nastavením přenosového kanálu dosáhneme spolehlivějšího bezdrátového připojení a vyšší datové propustnosti.

## ZÁVĚR V ANGLIČTINĚ

The wireless communication is the common part of the modern life, both personal and working. Radio nets are easily monitored and there is big space for an intruder to attack WiFi nets that are currently used also in the commercial security industry.

Regarding WiFi nets it is important to implement security elements – to choose as high level of coding as possible, which is provided by wireless equipment.

The theoretical part of my diploma thesis explains the principle of WiFi net working and describes individual kinds of sky wires, which are used for the wireless connection. If the sky wire or its settings for signal transmission is chosen wrongly, it can grant the opportunity to an intruder to make an attack. It is important to keep the wireless net in the space where it is needed.

In the theoretical part a few monitoring programmes for the WiFi net are presented. All these programmes are available on the Internet to download for free. One of the presented programmes (InSSIDer) was chosen to the practical part for a research of WiFi security in a certain area of Jižní Svahy.

The research was done by Wardriving (which is an activity of searching WiFi from a car). The programme InSSIDer registered 837 WiFi nets in 30 standpoints. Also some information about the nets was collected. The result of the research of WiFi security in the certain area showed that more than 60% of the WiFi nets were protected by high-quality security elements. To compare it with the recent years, people are now more awarded of the importance of personal data security.

In the practical part a manual for Wi-Spy 2.4i was created and individual elements were described. Wi-Spy is a spectrum analyzer for WiFi 2,4GHz and it was used for our own and surrounding nets. Our own WiFi net was analyzed in the current channel and consequently it was changed to a more open transmission channel. Then, 3 tests of data throughput were launched for the verification of the transmission channel change. All 3 tests proved that the change of the transmission channel caused the bigger data throughput. The diploma thesis will be serving as a manual for searching and checking of a more open transmission channel of wireless nets.



The usage of the wireless nets is getting higher. The zone 2,4 GHz is overloaded by other devices which can influence the wireless connection and lower the data throughput. If the transmission channel is set up correctly, we can get more reliable wireless connection and higher data throughput.

## SEZNAM POUŽITÉ LITERATURY

- [1] SPURNÁ, Helena, SKOVAJSOVÁ, Kateřina. Bezpečnost bezdrátové sítě WiFi. *Security magazín*. 2008, č. 3, s. 2-3.
- [2] SKOVAJSOVÁ, Kateřina, SPURNÁ, Helena. Rušivé signály elektromagnetické kompatibility a odolnost budov. In TD 2008 - DIAGON 2008. Zlín, 2008. s. 56-59. ISBN 978-80-7318-707-1.
- [3] Iperf. In *Wikipedia : the free encyclopedia* [online]. St. Petersburg (Florida) : Wikipedia Foundation, 19 December 2007 , last modified on 13 January 2011 [cit. 2011-04-23]. Dostupné z WWW: <<http://en.wikipedia.org/wiki/Iperf>>.
- [4] IVANKA, Ján, ČANDÍK, Marek. Konfigurace a zabezpečení WiFi sítí. *Security magazín*. 2007, č. 14, s. 4-18.
- [5] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť Wi-Fi*. Brno : Computer Press, 2004. War driving: nástroje a techniky, s. 176.
- [6] HORSKÝ, Radek. *Bezdrátové sítě Wi-Fi v rekordním čase*. Praha : Grada, 2006. 84 s.
- [7] STRÁNSKÝ, Petr. *Svět hardware* [online]. 2.10.2009 [cit. 2010-10-17]. Historie Wi-Fi od FHSS k bezdrátu. Dostupné z WWW: <[http://www.svethardware.cz/art\\_doc-E8854472EA5653EBC1257636003B03D0.html](http://www.svethardware.cz/art_doc-E8854472EA5653EBC1257636003B03D0.html)>.
- [8] BARKEN, Lee. *Jak zabezpečit bezdrátovou síť Wi-Fi*. Brno : Computer Press, 2004. Seznámení s rádiovými technologiemi, s. 176.
- [9] HORÁK, Jaroslav; KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. 4.aktualizované. Brno : Computer Press, a.s., 2008. 328 s.
- [10] KOHRE, Thomas. Stavíme si bezdrátovou síť Wi-Fi. Vyd. 1. Brno : Computer Press, a.s., 2004. 296 s.
- [11] HAŇKA, Ladislav. Teorie elektromagnetického pole. Praha : SNTL, 1982. 224 s.
- [12] BÁRTA, Jiří. *Úvod do počítačových sítí*. České Budějovice : Koop, 1995. 168 s.

- [13] *Dashův web* [online]. 12.8.2010 [cit. 2011-04-27]. Jak zvolit vhodný WiFi kanál?. Dostupné z WWW: <<http://dash.nazory.cz/c70-jak-zvolit-vhodny-wifi-kanal.html>>.
- [14] KUBEŠ, Radek. *Technet* [online]. 30.5.2010 [cit. 2010-09-30]. Nejdůležitější nástroje pro připojení i kontrolu wi-fi sítě. Dostupné z WWW: <[http://technet.idnes.cz/software.asp?c=A100528\\_151435\\_software\\_mbo](http://technet.idnes.cz/software.asp?c=A100528_151435_software_mbo)>.
- [15] *Slunečnice* [online]. c2010, 13.5.2010 [cit. 2010-09-30]. Vistumbler 9.8. Dostupné z WWW: <<http://www.slunecnice.cz/sw/vistumbler/>>.
- [16] *Comkids Club* [online]. c2010 [cit. 2010-09-30]. Program detekuje signály z bezdrátových sítí Metageek. Dostupné z WWW: <<http://www.comkidsclub.net/?p=212{=cs}>>.
- [17] *Slunečnice* [online]. c2010, 31.8.2010 [cit. 2010-10-04]. Wireshark 1.4.0. Dostupné z WWW: <<http://www.slunecnice.cz/sw/wireshark/>>.
- [18] *Vybusny.blog* [online]. 12.1.2010 [cit. 2010-10-04]. Výbušniny, elektronika a všechno možné. Dostupné z WWW: <<http://vybusny.blog.cz/>>.
- [19] *Wifi.aspa* [online]. c2010 [cit. 2010-10-16]. Anténa parabola MaxLink 22 dBi 5 GHz 30cm. Dostupné z WWW: <<http://wifi.aspa.cz/antena-parabola-maxlink-22-dbi-5-ghz-30cm-z81425/>>.
- [20] *Admet* [online]. c2009 [cit. 2010-10-16]. ASH13. Dostupné z WWW: <<http://www.admet.cz/?13,ash13>>.
- [21] *Comtel* [online]. c2008 [cit. 2010-10-16]. České vysoké učení v Praze. Dostupné z WWW: <[www.comtel.cz/files/download.php?id=2803](http://www.comtel.cz/files/download.php?id=2803)>.
- [22] *Hw* [online]. c2009 [cit. 2010-10-17]. Warchalking a bezpečnost WiFi sítě. Dostupné z WWW: <[http://hw.cz/ethernet/wifi/wifi\\_warchalking.html](http://hw.cz/ethernet/wifi/wifi_warchalking.html)>.
- [23] *ThinkGeek* [online]. c2011 [cit. 2011-04-13]. Wi-Spy 2.4i Spectrum Analyzer. Dostupné z WWW: <<http://www.thinkgeek.com/gadgets/electronic/c240/>>.
- [24] *EuroShop store* [online]. c2011 [cit. 2011-04-13]. Wi-Spy 2.4i USB WiFi Spektrální analyzer MetaGeek. Dostupné z WWW: <<http://www.antiradary-distributor.cz/wispy-24i-usb-wifi-spektralni-analyzer-metageek-p-20551.html>>.

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

|         |  |
|---------|--|
| AP      | Access Point   |
| GPS     | Global Positioning System  |
| IEEE    | The Institute of Electrical and Electronics Engineers                          |
| IPSec   | Internet Protocol Security   |
| MAC     | Media Access Control   |
| PCATTCP | Printing Communications Association Port of Test Transmission Control Protocol |
| SSID    | Service Set Identifier   |
| VoIP    | Voice over Internet Protocol   |
| WEP     | Wired Equivalent Privacy   |
| WIFI    | Wireless Fidelity  |
| WPA     | WiFi Protected Access  |
| WPA2    | WiFi Protected Access 2  |

## SEZNAM OBRÁZKŮ

|  |    |
|--|----|
| Obr. 1: Topologie uspořádání komponent v síti .....  | 12 |
| Obr. 2: Vyzařovací diagram směrové antény v horizontální a vertikální rovině[19] .....                   | 17 |
| Obr. 3: Vyzařovací diagram sektorové antény v horizontální (vlevo) a vertikální rovině(vpravo)[20] ..... | 18 |
| Obr. 4: Vyzařovací diagram všesměrové antény v horizontální a vertikální rovině[21] .....                | 18 |
| Obr. 5: Asociace v otevřené síti[5] .....  | 19 |
| Obr. 6: Asociace v uzavřené síti[5] .....  | 20 |
| Obr. 7: Warchalking – ukázka symbolů[5] .....  | 22 |
| Obr. 8: Vizualizace programu NetStumbler[14] .....   | 24 |
| Obr. 9: Vizualizace programu NetSurveyor[14] .....   | 25 |
| Obr. 10: Vizualizace programu Xirrus WiFi Inspector[14] .....  | 26 |
| Obr. 11: Vizualizace programu Vistumbler[15] .....   | 27 |
| Obr. 12: Vizualizace programu InSSIDer[16] .....   | 28 |
| Obr. 13: Vizualizace programu Wireshark[17] .....  | 29 |
| Obr. 14: Vizualizace programu Easy WiFi Radar[18] .....  | 30 |
| Obr. 15: Mapa stanovišť pro monitoring WiFi sítí .....   | 33 |
| Obr. 16: Graf vyhodnocení dat z 1. měření .....  | 41 |
| Obr. 17: Graf vyhodnocení dat z 2. měření .....  | 41 |
| Obr. 18: Zapojení Wi-Spy přes USB do laptopu[23] .....   | 42 |
| Obr. 19: Planar view .....   | 43 |
| Obr. 20: Markers .....   | 43 |
| Obr. 21: Density view .....  | 44 |
| Obr. 22: Waterfall view .....  | 44 |
| Obr. 23: WiFi sítě (vlevo) a menu pro zobrazení WiFi sítí (vpravo) .....                                 | 45 |
| Obr. 24: WiFi kanály (vlevo) a menu pro zobrazení WiFi kanálů (vpravo) .....                             | 45 |
| Obr. 25: Zobrazení síly sítě .....   | 45 |
| Obr. 26: Aktivita kanálu v čase .....  | 46 |
| Obr. 27: Aktivita WiFi sítí na kanálech .....  | 46 |
| Obr. 28: 3D zobrazení aktivity WiFi sítě při spuštění programu iperf .....                               | 47 |
| Obr. 29: Analýza WiFi kanálů .....   | 48 |
| Obr. 30: Překrývání WiFi kanálů[13] .....  | 48 |

|   |    |
|---|----|
| Obr. 31: Výpis konfigurace laptopu č. 1 .....                           | 49 |
| Obr. 32: Výpis konfigurace laptopu č. 2 .....                           | 49 |
| Obr. 33: Naměřené hodnoty laptopu č. 1 .....                            | 50 |
| Obr. 34: Naměřené hodnoty laptopu č. 2 .....                            | 50 |
| Obr. 35: Výpis naměřených hodnot programem PCATTCP laptopu č. 1 .....   | 50 |
| Obr. 36: Výpis naměřených hodnot programem PCATTCP laptopu č. 2 .....   | 51 |
| Obr. 37: Změna WiFi kanálu .....  | 51 |
| Obr. 38: Zobrazení změny na WiFi kanál 1 pomocí Wi-Spy .....            | 52 |
| Obr. 39: Měření programem Iperf po změně kanálu na laptopu č. 1 .....   | 52 |
| Obr. 40: Měření programem Iperf po změně kanálu na laptopu č. 2 .....   | 52 |
| Obr. 41: Měření programem PCATTCP po změně kanálu na laptopu č. 1 ..... | 52 |
| Obr. 42: Měření programem PCATTCP po změně kanálu na laptopu č. 2 ..... | 53 |

**SEZNAM TABULEK**

|   |    |
|---|----|
| Tabulka 1: Základní charakteristika rádiové vlny[8] .....           | 14 |
| Tabulka 2: Základní vztahy mezi veličinami rádiové vlny[8] .....    | 14 |
| Tabulka 3: Shrnutí specifikací programu NetStumbler .....           | 23 |
| Tabulka 4: Tabulka shrnutí specifikací programu NetSurveyor .....   | 24 |
| Tabulka 5: Shrnutí specifikací programu Xirrus WiFi Inspector ..... | 25 |
| Tabulka 6: Shrnutí specifikací programu Vistumbler .....            | 27 |
| Tabulka 7: Shrnutí specifikací programu InSSIDer .....              | 28 |
| Tabulka 8: Shrnutí specifikací programu Wireshark .....             | 29 |
| Tabulka 9: Shrnutí specifikací programu Easy WiFi Radar .....       | 30 |
| Tabulka 10: Souhrn dat ze stanoviště č. 1 .....                     | 34 |
| Tabulka 11: Souhrn dat ze stanoviště č. 2 .....                     | 34 |
| Tabulka 12: Souhrn dat ze stanoviště č. 3 .....                     | 34 |
| Tabulka 13: Souhrn dat ze stanoviště č. 4 .....                     | 34 |
| Tabulka 14: Souhrn dat ze stanoviště č. 5 .....                     | 34 |
| Tabulka 15: Souhrn dat ze stanoviště č. 6 .....                     | 35 |
| Tabulka 16: Souhrn dat ze stanoviště č. 7 .....                     | 35 |
| Tabulka 17: Souhrn dat ze stanoviště č. 8 .....                     | 35 |
| Tabulka 18: Souhrn dat ze stanoviště č. 9 .....                     | 35 |
| Tabulka 19: Souhrn dat ze stanoviště č. 10 .....                    | 35 |
| Tabulka 20: Souhrn dat ze stanoviště č. 11 .....                    | 36 |
| Tabulka 21: Souhrn dat ze stanoviště č. 12 .....                    | 36 |
| Tabulka 22: Souhrn dat ze stanoviště č. 13 .....                    | 36 |
| Tabulka 23: Souhrn dat ze stanoviště č. 14 .....                    | 36 |
| Tabulka 24: Souhrn dat ze stanoviště č. 15 .....                    | 36 |
| Tabulka 25: Souhrn dat ze stanoviště č. 16 .....                    | 37 |
| Tabulka 26: Souhrn dat ze stanoviště č. 17 .....                    | 37 |
| Tabulka 27: Souhrn dat ze stanoviště č. 18 .....                    | 37 |
| Tabulka 28: Souhrn dat ze stanoviště č. 19 .....                    | 37 |
| Tabulka 29: Souhrn dat ze stanoviště č. 20 .....                    | 37 |
| Tabulka 30: Souhrn dat ze stanoviště č. 21 .....                    | 38 |
| Tabulka 31: Souhrn dat ze stanoviště č. 22 .....                    | 38 |

|   |    |
|---|----|
| Tabulka 32: Souhrn dat ze stanoviště č. 23 .....                            | 38 |
| Tabulka 33: Souhrn dat ze stanoviště č. 24 .....                            | 38 |
| Tabulka 34: Souhrn dat ze stanoviště č. 25 .....                            | 38 |
| Tabulka 35: Souhrn dat ze stanoviště č. 26 .....                            | 39 |
| Tabulka 36: Souhrn dat ze stanoviště č. 27 .....                            | 39 |
| Tabulka 37: Souhrn ze stanoviště č. 28 .....                                | 39 |
| Tabulka 38: Souhrn dat ze stanoviště č. 29 .....                            | 39 |
| Tabulka 39: Souhrn dat ze stanoviště č. 30 .....                            | 39 |
| Tabulka 40: Shrnutí počtu monitorovaných sítí a jejich zabezpečení .....    | 40 |
| Tabulka 41: Specifikace Wi-Spy 2.4i .....                                   | 43 |
| Tabulka 42: Shrnutí naměřených dat před změnou WiFi kanálu a po změně ..... | 53 |



## **PŘÍLOHA P I: NÁZEV PŘÍLOHY**

**P I:** Naměřená data wardrivingem