

# Monitorování Wi-Fi sítí ve vybrané oblasti

Stanislav Tomek

---

Bakalářská práce  
2018



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2017/2018

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Stanislav Tomek**  
Osobní číslo: **A15127**  
Studijní program: **B3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**  
Forma studia: **prezenční**

Téma práce: **Monitorování Wi-Fi sítí ve vybrané oblasti**  
Téma anglicky: **Monitoring Wi-Fi networks in a Selected Area**

Zásady pro vypracování:

1. Seznamte se s problematikou WiFi sítí a jejich monitorováním.
2. Uvedte rozdělení bezdrátových sítí, jejich strukturu a zabezpečení.
3. Charakterizujte základní typy antén pro WiFi síť.
4. Zmapujte zabezpečení WiFi sítí ve vybrané části města Vsetín, pomocí programu inSSiDer, metodou wardriving.
5. Verifikujte získaná data pomocí Wi-Spy Chanalyzer Lite.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. PUŽMANOVÁ, Rita. **Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G.** Brno: CP Books, 2005. ISBN 80-251-0791-4
2. BARKEN, Lee. **Wi-Fi: jak zabezpečit bezdrátovou síť.** Brno: Computer Press, 2004. ISBN 80-251-0346-3
3. IVANKA, Ján a Petr NAVRÁTIL. **Standardizace WiFi sítí a jejich využití v průmyslu komerční bezpečnosti.** In: Security magazín. Praha: Familymedia, 2009, 2531. ISSN 1210-8723
4. IVANKA, Ján a Petr NAVRÁTIL: **Prenosové vrstvy WiFi sietí a ich využitie v priemysle komerčnej bezpečnosti.** Security magazín – Alarm, vyd. Plettac Security, ročník XI, č.:4/2009, Infodom s.r.o., Slovenská republika , s. 16 21, ISSN 1335 504 X
5. IVANKA, Ján a Petr NAVRÁTIL: **Sposoby ohrozenia wifi sietí z pohľadu bežného užívateľa v PKB.** Security magazín – Alarm, vyd. Plettac Security, ročník XI, č.:4/2009, Infodom s.r.o., Slovenská republika , s. 22 27, ISSN 1335 504 X
6. IVANKA, Ján a Marek ČANDÍK, Marek: **Konfigurace a zabezpečení WIFI sítí.** In. Security magazín, Ročn. XIV., vyd. 63, 6/2007, vyd. Familymedia, Praha, 2007, str.4 8, ISSN 1210 8723
7. IVANKA, Ján a Rudolf DRGA: **Využití spektrálních analyzátorů WI-SPY v průmyslu komerční bezpečnosti.** In: Security magazín – Alarm, vyd. Plettac Security, ročník XIII, č.:3/2011, Infodom s.r.o., Slovenská republika , s. 10 13, ISSN 1335 504 X

Vedoucí bakalářské práce:

**Ing. Ján Ivanka**

Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce:

**12. prosince 2017**

Termín odevzdání bakalářské práce:

**24. května 2018**

Ve Zlíně dne 12. prosince 2017



doc. Mgr. Milan Adámek, Ph.D.  
*děkan*



Ing. Jan Valouch, Ph.D.  
*ředitel ústavu*

**Jméno, příjmení: Stanislav, Tomek**

**Název bakalářské/diplomové práce: Monitorování Wi-Fi sítí ve vybrané oblasti**


**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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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, dne 17.5.2018

  
.....  
podpis diplomanta

## **ABSTRAKT**

Bakalářská práce se zabývá problematikou Wi-Fi sítí a je rozdělena na teoretickou a praktickou část. V teoretické části jsou popsány potřebné komponenty pro bezdrátové sítě a jejich dělení. Jsou zde charakterizovány bezdrátové technologie, používané standardy, typy zabezpečení a jednotlivé útoky a hrozby Wi-Fi sítí. V praktické části je popis jednotlivých funkcí softwaru inSSIDer a Chanalyzer Lite, pomocí kterých bylo provedeno měření a vyhodnocení naměřených dat. Monitorování bylo provedeno v centru města Vsetína. V závěru práce je vyhodnocení naměřených dat a uvedení statistických údajů.

Klíčová slova: Wi-Fi, inSSIDer, Wi-Spy, wardriving, Chanalyzer Lite.

## **ABSTRACT**

The bachelor thesis deals with the problems of Wi-Fi networks and is divided into the theoretical and practical part. The theoretical part describes the necessary components for wireless networks and their division. There are wireless technologies, standards used, security types, and individual attacks and threats to Wi-Fi networks. In the practical part is a description of the individual functions of softwares inSSIDer and Chanalyzer Lite, which were used to measure and evaluate the measured data. Monitoring was carried out in the city center Vsetin. At the end of the thesis is evaluation of measured data and statistical data.

Keywords: Wi-Fi, inSSIDer, Wi-Spy, wardriving, Chanalyzer Lite.

## **Poděkování**

Tímto chci poděkovat svým rodičům, za umožnění studia na vysoké škole a sourozencům za psychickou podporu. Děkuji také vedoucímu bakalářské práce panu Ing. Jánovi Ivankovi za pomoc při vedení a zpracovávání tématu.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

*„Smutné je, že hlupáci jsou tak sebejistí, zatímco moudří lidé jsou vždy plní pochybností.“*

Bertrand Russell

# OBSAH

<b>ÚVOD.....</b>	<b>8</b>
<b>I TEORETICKÁ ČÁST.....</b>	<b>9</b>
<b>1 BEZDRÁTOVÉ SÍTĚ.....</b>	<b>10</b>
1.1 KOMPONENTY BEZDRÁTOVÉ SÍTĚ.....	10
1.2 ROZDĚLENÍ BEZDRÁTOVÝCH SÍTÍ.....	11
1.2.1 Wireless Personal Area Network.....	12
1.2.2 Wireless Local Area Network.....	12
1.2.3 Wireless Metropolitan Area Network.....	13
1.2.4 Wireless Wide Area Network.....	14
1.3 TOPOLOGIE BEZDRÁTOVÝCH SÍTÍ.....	15
1.3.1 Síť Ad – Hoc.....	15
1.3.2 Síť Infrastruktura.....	16
<b>2 ZABEZPEČENÍ WI-FI SÍTÍ.....</b>	<b>17</b>
2.1 AUTENTIZACE.....	17
2.2 ŠIFROVÁNÍ.....	18
2.2.1 Symetrické šifrování.....	19
2.2.2 Asymetrické šifrování.....	19
2.2.3 Hybridní šifrování.....	20
<b>3 HROZBY A ÚTOKY NA WI-FI SÍTĚ.....</b>	<b>22</b>
3.1 ZJIŠTĚNÍ KLÍČE.....	22
3.2 ZJIŠTĚNÍ MAC ADRESY.....	22
3.3 ÚTOK MAN-IN-THE-MIDDLE.....	23
3.4 SLOVNÍKOVÝ ÚTOK.....	23
3.5 DoS A DDoS ÚTOKY.....	23
3.6 SKENOVÁNÍ SÍTÍ.....	26
<b>4 CHARAKTERISTIKA ANTÉN VE WI-FI SÍTÍCH.....</b>	<b>27</b>
4.1 PARAMETRY.....	27
4.2 TYPY ANTÉN.....	27
4.2.1 Všesměrové antény.....	28
4.2.2 Sektorové antény.....	28
4.2.3 Směrové antény.....	29
4.3 PROBLÉMY SE ŠÍŘENÍM SIGNÁLU VE WI-FI SÍTÍCH.....	30
4.3.1 Vytížené frekvenční pásmo.....	30
4.3.2 Viditelnost.....	31
<b>II PRAKTICKÁ ČÁST.....</b>	<b>32</b>
<b>5 SOFTWARE PRO MONITOROVÁNÍ WI-FI SÍTÍ.....</b>	<b>33</b>
5.1 INSSIDER.....	33
<b>6 SPEKTRÁLNÍ ANALYZÁTOR WI-SPY 2.4I.....</b>	<b>35</b>
6.1 NÁSTROJE PROGRAMU.....	36
6.1.1 Planar zobrazení.....	36
6.1.2 Density zobrazení.....	37
6.1.3 Waterfall zobrazení.....	38

6.1.4	Wi-Fi síť.....	38
6.1.5	Wi-Fi kanály.....	39
6.1.6	Síla síť.....	40
6.1.7	Aktivita kanálu v čase.....	40
6.1.8	Aktivita Wi-Fi sítí na kanálech.....	41
6.1.9	3D zobrazení.....	41
<b>7</b>	<b>MONITOROVÁNÍ WI-FI SÍTÍ A ZPRACOVÁNÍ DAT.....</b>	<b>43</b>
7.1	POUŽITÉ PROSTŘEDKY.....	43
7.2	MAPA MĚŘENÝCH STANOVÍŠŤ.....	43
7.3	NAMĚŘENÁ DATA NA STANOVÍŠTÍCH.....	45
7.4	VYHODNOCENÍ NAMĚŘENÝCH DAT.....	51
	<b>ZÁVĚR.....</b>	<b>54</b>
	<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>56</b>
	<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>58</b>
	<b>SEZNAM OBRÁZKŮ.....</b>	<b>60</b>
	<b>SEZNAM TABULEK.....</b>	<b>61</b>
	<b>SEZNAM PŘÍLOH.....</b>	<b>62</b>

## ÚVOD

Není tomu dlouho, co došlo k obrovskému nárůstu používání bezdrátových technologií. Příčinou byl technologický posun, kdy ceny zařízení klesaly a výkon prudce rostl. Navíc i veškeré vyráběné součástky byly značně miniaturizovány. Hlavními výhodami bezdrátového připojení jsou cena, pohodlnost a mobilita.

S používáním těchto technologií také přichází jistá rizika, která ohrožují síť či samotného uživatele. Hrozby mohou být různého druhu, od škodlivého softwaru přes různé druhy útoků, až už mířené na bezdrátovou síť tak na samotného uživatele. Také ztráta dat může pro některé společnosti či instituce představovat nepříjemnou situaci. To je také důvodem, proč se v dnešní době rozmohly tzv. cloud služby. Spousta výrobců bezdrátových zařízení má defaultně nastaveno žádné šifrování a uživatelé, kteří nemají znalosti ve Wi-Fi sítích, tak si při nastavování neví rady a nechají síť všem přístupnou.

Odposlouchávání bezdrátových sítí je zcela legální činnost a lze se dozvědět celou řadu zajímavých a někdy i důležitých informací. Stačí pokud daná osoba disponuje Wi-Fi kartou a softwarem, jež je k tomu určený. K dispozici je několik druhů softwaru, které jsou ve většině případech volně dostupné. Softwary se liší ve funkcích a vyobrazování naměřených dat. Mezi ty základní informace se považuje název sítě, síla signálu a používané šifrování.

Bakalářská práce je rozdělena na teoretickou a praktickou část. V teoretické části je přiblížení čtenáře s problematikou Wi-Fi sítí a komponent k tomu určeným. Dále je rozdělení bezdrátových sítí nejen podle velikosti, ale i způsobu jež se v ní komunikuje. Důležitým tématem spojeným s bezdrátovými sítěmi je jejich zabezpečení. Nechceme-li aby se do naší sítě mohl připojit každý, kdo spatří název Wi-Fi sítě je nutné, aby signál, jež vyzařuje náš Wi-Fi router, byl směřován pouze do dané lokality a používal šifrování a autentizaci.

Hlavním cílem práce je monitorování Wi-Fi sítí, prostřednictvím freeware programu a verifikování rušných míst pomocí spektrálního analyzátoru Wi-Spy 2.4i, v centru města Vsetína. Přínos práce spočívá v podrobném zmapování aktivit bezdrátových sítí, síly signálů, typu používaného zabezpečení veřejností a následné vyhodnocení naměřených dat.

## **I. TEORETICKÁ ČÁST**

## 1 BEZDRÁTOVÉ SÍTĚ

V bezdrátových sítích probíhá přenos dat prostřednictvím elektromagnetického vlnění, namísto klasických elektrických signálů v metalickém kabelu či světelných signálů v optickém vlákne. Elektromagnetické vlnění má odlišnou jak vlnovou délku, tak frekvenci [1].

Použití těchto sítí se osvědčilo a staly se velice používaným přenosovým médiem. Volně dostupných frekvencí je bohužel málo, navíc pro bezdrátové sítě byly vyhrazeny 2,4 GHz a 5 GHz pásma. První z uvedených frekvencí je volně použitelné pásmo, tudíž její provoz není jakkoliv omezován. Avšak nešvarem dnešní doby je obrovské množství elektronických zařízení (mikrovlnné trouby, jiné Wi-Fi, Bluetooth atd.), která používají právě toto pásmo a dochází k rušení komunikace mezi zařízeními. Pásmo 5 GHz je oproti předešlému regulováno pravidly Českého telekomunikačního úřadu (dále jen ČTU) [1].

### 1.1 Komponenty bezdrátové sítě

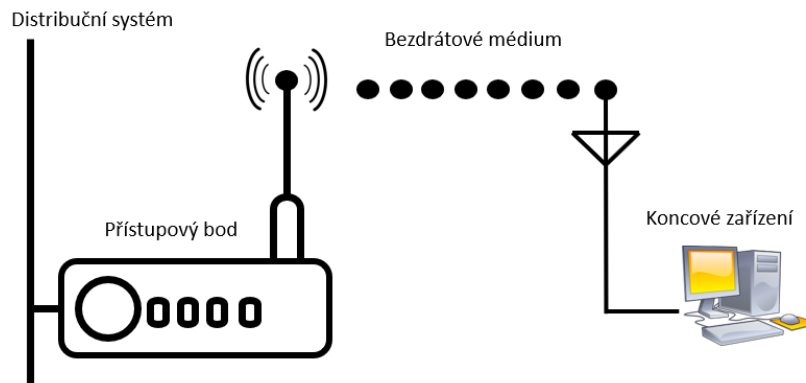
Plně funkční bezdrátová Wi-Fi síť musí být vybavena čtyřmi základními komponenty:

Distribuční systém – slouží k vzájemné komunikaci mezi více přístupovými body. Je důležité, aby směrování dat v distribučním systému bylo správně nastaveno, jinak by mohlo dojít k vytvoření smyčky a tím k nekonečnému cyklu [2].

Přístupový bod – neboli Access Point (zkráceně AP). Jedná se o zařízení, které slouží k převodu z kabelové sítě na síť bezdrátovou. Veškerá zařízení se připojují právě k přístupovému bodu. Přístupový bod zajišťuje převod signálu a také bezpečnost sítě [2].

Přenosové médium – je to přenosová cesta, po které proudí všechna data. V případě lokální sítě by to byl metalický kabel nebo optické vlákno, ale u bezdrátové technologie se používají rádiové vlny. Použitelná frekvenční pásma, která povoluje The Institute of Electrical and Electronic Engineers (dále jen IEEE), 802.11 jsou 2,4 GHz a 5 GHz [2].

Koncová zařízení – jedná se o zařízení, která mají spolu komunikovat a kvůli kterým vůbec vzniká síť (notebook, telefon, počítač atd.).



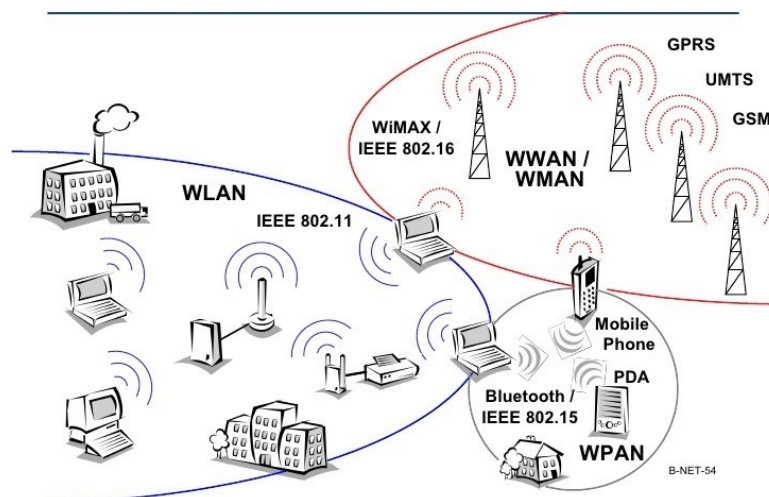
Obr. 1. Komponenty bezdrátové sítě [2], upravil Tomek 2018

## 1.2 Rozdělení bezdrátových sítí

Rozdělení bezdrátových sítí se nejčastěji provádí na základě vzdálenosti uživatele od přístupového bodu či dalšího účastníka. To je hlavním kritériem, podle kterého se sítě rozdělují. Používají se čtyři základní skupiny bezdrátových sítí.

Sítě je také možné dělit podle způsobu jejich komunikace, zda komunikují skrze určitého prostředníka (přístupový bod), to je typ infrastruktury, nebo bez přístupového bodu, to je pak síť Ad-hoc.

### Přehled bezdrátových sítí



Obr. 2. Členění bezdrátových sítí [9], upravil Tomek 2018

V praxi se však používá dělení podle jejich velikosti a je následující:

### 1.2.1 Wireless Personal Area Network

Wireless Personal Area Network běžně označována jako WPAN síť. Jedná se o kategorii bezdrátového přenosu, která disponuje velice malým dosahem, tj. přibližně do 10 metrů. Ačkoli uživatelé umožňuje bezdrátové připojení k internetu, tak se nedoporučuje její používání. Připojení k internetu prostřednictvím této sítě je prakticky možné pouze v jedné místnosti, a to jen za určitých podmínek. Prostřednictvím sdíleného připojení přes počítač, který používá odlišný typ připojení k internetu. Síť WPAN tedy není nejlepší volbou pro připojení [10].

Používá se především pro propojení zařízení mezi sebou a to režimem, který je označován jako ad-hoc. Jedná se o vzájemné propojení dvou a více účastníků, kteří jsou vůči sobě v rovnocenné pozici. To znamená, že jednotliví účastníci komunikují pouze mezi sebou a to bez použití jakéhokoli prostředníka - přístupového bodu. Nejvíce používané technologie v této kategorii jsou v současné době Bluetooth a Infrared Data Association (dále jen IrDA), v překladu infračervený port. Méně pak průmyslové technologie jako jsou, Zigbee a Ultra Wide Band. Zařízení, jež používají tyto technologie, spadají do pracovní skupiny IEEE 802.15 [10].

### 1.2.2 Wireless Local Area Network

Wireless Local Area Network, zkráceně WLAN, je termínem pro bezdrátové lokální síť. Zástupcem je Wireless Fidelity, v překladu to znamená bezdrátová věrnost, (dále jen Wi-Fi). Jedná se o certifikát, který získá výrobek, vyhovuje-li standardům IEEE a splňuje požadavky pro vzájemnou kompatibilitu s ostatními. WLAN spadá do standardizační skupiny IEEE 802.11 [10].

Výše uvedená síť se skládá z několika koncových zařízení (notebook, telefon, televize, tiskárna atd.), které jsou připojené k jednomu přístupovému bodu a jednotně adresovanému segmentu. To znamená, že všechna připojená zařízení mají přiřazenou jednoznačně identifikovatelnou adresu síťového rozhraní (dále jen IP adresu) adresu ze speciálních rozsahů pro lokální síť. Výborným příkladem WLAN sítě jsou domácnosti, kde veškerá zařízení jsou připojena k jednomu přístupovému bodu – Wi-Fi routeru [10].

Při směrování komunikace mimo lokální síť pak router provádí překlad síťových adres (NAT: Network Address Translation). Výhodou tohoto překladu je, že veškerá komunikace

s internetem probíhá pod veřejnou adresou routeru, nikterak pod adresou zařízení umístěného v lokální síti. Další výhodou NATu je pak potřeba menšího počtu unikátních IP adres a ztěžuje přímému útoku na počítač do LAN sítě z prostředí Internetu [5].

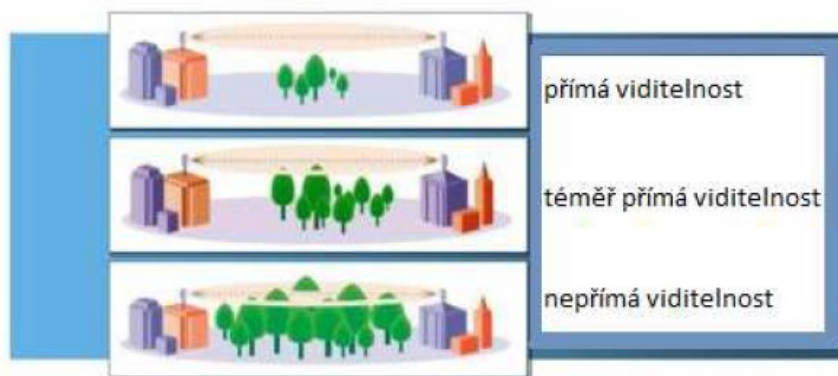
Společnost IEEE za dobu své existence vydala několik standardů. Ve většině případech šlo o navýšení maximálního teoretického datového přenosu. V některých pak o dodatečné funkce, upravující chod zařízení a jeho komunikaci.

Tab. 1. Vlastnosti standardů společnosti IEEE 802.11 [13], upravil Tomek 2018

Standard	Rok uvedení	Přenosová frekvence	Maximální teoretická přenosová rychlost
802.11	1997	2,4 GHz	1-2 Mbps
802.11a	1999	5 GHz	54 Mbps
802.11b	1999	2,4 GHz	11 Mbps
802.11g	2003	2,4 GHz	54 Mbps
802.11n	2009	2,4 / 5 GHz	600 Mbps
802.11ac	2013	5 GHz	1,35 Gbps
802.11ac Wave 2	2015	5 GHz	3,47 Gbps

### 1.2.3 Wireless Metropolitan Area Network

Jedná se o druh sítě, který byl navržen pro bezdrátový přenos v rámci metropole (velká města). V současné době tuto kategorii nejvíce zastupuje technologie Worldwide Interoperability for Microwave Access (dále jen WiMAX). WiMAX je normalizovaný společností IEEE ve skupině 802.16 a je zaměřen na bezdrátovou komunikaci v rámci metropolí. Komunikaci mezi vysílačem a přijímačem lze uskutečnit bez nutné přímé vizuální viditelnosti (technologie tzv. NLOS – Non Line Of Sight). Existuje také mód LOS, Line Of Sight – přímá vizuální viditelnost. Ten zahrnuje mimo vizuální viditelnost (pomyslná spojnice mezi vysílačem a anténou), také radiovou viditelnost, veškerý prostor v tzv. Fresnelově zóně. Použitím LOS v ideálních podmínkách jsme schopni dosáhnout většího dosahu než při NLOS [10].



Obr. 3. Fresnelova zóna a její režimy viditelnosti [4]

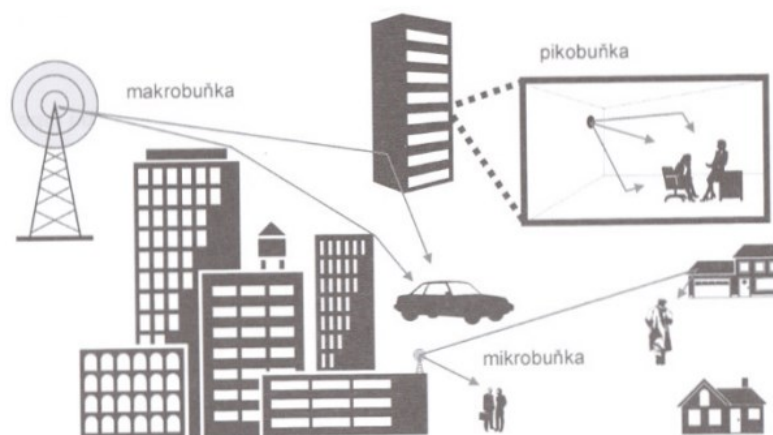
#### 1.2.4 Wireless Wide Area Network

Právě tato kategorie se odlišuje od ostatních nejen větším dosahem mezi vysílačem a přijímačem, ale také používáním pouze síťové infrastruktury pro mobilní operátory. Technologie v této kategorii poskytují nejvyšší mobilitu ze všech výše uvedených skupin [10].

Používá se především pro mobilní sítě jako jsou Global System for Mobile Communications (dále jen GSM) nebo Universal Mobile Telecommunications System (dále jen UMTS) [10].

Při použití technologií jako jsou mobilní síť, Wi-Fi nebo třeba WiMax, se setkáváme s buňkami, jakožto šířiteli signálu v síti [10].

- Pikobuňka – jedná se o šíření signálu v rámci několika desítek metrů (budovy, instituce) [10].
- Mikrobuňka – rozsah mikrobuňky je několik stovek metrů až kilometrů [10].
- Makrobuňka – pokrývá celé sídliště, dosah až 30 km [10].



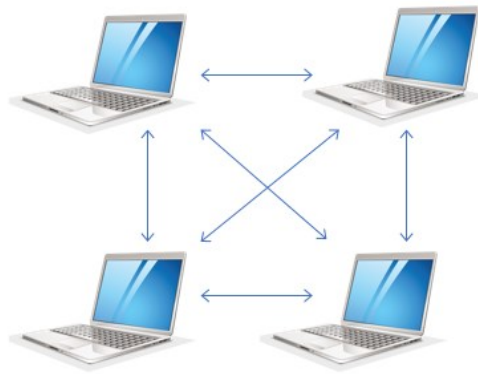
Obr. 4. Členění buněk v síti [10]

### 1.3 Topologie bezdrátových sítí

Způsobem, kterým mohou jednotlivá bezdrátová zařízení komunikovat je několik. Každé zařízení, které komunikuje bezdrátovým přenosem, musí být vybaveno vysílačem, přijímačem a anténou. Komunikace mezi jednotlivými zařízeními probíhá přes přístupový bod, který vytváří pro účastníky síťovou relaci, do které se daná zařízení připojují nebo prostřednictvím přímého spojení [3].

#### 1.3.1 Síť Ad – Hoc

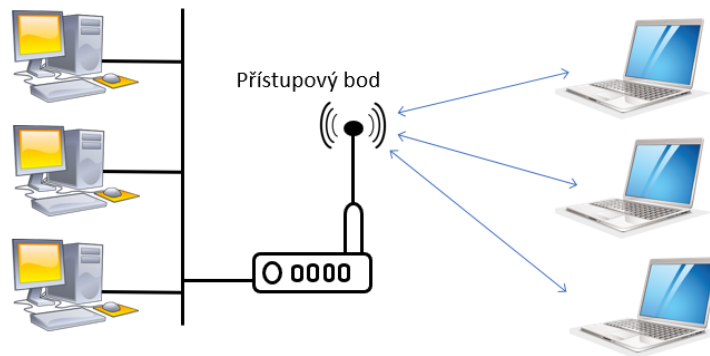
Sítě typu Ad-Hoc fungují v režimu Independent Basic Service Set (dále jen IBSS) a bývají nazývány jako nezávislé. Jednotlivá zařízení komunikují v síti přímo mezi sebou bez použití jakéhokoliv přístupového bodu. V případě propojení dvou a více zařízení (v rámci jednotek), jsou sítě typu Ad – Hoc nejjednodušší variantou. Velikost sítě se odvíjí od vzdálenosti jednotlivých zařízení, ty musí být ve vzájemném rádiovém dosahu. Použití této sítě je vhodné pro krátkodobé nebo dočasné užití, nikoli jako trvalou síť. Tyto sítě nejsou velké a nejčastěji se používají pro vytvoření sítě v rámci místnosti [3].



*Obr. 5. Ad – Hoc struktura [2],  
upravil Tomek 2018*

### 1.3.2 Síť Infrastruktura

Komunikace v síti neprobíhá přímo mezi jednotlivými zařízeními, jako bylo v předchozím případě, ale prostřednictvím přístupového bodu. Síť vždy obsahuje alespoň jeden takový přístupový bod, ke kterému se připojují ostatní zařízení. Veškerá komunikace je tedy uskutečňována právě přes tento uzel [3].



*Obr. 6. Infrastruktura [6], upravil Tomek 2018*

## 2 ZABEZPEČENÍ WI-FI SÍTÍ

Nevýhodou bezdrátových sítí je, že není nějak technicky možné omezit prostor, ve kterém se lze připojit k síti. U drátových sítí je nutné mít přístup právě k danému kabelu, aby bylo možné komunikaci odposlouchávat. Ale u bezdrátových sítí postačuje být v dané lokalitě, kde se signál vyskytuje. V některých případech se může jednat dokonce i o několik kilometrů od vysílače. Je tedy vhodné zavést bezpečnostní opatření, která budou zabraňovat možným útokům, vniknutí do sítě nebo její odposlouchávání [7].

Autentizace – ověření totožnosti, zda se jedná o osobu, za kterou se vydává.

Kódování – šifrování dat a veškeré komunikace.

### 2.1 Autentizace

Ověřování osob, zda mají oprávněný přístup do sítě, patří k důležité součásti k zajištění bezpečnosti sítě. Při použití metalického kabelu či optického vlákna není až tak obtížné zamezit přístupu neoprávněným osobám. Avšak v případě bezdrátových sítí, kde se lze připojit v podstatě z jakéhokoliv místa, kde je dostatečný signál, je zamezení přístupu těmto osobám zcela obtížnější. Pro ověření totožnosti se v bezdrátových sítí používají převážně tyto metody [2].

Autentizace otevřená – je nejjednodušší metodou autentizace, kterou je možné se do bezdrátové sítě připojit. Funguje následovně-klient zašle přístupovému bodu žádost na autentizaci spolu se svými údaji. Přístupový bod odpoví klientovi a následně mu je umožněn přístup do sítě, ovšem pokud mu není předem zakázán. Nepoužívá se zde žádné heslo, tudíž se její využití najde především u bezplatných veřejných sítí např. obchodních center, restaurací apod. [2].

Autentizace se sdíleným/před sdíleným klíčem – tento typ autentizace se používá spolu s bezpečnostním protokolem Wired Equivalent Privacy (dále jen WEP). Na rozdíl od otevřené autentizace je pro přístup do sítě nutné znát WEP klíč. Autentizace se sdíleným klíčem funguje následovně. Klient pošle požadavek o autentizaci přístupovému bodu. Přístupový bod odešle náhodně vygenerovaný řetězec dat zpátky klientovi. Klient jej přijme a pomocí WEP klíče tento řetězec zašifruje a zpátky odešle přístupovému bodu. Bude-li tento řetězec shodný s kopií správně zašifrovaným řetězcem v přístupovém bodě, tak autentizace proběhla úspěšně a klientovi bude následně umožněn přístup do sítě [2].

Nevýhodou sdíleného klíče je, že WEP používá statický klíč, který je po celou dobu autentizace stejný. Pro potenciálního útočníka pak není obtížné danou síť zcela ovládnout [2].

Autentizace s před sdíleným klíčem neboli Pre - Shader Key zkráceně PSK, je mnohem více odolnější kvůli použití protokolu Temporal Key Integrity Protocol, zkráceně TKIP. Komunikace obou zařízení je skoro stejná, liší se pouze v několika věcech. Asi největší změnou je, že protokol TKIP zajišťuje dynamicky se měnící klíč. Pro připojení do sítě klient opět použije předem zvolený klíč, stejně jako v předchozím případě. Pak však dojde k vytvoření nových, dočasných klíčů. Tato úprava autentizace pak ztěžuje útočnickovi podmínky pro zjištění hesla [2].

IEEE 802.1x – Předchozí dvě možnosti autentizace, ač pro mnohé domácnosti a provozovatele restauračního zařízení vhodné, tak nenabízí zrovna nejlepší stupeň zabezpečení, protože standard IEEE 802.11 a jeho dodatečné úpravy neobsahují jiné možnosti řízení přístupu a je zapotřebí použít jiný standard [2].

Bezpečnostní standard IEEE 802.1x nám poskytuje nové možnosti správy autentizace. Mezi největší výhody patří zejména pohodlná správa vysokého počtu uživatelů. Každý uživatel vlastní svůj pár přihlašovacích údajů nebo klientský certifikát. Oproti předchozím metodám, kde vystupovali pouze dva účastníci a tj. klient a přístupový bod, tak zde přibývá další účastník-autentizační server. Ten porovnává získané přihlašovací údaje od klienta s daty uloženými v paměti autentizačního serveru, popř. v externí databázi. Ten ze získaných dat od klienta rozhodne, jestli mu bude umožněn přístup do sítě. Dalšími výhodami tohoto standardu je jednoznačná identifikace uživatele, který se chce do sítě připojit, dále ověření samotného přístupového bodu, zda nedochází k záměně, útočnick-přístupový bod. Autentizační server dále zahrnuje funkci Authentication Authorization and Accounting, zkráceně AAA [2, 11].

## 2.2 Šifrování

Šifrování se používá pro preventivní ochranu dat před neautorizovaným únikem informací a k celkovému zvýšení úrovně bezpečnosti. Provádí se v těchto vrstvách síťové infrastruktury:

- v aplikační vrstvě (PGP),
- v transportní vrstvě (TLS/SSL),
- v síťové vrstvě (IPsec) [7].

V šifrování se lze setkat se dvěma základními typy šifrování, tj. symetricky – soukromým klíčem a asymetricky – soukromým a veřejným klíčem.

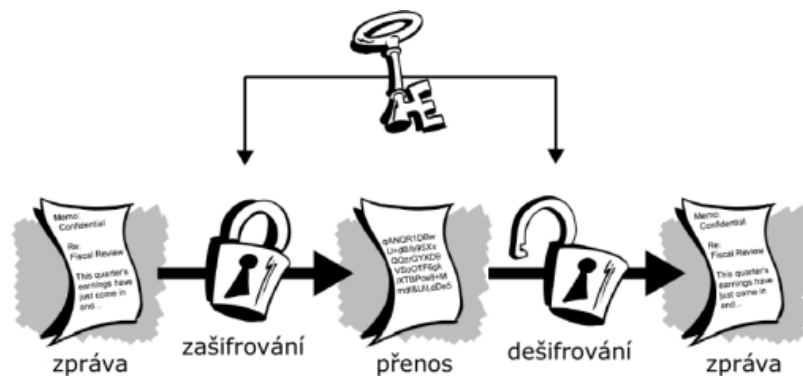
### 2.2.1 Symetrické šifrování

V symetrické kryptografii se k šifrování i dešifrování používá pouze jeden klíč. Je tedy zapotřebí dostat klíč od odesílatele k příjemci bezpečným způsobem tak, aby příjemce mohl zprávu dešifrovat [8].

Výhodou symetrického šifrování je jeho jednoduchost šifrovacího a dešifrovacího algoritmu spolu s jeho rychlostí, ta se pohybuje přibližně 100–200 i více Mbit/s [8].

Nevýhodami je nutnost sdílení klíče předem nebo při inicializaci komunikace. A při komunikaci s více stranami je pak nutnost velkého množství klíčů [8].

V současné době se používá šifrovací algoritmus AES (Advanced Encryption System). AES se používá s těmito délkami klíčů: 128, 196 a 256 bitů [8].



Obr. 7. Symetrické šifrování [8]

### 2.2.2 Asymetrické šifrování

Asymetrickým šifrováním se vyřešil problém s distribucí klíče k adresátu. Používají se zde dva klíče, veřejný a privátní. Tím odpadá potřeba dostat jeden tajný klíč na druhou stranu k příjemci [8].

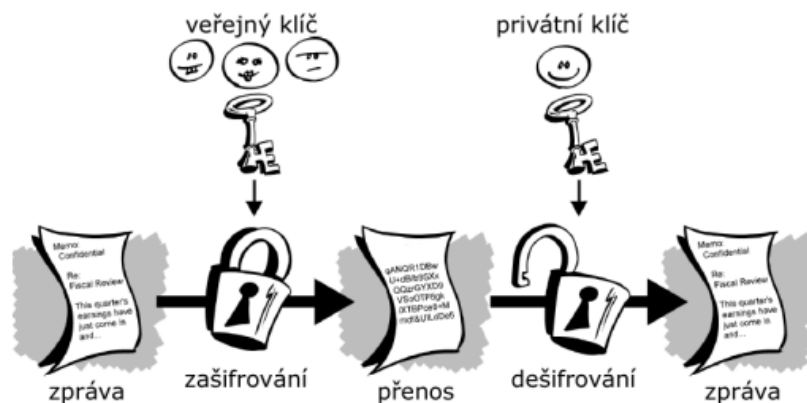
Každá ze stran má jeden pár klíčů, veřejný a privátní. Veřejný klíč musí znát každý, zatímco privátní je soukromý a zná jej pouze majitel [8].

Zpráva je tedy zašifrována veřejným klíčem adresáta. Ten obdrží zašifrovanou zprávu a dešifruje svým privátním klíčem. Žádná jiná osoba zprávu nedešifruje, protože nemá privátní klíč z daného klíčové páru [8].

Mezi nejpoužívanější algoritmy patří metoda RSA, pojmenována podle počátečních písmen autorů Rivest, Shamir a Adleman. Ta používá Malou Fermatovu větu a modulární aritmetiku. Modulární aritmetika se zabývá zbytky po dělení celých čísel. Šifra je založena na tom, že prozatím nebyl objeven rychlý způsob, jak rozložit velká čísla na prvočinitele. Pokud by se takový způsob objevil, od používání této šifry by se pravděpodobně upustilo [8].

Výhodou asymetrického šifrování je, že odpadá nutnost přenosu-sdílení klíče. Dále pro více uživatelů není potřeba tolik klíčů, postačuje pouze jeden klíčový pár [7].

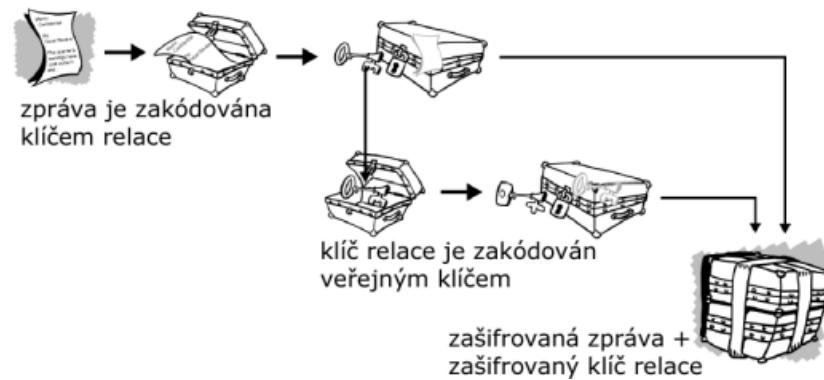
Nevýhodou asymetrického šifrování jsou velmi vysoké výpočetní náklady a s tím spojená nízká rychlost (přibližně 100x pomalejší než symetrická) [7].



Obr. 8. Asymetrické šifrování [8]

### 2.2.3 Hybridní šifrování

Náročné matematické operace a velké požadavky na výkon počítač, to jsou nevýhody asymetrického šifrování. Proto se začalo používat kombinace symetrického a asymetrického šifrování, tzv. hybridního způsobu. Využívá se výhod z obou způsobů, rychlost a jednoduchoť symetrického a praktičnost asymetrického [8].



Obr. 9. Hybridní šifrování [8]

Odesílatel zvoleným klíčem symetricky zašifruje zprávu. Tento klíč zašifruje veřejným klíčem příjemce a odešle jej dohromady se zprávou příjemci. Příjemce pak obdrží asymetricky zašifrovaný klíč a symetricky zašifrovanou zprávu. Klíč lze dešifrovat pouze privátním klíčem příjemce a získaným klíčem pak dešifruje zprávu. Tímto způsobem nevzniká problém s distribucí klíče při symetrickém šifrování a zároveň se celý proces urychlí [8].

### 3 HROZBY A ÚTOKY NA WI-FI SÍŤ

V kapitole se pojednává o možných útocích a hrozbách na zabezpečení Wi-Fi sítě. Jsou zde popsány způsoby a principy jednotlivých druhů útoků. Od prolomení klíče hrubou silou či slovníkovým útokem, záměnu MAC adresy přes odposlouchávání komunikace a DoS a DDoS útoky. Nutno říci, že ne všechny útoky slouží primárně k získávání dat nebo neoprávněného přístupu do sítě. Ale i k zamezení jakékoliv komunikace v síti.

#### 3.1 Zjištění klíče

Pro rozluštění klíče, kterým je zabezpečena Wi-Fi síť, existuje několik druhů softwaru, mezi nejznámější patří program AirSnort, který je open source nebo WEPCrack. Programy pasivně odposlouchávají komunikaci mezi zařízeními a po shromáždění dostatečného počtu paketů se snaží vypočítat šifrovací klíč. Pro zdárné zjištění klíče touto metodou je nutné, aby nedocházelo ke změně klíče během zachytávání komunikace [2].

Možnou obranu proti tomuto druhu útoku nám nabízí Virtual Private Network (dále jen VPN). VPN je systém propojujících počítačů do zabezpečené soukromé sítě. Mezi počítači se vytvoří šifrovaný tunel, přes který se komunikuje. Často se používá pro bezpečné připojení do firemní sítě ze vzdáleného místa. Je nutno vědět, že data nejsou šifrováním kompletně chráněna. Princip fungování VPN je následující: přes VPN klienta jsou data zašifrována a odeslána na VPN server poskytovatele, ten data dešifruje a odešle cílovému zařízení. Komunikace opačným směrem funguje stejně. Výhodami toho připojení je právě určitá anonymita, tzn. že ani váš poskytovatel internetu nevidí jaké stránky navštěvujete nebo s kým v internetu komunikujete. Dále ani stránka vámi navštěvovaná nevidí vaši skutečnou IP adresu. Obě komunikující strany znají pouze adresu VPN serveru.

#### 3.2 Zjištění MAC adresy

Media Access Control (dále jen MAC) adresa, je to fyzická adresa, která slouží pro jednoznačné identifikování síťového zařízení. Způsob útoku na bezdrátovou síť je obdobný jako u předešlého typu. Útočník zpočátku odposlouchává komunikaci mezi uživatelem a AP. Poté si vyhledá MAC adresu uživatele, a tou pak přepíše svoji a začne vystupovat jako autorizovaná osoba [2].

Předejit tomuto druhu útoku lze použitím ověřovacích mechanismů nebo VPN serveru [2].

### 3.3 Útok Man-in-the-middle

Jedná se o poměrně náročný druh útoku. V překladu znamená „Muž uprostřed“, protože útočník se vydává za AP a klienta zároveň. Pro klienta se útočník vydává za AP a pro opravdové AP jako klient. Přes útočníka tedy proudí veškerá komunikace a tím získává veškeré informace. Komunikaci pak může jakkoliv filtrovat, řídit nebo dokonce ovlivňovat. Dále to útočníkovi umožňuje posílat deautentizační rámce, kvůli kterým dochází k opakovanému odpojení klienta od skutečného AP [2].

Jako preventivní obranu lze opět použít VPN server a autentizační protokol 802.1x. Jinak je vhodné mít mapu připojených zařízení ve své síti a jednou za čas překontrolovat, zda se někde neobjevilo cizí AP [2].

### 3.4 Slovníkový útok

Jak už z názvu vyplývá, k útoku se používá slovník, databáze přihlašovacích jmen a hesel, a snaží se prolomit zabezpečení. Na internetu je dostupných několik open source programů. Ty pomáhají odhalit právě tyto přihlašovací jména a hesla. Pro české uživatele a správce sítí je výhodou, že tyto databáze tvoří uživatelská jména a hesla anglických názvů. Proto když je v uživatelském účtu obsažen prvek české abecedy, je to další výhoda, která zvyšuje bezpečnost uživatele [2].

Uživatelovu bezpečnost proti tomuto útoku lze zvýšit bezpečným heslem. Bezpečné heslo by mělo být dlouhé 16-32 znaků a mělo by obsahovat prvky, malých i velkých písmen, čísel a symbolů.

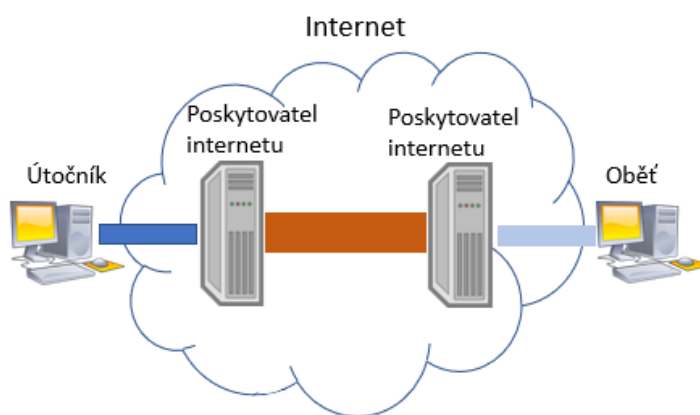
### 3.5 DoS a DDoS útoky

Denial of Service (dále jen DoS) a Distributed Denial of Service (dále jen DDoS) útoky, v překladu znamenají odmítnutí/zamítnutí služby. Útoky jsou si sobě velice podobné, liší se pouze v počtu používaných zařízení k útoku.

DoS a DDoS útoky spočívají v zahlcení sítě nebo přímo routeru oběti obrovským množstvím nepotřebných dat nebo operací a tím znemožnit jakoukoliv komunikaci v síti. Útočník může opakovaně posílat AP zbytečné žádosti o připojení. Přístupový bod pak musí všechny tyto žádosti vyhodnotit a odmítnout. Tímto způsobem lze přístupový bod zahltit natolik, že potom nestíhá odpovídat na žádosti pro přihlášení oprávněných uživatelů v reálném čase a tím dochází ke ztrátě plnění funkce bezdrátové sítě. Cílem těchto útoků je ve většině případů

vyřadit z provozu cílený server, jeho služby nebo celou síť. Následkem těchto druhů útoku bývá v menším případě snížení rychlosti sítě, v horším případě totální nefunkčnost a následný restart serveru [2].

V prvním z uvedených útoků, DoS, používá útočník pouze jedno zařízení, které zahlcuje síť nebo přístupový bod nepotřebnými žádostmi o připojení, popř. jinými zbytečnými daty.



Obr. 10. Denial of Service útok

Typy DoS útoků:

**Ping of Death** – už patří mezi starší typy útoků, protože snad všichni výrobci operačních systémů provedli opatření, které tomuto útoku zabráňují. Samotný příkaz se běžně používá a ověřuje se jím, zda vzdálené zařízení pracuje. Útočník použije příkaz ping a vytvoří paket, který je větší než maximální povolená velikost ve standardech IP protokolu tj. 65 536 bajtů a větší. Útočník pak pošle tento paket do sítě, jež chce poškodit. Tento útok může způsobit zamrznutí nebo restart celého systému.

**Teardrops attack** – jedná se o novější typ útoku a využívá chyby při opětovném sestavování fragmentů IP paketu. Datový paket je během své cesty rozložen na několik dalších menších paketů a po internetu cestují, jakožto původní IP pakety. Pakety obsahují položku offset, která říká, kde daný paket patří v rámci opětovném sestavování. Poté co se pakety na koncovém zařízení zpětně sestaví, je možné že některé systémy zamrznou nebo se restartují.

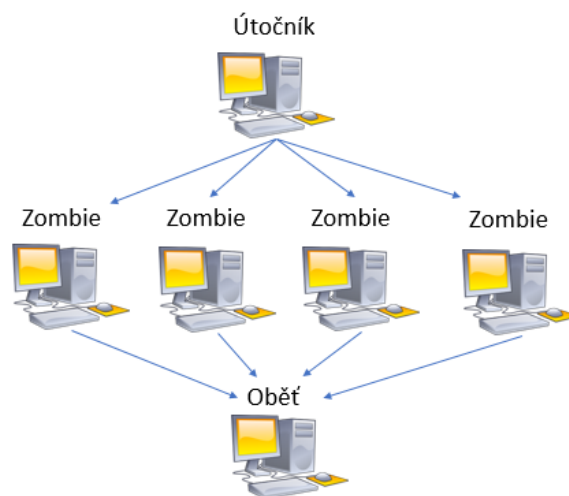
**SYN attack** – využívá způsobu, jakým se navazuje spojení TCP/IP protokolu. Tomuto procesu se říká „třífázový handshaking“ neboli three way handshake. Tento proces funguje na způsobu potvrzování. Zařízení, které chce komunikovat nebo posílat data, pošle příjemci synchronizační paket SYN. Příjemce odpoví potvrzovacím paketem TCP SYN-ACK, a na

tento paket poté iniciátor odpoví potvrzovacím paketem ACK. Proběhne-li vše v pořádku, tak zařízení jsou připravena posílat data.

Při tomto druhu útoku hacker zahlučuje příjemce TCP SYN paketama. Každým odeslaným paketem dochází k tomu, že cílové zařízení odešle odpověď SYN ACK a bude čekat na potvrzovací paket ACK, který má obdržet. Zatímco systém čeká na ACK, zařadí všechny nevyřízené SYN ACK odpovědi do fronty. Poté, co se naplní paměť pro žadatele, systém začne ignorovat veškeré příchozí SYN žádosti.

**Smurf útok** – jedná se o starší typ útoku, jež býval jeden z nejvíce používaných, dokud nebyla změněna konfigurace zařízení. To potom vedlo k nepoužitelnosti těchto útoků. Jedná se o zesílený útok, kdy se posílá paket se zdrojovou IP adresou oběti na broadcastovou adresu sítě. Příklad útoku. Síť, ve které se nacházíme je 192.168.0.0 s maskou 255.255.255.0 tj. 254 možných adres pro zařízení. Pošle se ping na broadcastovou adresu 192.168.0.255 a pokud v síti funguje smurf útok, dostaneme 254 odpovědí. V případě, že tento útok bude proveden v síti, kde je 65 534 adres, dojde k nárazovému datovému toku v síti, což může vést k restartu sítě. Jak už bylo na začátku řečeno, tento útok by v dnešní době neměl být použitelný na většině zařízeních.

Ve druhém ze zmíněných útoků, DDoS, používá útočník taky jedno zařízení, avšak tím napadne několik dalších zařízení (desítky až tisíce). Ty ve většině případech ani netuší že je u nich nainstalován škodlivý software tzv. zombie. A tyto napadené zařízení (zombies), společně zahlučují útočníkem vybranou síť.



Obr. 11. Distributed Denial of Service útok

### 3.6 Skenování sítí

S příchodem Wi-Fi sítí přišlo i jejich odposlouchávání. Bezdrátové Wi-Fi sítě lze odposlouchávat mnoha způsoby např. warstrolling, to je metoda odposlouchávání sítí za chůze. Metoda wardriving je zase způsob odposlouchávání za jízdy autem. Takových metod je několik a jsou různě technicky náročné např. warboating (za jízdy na lodi) nebo warflying (za letu).

Jedná se o zcela legální činnost, kdy „útočník“ různými metodami skenuje volně dostupné informace bezdrátových sítí, tak aniž by síť byla, jakkoliv využita. „Útočník“ zaznamenává hlavně typ zabezpečení bezdrátové sítě, MAC adresy zařízení v síti, název sítě, aktivní kanály apod.

Warchalker je osoba, která chodí v terénu s laptopem nebo s Personal Digital Assistant, zkráceně PDA a chová se určitým způsobem podezřele. Před skenováním sítí mnohdy mění svou MAC adresu, v ideálním případě ji periodicky mění.

Pro monitorování Wi-Fi sítí v dnešní době existuje celá řada programů, ať už pro operační systém Windows tak i Linux. Pro uživatele Windows je vhodná volba programu inSSIDer, jedná-li se o starší verze systému tak se doporučuje NetStumbler. Pro Linuxové uživatele je k dispozici program Kismet a Aircrack-ng.

Tímto monitorováním lze vytvořit obsáhlou databázi s výše uvedenými údaji a zveřejnit ji s GPS pozicemi.

## 4 CHARAKTERISTIKA ANTÉN VE WI-FI SÍTÍCH

Použití Wi-Fi se osvědčilo především ve vnitřních prostorech, avšak nejen zde našlo své uplatnění. Používá se také při propojení i několika kilometrů od sebe vzdálených bodů, nebo na českém telekomunikačním trhu pro připojení klienta v posledním úseku, kde to je jiným způsobem neřešitelné nebo finančně náročné [2].

Kvalitní pokrytí plochy Wi-Fi sítí nespočívá jen v použití drahé a výkonné antény. Pravým smyslem antény je nasměrovat vyzařovaný signál určitým směrem nebo tvarem do dané lokality.

### 4.1 Parametry

To, jak se budou antény v provozu chovat, se odvíjí od jejich provozních a výkonnostních charakteristik. Proto je každá anténa v závislosti na své délce vhodnější pro jinou vysílací a přijímací frekvenci. Každá anténa svým vyzařováním vytváří tzv. vyzařovací diagram. Pro lepší zobrazení oblasti, kterou anténa pokrývá se vyzařovací diagram vykresluje do několika směrů [2].

Při výběru antény jsou nejdůležitější tyto parametry:

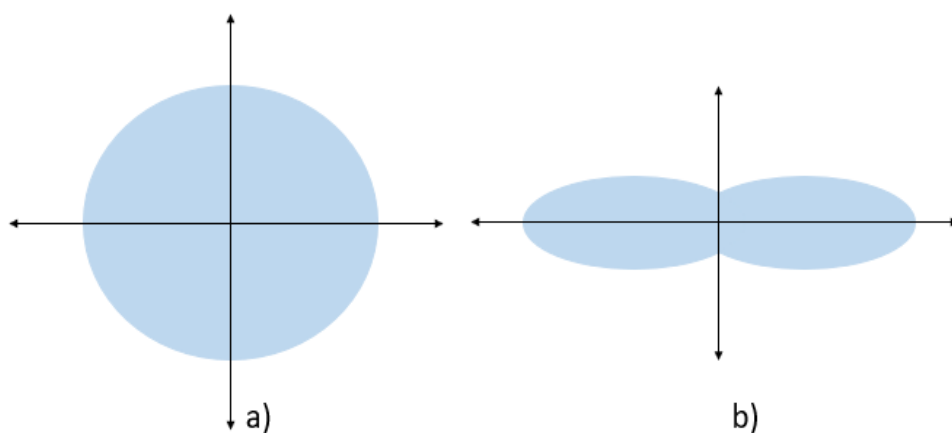
- směrovost – vyzařovanému elektromagnetickému poli udává, v jakém směru a pod jakým úhlem dokáže přijímat a vysílat,
- polarizace – udává, v jaké rovině se bude šířit signál. Jsou dva základní typy šíření, a to kruhová polarizace a lineární. Pro lineární šíření existují dva typy, horizontální a vertikální,
- zisk antény – měří se v decibelech na isotop, jednotkou je dBi. S rostoucí ziskovostí antény roste vzdálenost, kterou anténa pokryje svým signálem. V podstatě jde o poměr intenzit vyzařování v daném směru k intenzitě rovnoměrného vyzařování do všech směrů [2],
- frekvence – taktéž důležitým parametrem a udává, v jakém frekvenčním pásmu bude daná anténa fungovat. Existují antény pro 2,4 GHz nebo pro 5 GHz pásma nebo tzv. dual-band antény, které dokážou pracovat v obou frekvenčních pásmech [10].

### 4.2 Typy antén

Nezákladnější dělení antén je podle jejich směrovosti. Jsou tři základní typy a tj. všesměrové, sektorové a směrové.

#### 4.2.1 Všesměrové antény

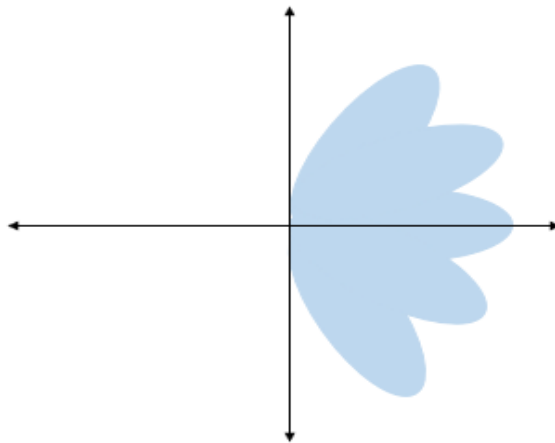
Tento druh antén šíří signál kolem sebe do všech stran a pokrývá úhel 360 stupňů v horizontálním řezu. V ideální situaci by tvar pokrytí byla kružnice, jenže vzhledem k různým překážkám, např. povětrnostní podmínky, počasí nebo prostředí, ve kterém je signál vyzařován, to bývá mnohdy křivá kružnice. Ve vertikálním směru je úhel šíření signálu dosti rozdílný. Vyzařovaný diagram se jeví jako tvar prstence. Tyto antény se používají v prostředí, kde je potřeba rovnoměrného pokrytí a umisťují se např. na sloupy, stropy, stožáry [2].



Obr. 12. Vyzařující diagram všesměrové antény a) v horizontálním směru b) ve vertikálním směru [12], upravil Tomek 2018

#### 4.2.2 Sektorové antény

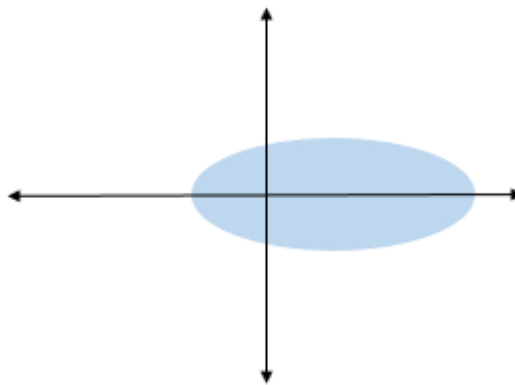
Sektorové antény vyzařují signál do určitého úhlu, většinou to je 30–120 stupňů, maximálně však 180 stupňů v horizontální i vertikální rovině. Tyto antény najdou využití v prostorech, kde je potřeba vykrytí prostoru ve speciálně tvarované oblasti nebo pokud nechceme, aby signál pronikl mimo žádanou oblast [2].



*Obr. 13. Vyzařující diagram sektorové antény [12],  
upravil Tomek 2018*

#### 4.2.3 Směrové antény

Jak už z názvu vyplývá, směrová parabolická anténa soustředí signál do určitého bodu, který může být od antény vzdálený až několik kilometrů. Tím, že je anténa směřována do jednoho bodu, musí mít velkou ziskovost, a naopak malou směrovost. Úhel, kterým anténa vysílá a přijímá nebývá větší než 10 stupňů. Tyto antény najdou své využití na střechách domů [2].



*Obr. 14. Vyzařující diagram směrové antény [12],  
upravil Tomek 2018*

### 4.3 Problémy se šířením signálu ve Wi-Fi sítích

V dnešní době moderních technologií existuje mnoho faktorů, které mohou přímo nebo nepřímo ovlivnit šíření rádiových signálů ve Wi-Fi síti.

#### 4.3.1 Vytížené frekvenční pásmo

Frekvenční pásmo, které využívá většina Wi-Fi sítí, 2,4 GHz poskytuje pouze tři na sobě nezávislé kanály z celkových třinácti (určené pro Evropu). Jedná se o kanály 1, 6 a 13. Počet nepřekrývajících se kanálů je velmi omezen, a proto najít takové pásmo, které se nepřekrývá a nezpůsobuje rušení komunikace je mnohdy obtížné, někdy až nemožné. Navíc, počet zařízení používajících tuto frekvenci stále roste. V dnešní době nejen telefony a notebooky používají bezdrátovou síť, ale i inteligentní lednice, hodinky, televize apod.

Tab. 2. Využívané kanály v Evropě  
pro 2,4 GHz [11], upravil Tomek 2018

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

### 4.3.2 Viditelnost

V prostoru mezi anténami by měla být zajištěna přímá viditelnost, jinak může nastat situace, kdy síť začne padat nebo vznikat chyby během komunikace. Možnými překážkami v přímé viditelnosti, které mají velký vliv na kvalitu spojení, jsou primárně železobetonové stavby, cihlové budovy ale také stromy, hlavně po dešti. Na kvalitu signálu má také negativní vliv počasí, zejména silné deště a průtrž mračen, méně pak sněžení. Voda totiž absorbuje signál a to vede ke snížení kvality pokrytí.

## **II. PRAKTICKÁ ČÁST**

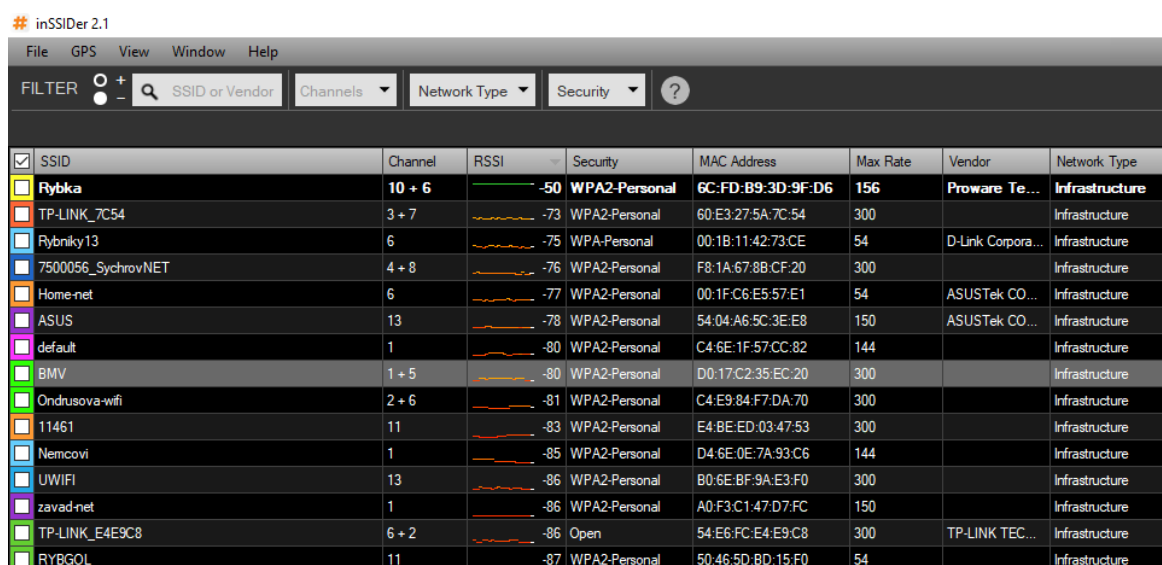
## 5 SOFTWARE PRO MONITOROVÁNÍ WI-FI SÍTÍ

Jak už bylo v předchozích kapitolách zmíněno, pro bezdrátovou síť Wi-Fi jsou vyhrazená určitá frekvenční pásma tj. 2,4 GHz a 5 GHz a určité kanály 1–13 (pro Evropu). Pro správný chod sítě je vhodné dbát několika zásad. Je důležité předcházet vzájemnému rušení sítí. Jedná se především o vysoce obydlené oblasti a místa, kde je vysoká pravděpodobnost výskytu dalších Wi-Fi sítí, např. obchodní centra.

Wi-Fi síť lze monitorovat několika druhy softwaru. Mezi ty nejzákladnější patří tzv. podpůrné programy, které bývají součástí síťové karty nebo operačního systému. Použitím daného softwaru se lze dostat k informacím o dané Wi-Fi síti. Cílem kapitoly je stručně popsat nejpoužívanější software pro monitoring Wi-Fi sítí.

### 5.1 inSSIDer

Jedná se o produkt od společnosti MetaGeek, který je dostupný v několika verzích. inSSIDer umožňuje vidět detailnější informace o Wi-Fi sítích, které jsou ve vašem okolí. Po zapnutí programu se zobrazí poměrně jednoduché prostředí, ve kterém lze najít základní informace skenovaných Wi-Fi sítí. V programu můžeme najít SSID (název sítě), MAC adresu, sílu signálu, používaný kanál, zabezpečení, maximální propustnost sítě, typ zařízení. Každá vyobrazená síť má od ostatních odlišnou barvu, pomocí které je práce s grafy mnohem jednodušší. Na základě získaných informací z programu můžeme najít vhodný přenosový kanál a nastavit Wi-Fi router tak, aby se co nejméně překrýval se zbylými routery.



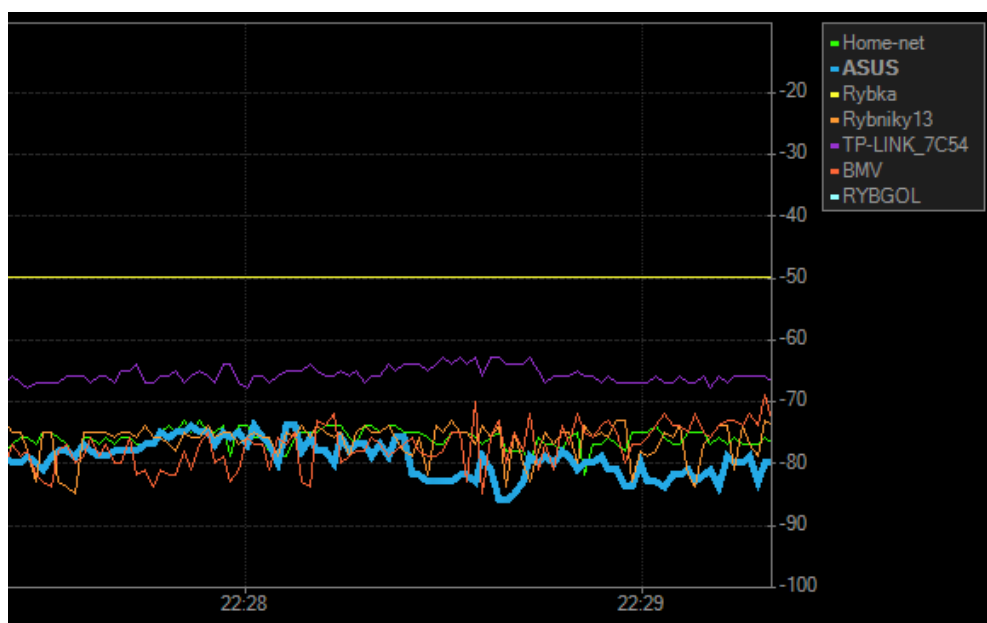
The screenshot shows the inSSIDer 2.1 application window. The interface includes a menu bar (File, GPS, View, Window, Help), a filter section with a search box for 'SSID or Vendor', and dropdown menus for 'Channels', 'Network Type', and 'Security'. Below this is a table of detected Wi-Fi networks. Each row represents a network with columns for SSID, Channel, RSSI (with a signal strength graph), Security, MAC Address, Max Rate, Vendor, and Network Type.

SSID	Channel	RSSI	Security	MAC Address	Max Rate	Vendor	Network Type
Rybka	10 + 6	-50	WPA2-Personal	6C:FD:B9:3D:9F:D6	156	Proware Te...	Infrastructure
TP-LINK_7C54	3 + 7	-73	WPA2-Personal	60:E3:27:5A:7C:54	300		Infrastructure
Rybniky13	6	-75	WPA2-Personal	00:1B:11:42:73:CE	54	D-Link Corpora...	Infrastructure
7500056_SychrovNET	4 + 8	-76	WPA2-Personal	F8:1A:67:8B:CF:20	300		Infrastructure
Home-net	6	-77	WPA2-Personal	00:1F:C6:E5:57:E1	54	ASUSTek CO...	Infrastructure
ASUS	13	-78	WPA2-Personal	54:04:A6:5C:3E:E8	150	ASUSTek CO...	Infrastructure
default	1	-80	WPA2-Personal	C4:6E:1F:57:CC:82	144		Infrastructure
BMV	1 + 5	-80	WPA2-Personal	D0:17:C2:35:EC:20	300		Infrastructure
Ondrusova-wifi	2 + 6	-81	WPA2-Personal	C4:E9:84:F7:DA:70	300		Infrastructure
11461	11	-83	WPA2-Personal	E4:BE:ED:03:47:53	300		Infrastructure
Nemcovi	1	-85	WPA2-Personal	D4:6E:0E:7A:93:C6	144		Infrastructure
UWIFI	13	-86	WPA2-Personal	B0:6E:BF:9A:E3:F0	300		Infrastructure
zavad-net	1	-86	WPA2-Personal	A0:F3:C1:47:D7:FC	150		Infrastructure
TP-LINK_E4E9C8	6 + 2	-86	Open	54:E6:FC:E4:E9:C8	300	TP-LINK TEC...	Infrastructure
RYBGOL	11	-87	WPA2-Personal	50:46:5D:BD:15:F0	54		Infrastructure

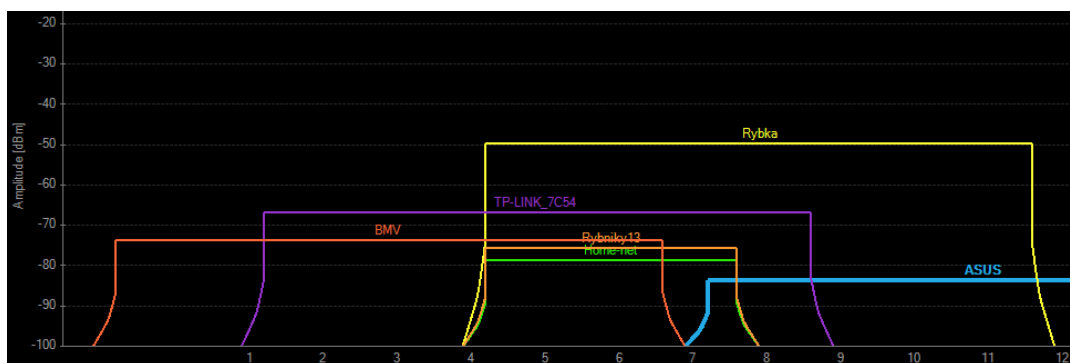
Obr. 15. inSSIDer – zobrazené Wi-Fi sítě a jejich parametry

Práce s programem je jednoduchá a díky barevnému rozlišení všech dostupných sítí na černém pozadí také přehledná. V horním panelu programu jsou různé druhy filtrů, které umožňují nevyobrazovat sítě, které nechceme. Síť lze filtrovat podle jejich SSID nebo značky prodejce, dle používaného kanálu, dle síly signálu, dle zabezpečení, dle MAC adresy, dle datové propustnosti routeru nebo podle typu sítě.

Program také dokáže vykreslit časový průběh síly signálů všech vybraných Wi-Fi sítí v jednom grafu.



Obr. 16. inSSIDer – síla signálů sítí v čase



Obr. 17. inSSIDer – síla signálu a používané kanály

## 6 SPEKTRÁLNÍ ANALYZÁTOR WI-SPY 2.4I

Jedná se o cenově nejpřijatelnější software, který je určen pro všechny síťáře nebo Wi-Fi nadšence. Wi-Spy 2.4i je základní model, který je na trhu dostupný přibližně za 1 200 Kč a je vhodnou volbou pro mapování Wi-Fi sítí v okolí.

Wi-Spy 2.4i je taktéž produktem společnosti MetaGeek a spolu se softwarem inSSIDer budou použity pro monitorování Wi-Fi sítí v centru města Vsetína. Společnost MetaGeek nabízí na trhu několik dalších, odlišných spektrálních analyzátorů pro tato frekvenční pásma 900 MHz, 2,4 GHz a 5 GHz. K těmto analyzátorům je možnost dokoupit další příslušenství, např. antény nebo zesilovače. Cena vyššího modelu, který dokáže pracovat ve dvou frekvenčních pásmech najednou, je možno pořídit do 14 000 Kč. Wi-Spy DBx je nejvyšší řadou těchto analyzátorů. Tento model je vhodný pro skenování Wi-Fi a GSM sítí v oblastech, kde se předpokládá velké množství těchto sítí, tj. sídliště, centra měst nebo obchodní centra.

Wi-Spy 2,4i je vybaven Universal Serial Bus (dále jen USB), pomocí kterého je možné jej pohodlným způsobem připojit do přenosného laptopu nebo stolního počítače. Wi-Spy byl vyvinut pro vyhledání volnějšího frekvenčního pásma, pro odstranění možných problémů s připojením do sítě. Pracovat se signály je možné nejen v reálném čase, ale i z pořízeného záznamu.

Zařízení zachytává veškerou aktivitu bezdrátových sítí a vytíženost kanálů. Nejedná se pouze o Wi-Fi sítě, nýbrž i Bluetooth a mikrovlnné trouby, v podstatě všechna zařízení, která pracují na frekvenci 2,4 GHz.



Obr. 18. Spektrální analyzátor Wi-Spy 2.4i

Tab. 3. Specifikace Wi-Spy 2.4i

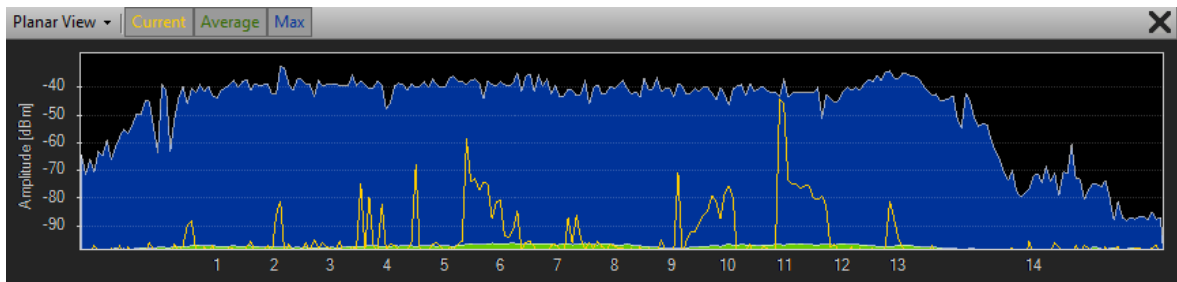
Wi-Spy 2.4i	
Anténa	interní
Frekvenční rozsah	2,400 až 2,495 GHz
Frekvenční rozlišení	373 KHz
Šířka pásma filtru	429 KHz
Rozsah amplitudy	-102 až -6,5 dBm
Rozlišení amplitudy	0,5 dBm
Software	Chanalyzer Lite

## 6.1 Nástroje programu

Pro plnohodnotné využití zařízení je potřeba doinstalovat k tomu určený software. Jedná se o Chanalyzer Lite, ten je určen pro spolupráci s tímto zařízením, navíc jeho funkčnost je závislá na připojeném zařízení do počítače či laptopu. Při každém spuštění programu dochází k automatickému mapování okolních bezdrátových sítí, resp. signálů. Získané informace jsou poté vypsány v pravé části programu. Program dokáže zjistit název sítě, používaný kanál, sílu signálu, typ zařízení, typ zabezpečení, čas prvního detekování, MAC adresu routeru, typ sítě a její maximální přenosovou rychlost.

### 6.1.1 Planar zobrazení

Planar zobrazení je základní funkce, která zobrazuje aktuální, průměrnou a maximální amplitudu v době pořizování snímku a v době jež byl pořizován. Pro přehlednější náhled jsou tyto kategorie barevně rozlišeny. Žlutá barva vykresluje momentální amplitudu, zelená barva průměrnou amplitudu a modrou barvou je zvýrazněna maximální amplituda, jež nastala v době monitorování. V náhledu je možné se přepínat mezi jednotlivými filtry. Pro zobrazení přesné frekvence je program vybaven funkcí Marker. Ten má ikonku v podobě tužky a nachází se v horní liště. Umístěním značky do požadovaného místa se dostaneme k přesným informacím o amplitudě, tyto informace jsou zobrazeny v tabulce.



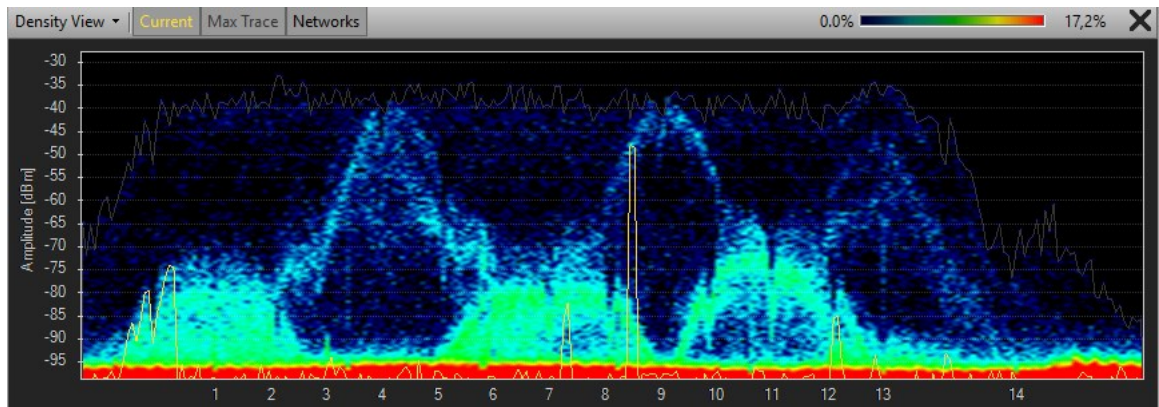
Obr. 19. Chanalyzer Lite – Planar zobrazení

Markers			
Frequency	Current	Average	Max
2 452,19	-102	-96,7	-44,5
2 461,14	-101	-97,1	-43,0
2 414,17	-98	-97,6	-42,0
2 423,49	-101	-97,9	-40,5
2 435,04	-97	-97,6	-39,0
2 445,11	-101	-98,5	-50,5

Obr. 20. Chanalyzer Lite – Markers

### 6.1.2 Density zobrazení

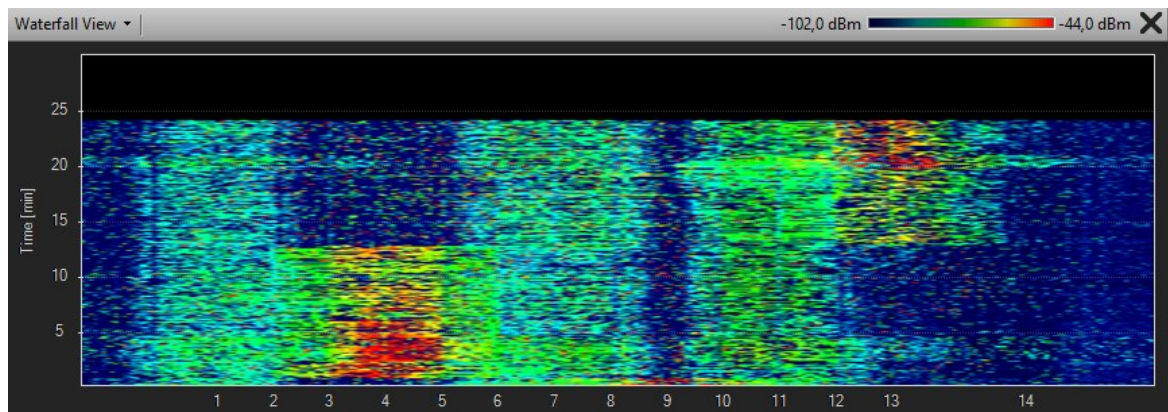
Jedná se o mapu hustoty aktivity bezdrátových sítí. Density náhled už neumožňuje zobrazení aktuální amplitudy každé frekvence, ale máme k dispozici hustotu vysílání v konkrétních frekvencích v daný čas. Hustotu vysílání, které nahradilo amplitudu, opět zobrazují barvy. Modrá barva představuje nízkou hustotu vysílání, červená pak vysokou aktivitu. Platí zde, čím větší aktivita je, tím více červené se v grafu objeví. Pro specifikování konkrétního frekvenčního bodu je k dispozici funkce Inspektor. Ta se nachází v horní části programu hned vedle nástroje Marker. V tomto náhledu je k dispozici také legenda. Ta na základě jejich barvy zobrazuje, jak moc jsou jednotlivé body vytížené.



Obr. 21. Chanalyzer Lite – Density zobrazení

### 6.1.3 Waterfall zobrazení

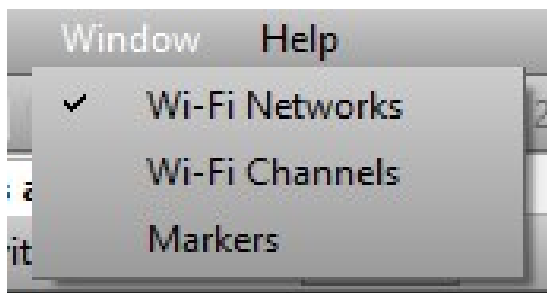
Neboli Waterfall view, zachycuje změny v čase. Tmavě modrá barva vyobrazuje slabý signál, resp. malý signál amplitudy, a naopak červená barva vyobrazuje maximum, tedy nejvyšší amplitudu. Zelená barva tedy představuje střední hodnoty ze zachyceného spektra.



Obr. 22. Chanalyzer Lite – Waterfall zobrazení

### 6.1.4 Wi-Fi sítě

Pro práci s vybranými sítěmi je v programu zabudovaná karta Wi-Fi Networks. Po kliknutí na kartu Window, se objeví tři možnosti (Wi-Fi Networks, Wi-Fi Channels a Markers), zde vybereme Wi-Fi Networks. Poté se nám objeví tabulka zobrazující sítě, kde vybereme požadovanou síť, se kterou chceme pracovat a tu si označíme. V tabulce jsou podobné informace o každém Wi-Fi routeru, jaké jsou k dostání v programu inSSIDer.



Obr. 23. Chanalyzer Lite – Window karta

Graph	SSID	Channel	RSSI	Time	Vendor	Privac	MAC Address	Supported	Max	Netwo
<input checked="" type="checkbox"/>	Rybka	6	-50	17:39:27		RS...	6cfd:b9:3d:9f:d6	6,5/16/1...	117	Infra...
<input checked="" type="checkbox"/>	BMV	1	-76	17:39:27		RS...	d0:17:c2:35:ec:20	1/2/5,5/...	18	Infra...
<input checked="" type="checkbox"/>	TP-LINK_7C54	1	-77	17:39:27		RS...	60:e3:27:5a:7c:54	1/2/5,5/...	11	Infra...
<input checked="" type="checkbox"/>	default	1	-78	17:39:24		RS...	c4:6e:1f:57:cc:82	1/2/5,5/...	18	Infra...
<input checked="" type="checkbox"/>	Home-net	6	-82	17:39:27	ASUSTe...	RS...	00:1f:c6:e5:57:e1	1/2/5,5/...	24	Infra...
<input checked="" type="checkbox"/>	RYBGOL	13	-82	17:39:27		RS...	50:46:5d:bd:15f0	1/2/5,5/...	11	Infra...
<input type="checkbox"/>	ASUS	13	-86	17:39:24		RS...	54:04:a6:5c:3e:e8	1/2/5,5/...	11	Infra...
<input checked="" type="checkbox"/>	Byt Wifi	1	-87	17:07:23		RS...	f4f2:6d:97:28:ea	1/2/5,5/...	11	Infra...

Obr. 24. Chanalyzer Lite – tabulka Wi-Fi sítí

### 6.1.5 Wi-Fi kanály

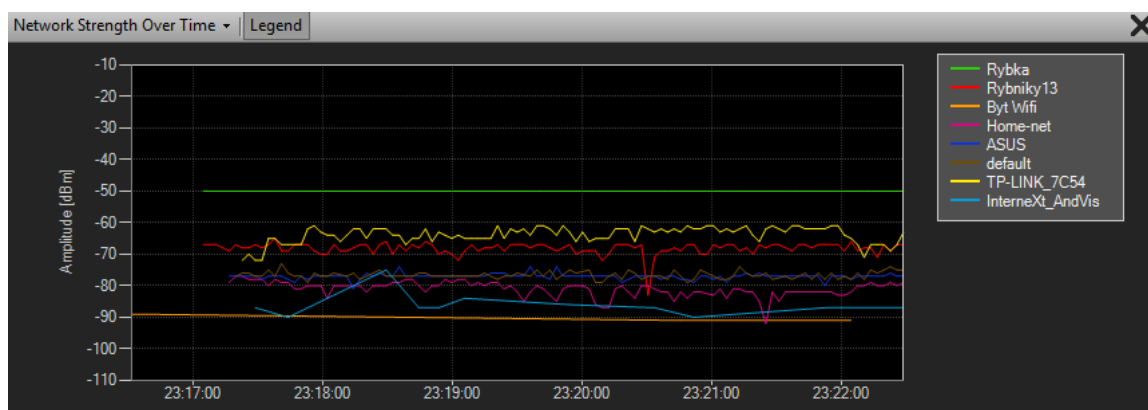
Pro práci s Wi-Fi kanály je v programu zabudovaná karta Wi-Fi Channels. Po kliknutí na kartu Window, se objeví tři možnosti (Wi-Fi Networks, Wi-Fi Channels a Markers), zde vybereme Wi-Fi Channels. Poté se nám objeví tabulka s kanály v rozsahu 1 až 14. Vybereme si přenosový kanál, který chceme monitorovat a následně jej označíme.

Graph	Channel	Average	Max	Current
<input checked="" type="checkbox"/>	1	-97	-38	-89
<input checked="" type="checkbox"/>	2	-97	-37	-84
<input checked="" type="checkbox"/>	3	-98	-36	-83
<input checked="" type="checkbox"/>	4	-97	-36	-81
<input checked="" type="checkbox"/>	5	-96	-35	-83

Obr. 25. Chanalyzer Lite – tabulka s Wi-Fi kanály

### 6.1.6 Síla sítě

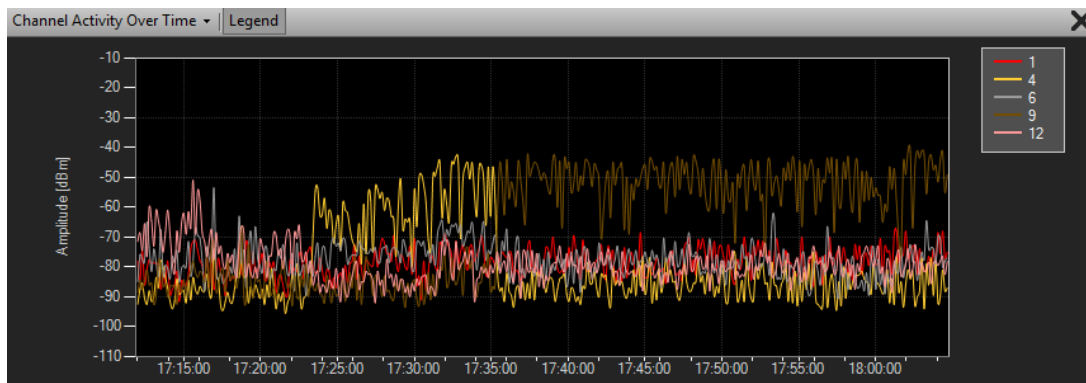
Další z možných zobrazení v programu je graf síly signálu každého routeru v čase. A prostřednictvím předchozí funkce Wi-Fi sítě je možné si zobrazit pouze sítě, které chceme monitorovat.



Obr. 26. Chanalyzer Lite – síla vybraných sítí v čase

### 6.1.7 Aktivita kanálu v čase

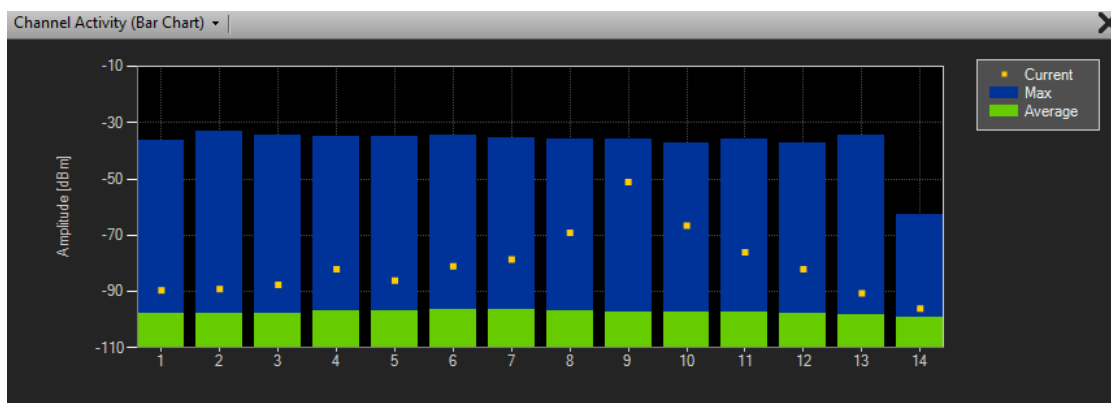
Filtr umožňuje náhled aktivity na kanálech v závislosti na čase, pro všech 14 Wi-Fi kanálů. Pomocí výše zmíněné funkce Wi-Fi Channels je možné si zobrazit pouze ty kanály, které chceme monitorovat. Pokud se v grafu zobrazují dlouhodobě nízké amplitudy, znamená to, že vybrané kanály jsou málo používané nebo volné.



Obr. 27. Chanalyzer Lite – aktivita kanálů v čase

### 6.1.8 Aktivita Wi-Fi sítí na kanálech

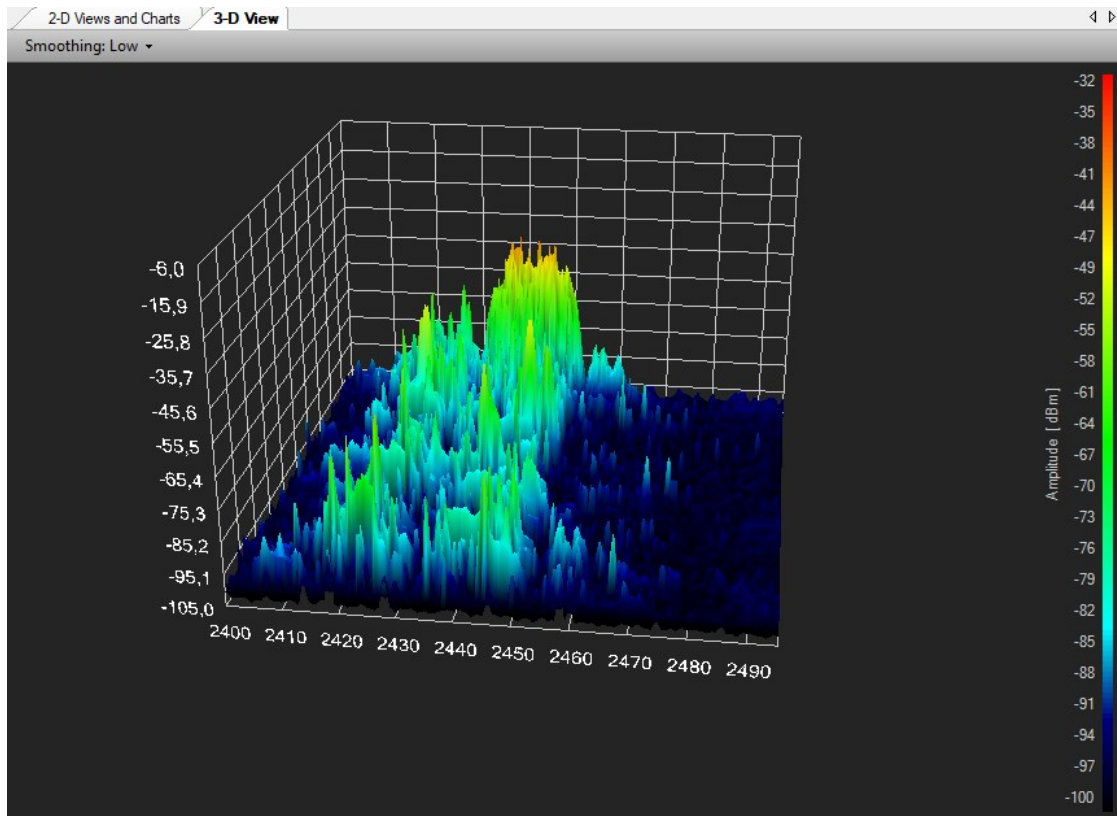
Tento druh filtru vyobrazuje aktuální, maximální a průměrnou aktivitu Wi-Fi sítí ve všech kanálech. Aktuální aktivitu na kanálu zastupují žluté čtverečky, ty se pohybují ve svislém směru. Maximální aktivitu vyobrazuje modrá barva a průměrnou aktivitu zelená barva. Čím větší amplituda v daném kanálu je, tím je větší aktivita. Pro běžného uživatele to znamená, že čím menší je průměrná a maximální hodnota, tím je síť vhodnější.



Obr. 28. Chanalyzer Lite – aktivita na Wi-Fi kanálech

### 6.1.9 3D zobrazení

Jedná se o trojrozměrné vykreslení amplitudy a frekvence v čase. Tato funkce umožňuje náhled na Wi-Fi aktivitu v pásmu. Ve srovnání běžných dvojrozměrných funkcí a trojrozměrného náhledu, tak 2D poskytuje bližší informace o frekvencích a 3D náhled všechny tyto informace dává do jednoho celku. Ve 3D náhledu je možné pohledem manipulovat, a to otočit kliknutím a tažením nebo pohled přiblížit a oddálit. K dispozici je filtr, který nebude zobrazovat šумы přístrojů, které často mění frekvenci.



Obr. 29. Chanalyzer Lite – 3D náhled aktivity Wi-Fi sítě

Výsledky z oblasti probíhajícího měření byly verifikovány prostřednictvím spektrálního analyzátoru Wi-Spy 2.4i a následně vyobrazeny v grafech. Vzhledem k velkému počtu Wi-Fi zařízení dochází k vzájemnému rušení, protože mnoho zařízení komunikuje na stejných kanálech. To zpříčiňuje pohyb amplitudy ve velkém rozsahu a tím zhoršuje kvalitu přijímacího signálu a vzniká neustálé rušení.

## 7 MONITOROVÁNÍ WI-FI SÍTÍ A ZPRACOVÁNÍ DAT

Vlastnit v dnešní době databázi, která obsahuje přibližnou polohu Wi-Fi zařízení, jejich MAC adresu a typ zabezpečení, může pro potenciálního hackera představovat cenný materiál. V dnešní době si málokterý provozovatel Wi-Fi uvědomuje důležitost bezpečnosti tohoto druhu informací.

Monitorování Wi-Fi sítí bude provedeno ve vybrané části centra města Vsetína. Právě centrum města je vhodné pro monitorování vzájemného rušení a překrývání Wi-Fi kanálů. Je to taky ideální místo pro monitorování metodou wardriving, kvůli překonávání větších vzdáleností při měření. Výstupem monitorování bude statistické vyhodnocení získaných dat o typu zabezpečení Wi-Fi sítí v lokalitě.

### 7.1 Použité prostředky

Pro monitorování byl použit osobní automobil, který sloužil pro snadnější přesun wadrivera (osoby, která monitoruje Wi-Fi sítě). Další prostředek, který byl použit pro monitorování, je laptop značky Dell, který má zabudovanou interní Wi-Fi kartu Intel® Centrino® Wireless-N 2230. Pro měření je nezbytné, aby laptop dokázal pracovat na baterii. Výdrž baterie se odvíjí od délky měření. Další důležitým prostředkem je software inSSIDer, který je pro monitoring volně dostupný.

Monitorování probíhalo ve všedních dnech v podvečerních až večerních hodinách kvůli menšímu provozu v lokalitě a většího množství připojení uživatelů do sítě.

### 7.2 Mapa měřených stanovišť

Jednotlivá stanoviště byla zvolena na základě jejich dostupnosti autem, tak aby nedocházelo k omezení provozu nebo dopravním přestupkům, a také podle množství okolních restauračních zařízení, hospod, obchodů apod. Právě v těchto lokalitách je velká pravděpodobnost, že bude docházet ke vzájemnému rušení a překrývání se na kanálech. Pro vytvoření mapového podkladu s umístěním všech měřících stanovišť byly použity mapy.cz od společnosti Seznam.cz.



Obr. 30. Mapa stanovišť

Měření na každém stanovišti je prováděno monitorováním prostřednictvím softwaru inSSIDer po dobu 10 vteřin. Doba měření je ošetřena tlačítky „Start“ a „Stop“, které jsou integrovány přímo v programu. Naměřené data jsou následně vložena do Excelu, který je přílohou bakalářské práce.

### 7.3 Naměřená data na stanovištích

V níže uvedených tabulkách jsou shrnuta naměřená data z každého stanoviště zvlášť. V tabulkách jsou uvedeny statistické údaje jako celkový počet detekovaných Wi-Fi sítí a jejich typ zabezpečení spolu s procentuálním vyjádřením.

Tab. 4. Naměřená data, stanoviště č. 1

Typ šifrování	Stanoviště č. 1	
	počet sítí	počet sítí v %
Žádné	1	2
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	4	9
RSNA-TKIP	0	0
RSNA-CCMP	39	89
<b>Celkem sítí</b>	<b>44</b>	

Tab. 5. Naměřená data, stanoviště č. 2

Typ šifrování	Stanoviště č. 2	
	počet sítí	počet sítí v %
Žádné	4	9
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	2	4
RSNA-TKIP	0	0
RSNA-CCMP	41	87
<b>Celkem sítí</b>	<b>47</b>	

Tab. 6. Naměřená data, stanoviště č. 3

Typ šifrování	Stanoviště č. 3	
	počet sítí	počet sítí v %
Žádné	0	0
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	1	6
RSNA-TKIP	0	0
RSNA-CCMP	16	94
<b>Celkem sítí</b>	<b>17</b>	

Tab. 7. Naměřená data, stanoviště č. 4

Typ šifrování	Stanoviště č. 4	
	počet sítí	počet sítí v %
Žádné	1	4
WEP	0	0
WPA-TKIP	1	4
WPA-CCMP	1	4
RSNA-TKIP	0	0
RSNA-CCMP	21	88
<b>Celkem sítí</b>	24	

Tab. 8. Naměřená data, stanoviště č. 5

Typ šifrování	Stanoviště č. 5	
	počet sítí	počet sítí v %
Žádné	3	12
WEP	3	12
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	19	76
<b>Celkem sítí</b>	25	

Tab. 9. Naměřená data, stanoviště č. 6

Typ šifrování	Stanoviště č. 6	
	počet sítí	počet sítí v %
Žádné	4	12
WEP	1	3
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	28	85
<b>Celkem sítí</b>	33	

Tab. 10. Naměřená data, stanoviště č. 7

Typ šifrování	Stanoviště č. 7	
	počet sítí	počet sítí v %
Žádné	1	7
WEP	0	0

WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	14	93
<b>Celkem sítí</b>	15	

Tab. 11. Naměřená data, stanoviště č. 8

Typ šifrování	Stanoviště č. 8	
	počet sítí	počet sítí v %
Žádné	10	29
WEP	3	9
WPA-TKIP	2	6
WPA-CCMP	1	3
RSNA-TKIP	0	0
RSNA-CCMP	18	53
<b>Celkem sítí</b>	34	

Tab. 12. Naměřená data, stanoviště č. 9

Typ šifrování	Stanoviště č. 9	
	počet sítí	počet sítí v %
Žádné	2	7
WEP	2	7
WPA-TKIP	2	7
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	23	79
<b>Celkem sítí</b>	29	

Tab. 13. Naměřená data, stanoviště č. 10

Typ šifrování	Stanoviště č. 10	
	počet sítí	počet sítí v %
Žádné	3	14
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	1	5
RSNA-CCMP	18	82
<b>Celkem sítí</b>	22	

Tab. 14. Naměřená data, stanoviště č. 11

Typ šifrování	Stanoviště č. 11	
	počet sítí	počet sítí v %
Žádné	4	11
WEP	1	3
WPA-TKIP	0	0
WPA-CCMP	1	3
RSNA-TKIP	1	3
RSNA-CCMP	30	81
<b>Celkem sítí</b>	<b>37</b>	

Tab. 15. Naměřená data, stanoviště č. 12

Typ šifrování	Stanoviště č. 12	
	počet sítí	počet sítí v %
Žádné	2	29
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	5	71
<b>Celkem sítí</b>	<b>7</b>	

Tab. 16. Naměřená data, stanoviště č. 13

Typ šifrování	Stanoviště č. 13	
	počet sítí	počet sítí v %
Žádné	0	0
WEP	0	0
WPA-TKIP	1	5
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	21	95
<b>Celkem sítí</b>	<b>22</b>	

Tab. 17. Naměřená data, stanoviště č. 14

Typ šifrování	Stanoviště č. 14	
	počet sítí	počet sítí v %
Žádné	1	5
WEP	0	0

WPA-TKIP	0	0
WPA-CCMP	1	5
RSNA-TKIP	0	0
RSNA-CCMP	18	90
<b>Celkem sítí</b>	<b>20</b>	

Tab. 18. Naměřená data, stanoviště č. 15

Typ šifrování	Stanoviště č. 15	
	počet sítí	počet sítí v %
Žádné	1	7
WEP	1	7
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	12	86
<b>Celkem sítí</b>	<b>14</b>	

Tab. 19. Naměřená data, stanoviště č. 16

Typ šifrování	Stanoviště č. 16	
	počet sítí	počet sítí v %
Žádné	1	6
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	16	94
<b>Celkem sítí</b>	<b>17</b>	

Tab. 20. Naměřená data, stanoviště č. 17

Typ šifrování	Stanoviště č. 17	
	počet sítí	počet sítí v %
Žádné	2	11
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	16	89
<b>Celkem sítí</b>	<b>18</b>	

Tab. 21. Naměřená data, stanoviště č. 18

Typ šifrování	Stanoviště č. 18	
	počet sítí	počet sítí v %
Žádné	3	43
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	4	57
<b>Celkem sítí</b>	<b>7</b>	

Tab. 22. Naměřená data, stanoviště č. 19

Typ šifrování	Stanoviště č. 19	
	počet sítí	počet sítí v %
Žádné	2	14
WEP	0	0
WPA-TKIP	0	0
WPA-CCMP	0	0
RSNA-TKIP	0	0
RSNA-CCMP	12	86
<b>Celkem sítí</b>	<b>14</b>	

Tab. 23. Naměřená data, stanoviště č. 20

Typ šifrování	Stanoviště č. 20	
	počet sítí	počet sítí v %
Žádné	7	30
WEP	0	0
WPA-TKIP	3	13
WPA-CCMP	0	0
RSNA-TKIP	1	4
RSNA-CCMP	12	52
<b>Celkem sítí</b>	<b>23</b>	

Tab. 24. Naměřená data, stanoviště č. 21

Typ šifrování	Stanoviště č. 21	
	počet sítí	počet sítí v %
Žádné	0	0
WEP	0	0

WPA-TKIP	0	0
WPA-CCMP	2	20
RSNA-TKIP	0	0
RSNA-CCMP	8	80
<b>Celkem sítí</b>	<b>10</b>	

Tab. 25. Naměřená data, stanoviště č. 22

Typ šifrování	Stanoviště č. 22	
	počet sítí	počet sítí v %
Žádné	6	29
WEP	1	5
WPA-TKIP	0	0
WPA-CCMP	2	10
RSNA-TKIP	0	0
RSNA-CCMP	12	57
<b>Celkem sítí</b>	<b>21</b>	

Protože, signál některých Wi-Fi zařízení byl naměřen nejenom na jednom stanovišti, ale zasahoval i do sousedních stanovišť, byla provedena úprava tak, aby to nezkruslovalo výstupní statistické údaje, a to odstraněním duplicitních hodnot.

#### 7.4 Vyhodnocení naměřených dat

Monitorování probíhalo celkem na 22 stanovištích. Veškerá naměřená data byla exportována do programu Excel a poté zpracována. Protože některé Wi-Fi sítě byly detekovány na vícero stanovištích, což by způsobovalo zkreslení výstupních hodnot, tak byla provedena úprava naměřených dat. Pomocí několika zabudovaných funkcí uvnitř Excelu byly odstraněny duplicitní MAC adresy. Tím bude zaručeno, že v seznamu nebude žádná Wi-Fi síť vícekrát.

Celkově detekovaných sítí bylo 1089, avšak jen 500 z nich je unikátních. Proto lze říci, že více jak polovina sítí jednoho ze stanovišť zasahovala svým signálem do dalšího stanoviště a tím se zkreslovalo měření.

V níže uvedené tabulce je statistický přehled o zabezpečení Wi-Fi sítí v centru města Vsetína. Wi-Fi sítě byly tříděny podle jejich typů zabezpečení na žádné, WEP, WPA-TKIP, WPA-CCMP, RSNA-TKIP a RSNA-CCMP.

Mezi typy zabezpečení, které jsou označovány za nedostatečnou ochranu, patří rozhodně WEP. Hlavními důvody je jeho zastaralost a nekomplexnost. Mnohdy se říká, že používání

šifrovacího protokolu WEP je skoro stejně riskantní jako nepoužití žádného hesla. Jediné pozitivum, co má oproti žádnému heslu a šifrování je, že zadávání hesla vyvolává pocit falešné bezpečnosti. Dále je možné na internetu dohledat postupy, jak odposlouchávat komunikaci a následně zjistit heslo pro připojení se do sítě. Z naměřených výsledků je patrné, že většina provozovatelů Wi-Fi si tuto problematiku uvědomuje a drží krok s dobou. Počet zařízení, který tento typ zabezpečení používá, je nepatrný a to pouze 12 Wi-Fi zařízení z celkových 500. To odpovídá pouhým 2 %.

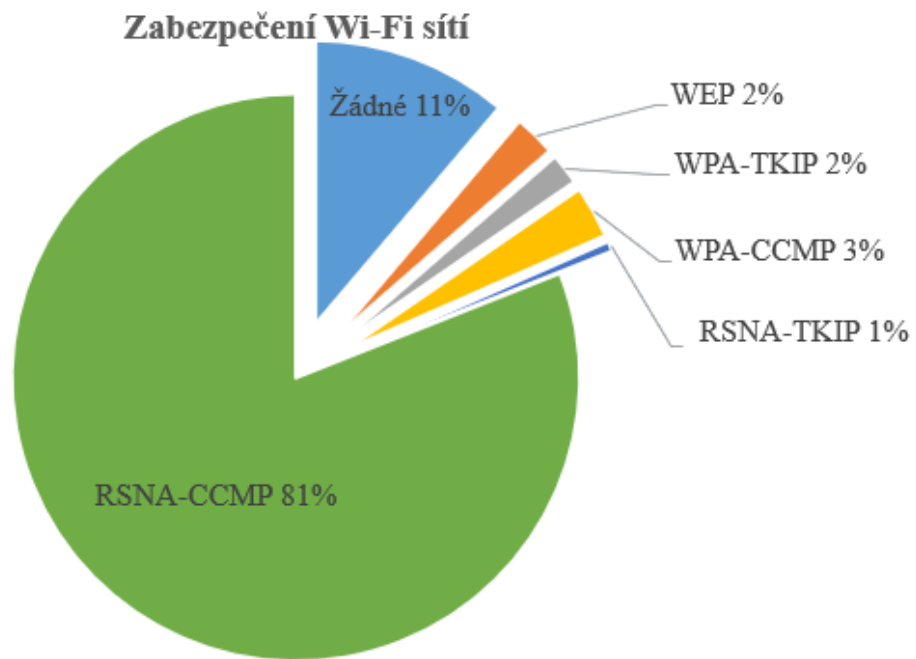
Zařízení, která používají WPA-TKIP a WPA-CCMP bylo detekováno 24, to odpovídá 5 % procentům z celkového počtu. CCMP představuje zkratku pro šifrování v AES režimu. Ač se nejedná o nejbezpečnější typ, jsou výsledky uspokojivé kvůli jejich nízkému počtu.

Nejbezpečnější a také nejpoužívanější, odvozeno z naměřených dat, šifrovací protokol je RSNA, opět ve dvojím provedení TKIP a CCMP. Celkový počet bezdrátových sítí, které používají RSNA-CCMP jako šifrovací protokol je 405, to odpovídá 81 %. A 1 % provozovatelů používá RSNA-TKIP.

Posledním typem zabezpečení je žádné. Pokud síť není zabezpečena jakýmkoliv typem šifrování, je tu riziko odposlechu dat. Existuje několik druhů softwaru, ve kterém si útočník může zobrazit veškerou vaši aktivitu a vyhledávat potřebné informace. Pokud je tedy na výběr, je vhodné se připojovat k autorizovaným Wi-Fi sítím. Počet detekovaných sítí, které neměli žádné šifrování je 56, to odpovídá 11 % z celkového počtu. Počet nezabezpečených, tudíž volně dostupných Wi-Fi sítí je poměrně velký. Bylo by vhodné, aby si provozovatelé uvědomili vznikající se rizika způsobena tímto lehkovážným jednáním a také zvažili důležitost ochrany informací.

Tab. 26. Shrnutí naměřených dat

Typ šifrování	Data ze všech stanovišť	
	počet sítí	počet sítí v %
Žádné	56	11
WEP	12	2
WPA-TKIP	9	2
WPA-CCMP	15	3
RSNA-TKIP	3	1
RSNA-CCMP	405	81
<b>Celkem sítí</b>	<b>500</b>	



Obr. 31. Vyhodnocení zabezpečení Wi-Fi sítí

## ZÁVĚR

V úvodu bakalářské práce bylo zmíněno, co vůbec jsou bezdrátové sítě, na jakém fyzikálním principu fungují a které komponenty jsou nezbytně nutné pro vytvoření plně funkční bezdrátové sítě. Bezdrátové sítě dále byly členěny na čtyři základní skupiny a to WPAN, WLAN, WMAN a WWAN. Skupiny se liší nejen ve svých velikostech, ale také i v počtu zařízeních, která jsou k síti připojena. Dále existují pouze dva způsoby, kterým mohou zařízení v síti komunikovat. Jedná se o topologie Ad-Hoc a Infrastruktura. V topologii Ad-Hoc zařízení komunikují přímo mezi sebou bez jakéhokoliv prostředníka. Ve druhém typu zařízení komunikují právě přes určitý přístupový bod.

Pro bezpečnost bezdrátových sítí jsou velice důležitými pojmy autentizace a šifrování. Autentizace nám zaručuje, že se do sítě nepřipojí osoba, která k tomu nemá oprávnění. Mezi nejjednodušší metodu patří autentizace otevřená, ta je rozšířená především mezi restauračními zařízeními a obchodními centry. Potom běžně používaná v domácnostech je autentizace se sdíleným/před sdíleným klíčem. A nakonec nejnovějším typem autentizací je standard IEEE 802.1x, ten nabízí pohodlnou správu vysokého počtu uživatelů. A v šifrování je možné se setkat se třemi typy šifrování a to symetrickým, asymetrickým a hybridním.

Právě autentizace a šifrování ztěžuje hackerům provést útok na Wi-Fi síť. Druhů útoků je celá řada, některé jsou už zastaralé a nepoužívají se a některé běžně používané. Cílem těchto útoků nemusí vždy být získání dat či neoprávněného přístupu do sítě, ale i zamezení jakékoliv komunikace.

V teoretické části bakalářské práce jsou dále popsány jednotlivé typy antén, které se používají pro bezdrátové připojení. Kvalitní pokrytí požadované lokality nespočívá jen v použití drahé a výkonné antény, ale je třeba nasměrovat vyzařovaný signál určitým směrem do dané lokality. Právě nesprávně zvoleným typem antény můžeme dát útočníkovi příležitost pro provedení útoku na síť. Je tedy nutné nasměrovat signál pouze do těch prostor, kde ji ve skutečnosti potřebujeme.

V praktické části byl proveden monitoring Wi-Fi sítí v centru města Vsetína metodou wardriving. Pro monitorování byl vybrán software inSSIDer, se kterým měl autor už zkušenosti. inSSIDer vyobrazuje dostatečné množství informací a výsledky měření bylo jednoduché exportovat do prostředí Excelu.

Měření probíhalo na 22 stanovištích, která se nacházela v centru města. Stanoviště byla umístěna poblíž státních institucí např. Pošty, Městského úřadu Vsetín nebo Masarykova Gymnázia, ale i restaurací a hospod.

Počet detekovaných sítí bylo rovných 500, z toho 405 provozovatelů měla svou Wi-Fi síť zabezpečenou dostatečně, to odpovídá 81 %. Druhou největší skupinou byly Wi-Fi sítě bez žádného zabezpečení a to s 56 zařízeními, to odpovídá 11 %. Počet zařízení, jež pro šifrování dat používá WPA-CCMP nebo WPA-TKIP je 24, to odpovídá 5 % z celkového počtu. Počet zařízení, která používají zastaralý šifrovací protokol WEP je 12, to odpovídá 2 % z celkového počtu.

Dále bylo vybráno stanoviště s největším počtem detekovaných Wi-Fi sítí a zde proběhlo podrobnější měření prostřednictvím spektrálního analyzátoru Wi-Spy 2.4i a následné vyobrazení. Vzhledem k velkému počtu bezdrátových sítí dochází k vzájemnému rušení. To způsobuje pohyb amplitudy ve velkém rozsahu a tím zhoršuje kvalitu přijímacího signálu a vzniká neustálé rušení.

Z průzkumu je patrné, že většina provozovatelů si uvědomuje možná rizika související s provozováním Wi-Fi sítí, avšak poměrně hojný počet Wi-Fi sítí nemá žádné zabezpečení nebo mají nedostatečné zabezpečení.

Používání bezdrátových sítí stále narůstá a nejvytíženějším frekvenčním pásmem je určitě 2,4 GHz. Vhodným nastavením přenosového kanálu a správným výběrem antény dosáhneme spolehlivějšího připojení a vyšší datové propustnosti.

Ačkoli je vše prolomitelné a je to jen otázkou času a výkonu, je pouze naším zájmem mít svou Wi-Fi zabezpečenou dostatečným způsobem tzn. používat bezpečné heslo, šifrování komunikace, skrytí názvu sítě nebo aspoň nepojmenovávat svou Wi-Fi podle svého jména.

**SEZNAM POUŽITÉ LITERATURY**

- [1] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 4. aktualizované a rozšířené vydání. Brno: Computer Press, a.s., 2008. ISBN 978-80-251-2073-6.
- [2] ZANDL, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Brno: Computer Press, 2003. ISBN 80-7226-632-2.
- [3] BARKEN, Lee. *Wi-Fi: jak zabezpečit bezdrátovou síť*. Brno: Computer Press, 2004. ISBN 80-251-0346-3.
- [4] MALOTOVÁ, Andrea. *Praktické využití programů pro analýzu a aktivitu kanálu WiFi sítí*. Zlín, 2012. Diplomová práce. Univerzita Tomáše Bati.
- [5] Základy IT gramotnosti.: *Lokální sítě (LAN)* [online]. Fakulta informatiky Masarykovy univerzity [cit. 2018-02-06]. Dostupné z: <https://is.muni.cz/do/1492/el/sitmu/law/html/lokalni-site-lan.html>
- [6] ROSS, Andy. B+B SMARTWORX.: *MAKE YOUR TABLETS AND SMART PHONES SMARTER - ADD SERIAL* [online]. [cit. 2018-02-14]. Dostupné z: <http://www.bb-elec.com/Learning-Center/All-White-Papers/Serial/•-Make-Your-Tablets-and-Smart-Phones-Smarter-Add-S.aspx>
- [7] Bezdrátové sítě [online]. [cit. 2018-02-16]. Dostupné z: [http://bezdratove-site.wz.cz/#\\_Toc170470616](http://bezdratove-site.wz.cz/#_Toc170470616)
- [8] PC tuning.: *Moderní metody šifrování* [online]. Redakce PCT, 2005 [cit. 2018-02-16]. Dostupné z: [https://pctuning.tyden.cz/software/ochrana-soukromi/4711-moderni\\_metody\\_sifrovani](https://pctuning.tyden.cz/software/ochrana-soukromi/4711-moderni_metody_sifrovani)
- [9] Slide share.: *Networking Basics* [online]. 2011 [cit. 2018-02-20]. Dostupné z: <https://www.slideshare.net/smceu/networking-basics-9423264>

- [10] KYSELA, Jiří. Internet pro všechny.: *Bezdrátový Internet a technologie Wi-Fi v České republice - internet pro všechny* [online]. 2010 [cit. 2018-02-06]. Dostupné z: <http://www.internetprovsechny.cz/bezdratovy-internet-a-technologie-wi-fi-v-ceske-republice/>
- [11] KUCHARŤ, Martin. *Svět Hardware: Jak zapojíme síť: WiFi bez tajemství - Jak funguje přenos dat | Svět hardware* [online]. 2009, 07.10. [cit. 2018-04-11]. Dostupné z: <https://www.svethardware.cz/jak-zapojime-sit-wifi-bez-tajemstvi/12953-2>
- [12] SEIDL, David. *Praktické zkušenosti s provozem WiFi Acess Pointu pod OS GNU/Linux* [online]. VŠB-TU Ostrava, 2005 [cit. 2018-04-05]. Dostupné z: [http://ols.vsb.cz/2005-12-15/wifi/wifi\\_na\\_linuxu.pdf](http://ols.vsb.cz/2005-12-15/wifi/wifi_na_linuxu.pdf)
- [13] *StartHub: Personal Mobile Phones, Broadband, TV, Voice and Rewards | StartHub* [online]. 2016 [cit. 2018-04-11]. Dostupné z: <https://community.starhub.com/t5/Fibre-BroadBand/Starhub-Fibre-Broadband/td-p/131370>

**SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK**

Wi-Fi	Wireless Fidelity
ČTU	Český telekomunikační úřad
AP	Access Point
IEEE	The Institute of Electrical and Electronic Engineers
WPAN	Wireless Personal Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WWAN	Wireless Wide Area Network
IrDA	Infrared Data Association
Wi-Fi	Wireless Fidelity
IP	Internet Protocol
NAT	Network Address Translation
WiMAX	Worldwide Interoperability for Microwave Access
NLOS	Non Line Of Sight
LOS	Line Of Sight
GSM	Global System for Mobile Communications
UMTS	Universal Mobile Telecommunications System
IBSS	Independent Basic Service Set
WEP	Wired Equivalent Privacy
PSK	Pre-Shared Key
AAA	Authentication Authorization and Accounting
AES	Advanced Encryption System
RSA	Rivest, Shamir, Adleman
VPN	Virtual Private Network

MAC	Media Access Control
DoS	Denial of Service
DDoS	Distributed Denial of Service
PDA	Personal Digital Assistant
USB	Universal Serial Bus
GHz/MHz	Gigahertz, Megahertz, jednotka frekvence
Mbps	Megabit za sekundu, jednotka přenosové rychlosti
dBi	Decibel na isotop, jednotka ziskovosti
dBm	Decibel nad miliwattem, jednotka RSSI

## SEZNAM OBRÁZKŮ

<i>Obr. 1. Komponenty bezdrátové sítě [2], upravil Tomek 2018</i> .....	11
<i>Obr. 2. Členění bezdrátových sítí [9], upravil Tomek 2018</i> .....	11
<i>Obr. 3. Fresnelova zóna a její režimy viditelnosti [4]</i> .....	14
<i>Obr. 4. Členění buněk v síti [10]</i> .....	15
<i>Obr. 5. Ad-Hoc struktura [2], upravil Tomek 2018</i> .....	16
<i>Obr. 6. Infrastruktura [6], upravil Tomek 2018</i> .....	16
<i>Obr. 7. Symetrické šifrování [8]</i> .....	19
<i>Obr. 8. Asymetrické šifrování [8]</i> .....	20
<i>Obr. 9. Hybridní šifrování [8]</i> .....	21
<i>Obr. 10. Denial of Service útok</i> .....	24
<i>Obr. 11. Distributed Denial of Service útok</i> .....	25
<i>Obr. 12. Vyzařující diagram všesměrové antény a) v horizontálním směru b) ve vertikálním směru [12], upravil Tomek 2018</i> .....	28
<i>Obr. 13. Vyzařující diagram sektorové antény [12], upravil Tomek 2018</i> .....	29
<i>Obr. 14. Vyzařující diagram směrové antény [12], upravil Tomek 2018</i> .....	29
<i>Obr. 15. inSSIDer – zobrazené Wi-Fi sítě a jejich parametry</i> .....	33
<i>Obr. 16. inSSIDer – síla signálů sítí v čase</i> .....	34
<i>Obr. 17. inSSIDer – síla signálu a používané kanály</i> .....	34
<i>Obr. 18. Spektrální analyzátor Wi-Spy 2.4i</i> .....	35
<i>Obr. 19. Chanalyzer Lite – Planar zobrazení</i> .....	37
<i>Obr. 20. Chanalyzer Lite – Markers</i> .....	37
<i>Obr. 21. Chanalyzer Lite – Density zobrazení</i> .....	38
<i>Obr. 22. Chanalyzer Lite – Waterfall zobrazení</i> .....	38
<i>Obr. 23. Chanalyzer Lite – Window karta</i> .....	39
<i>Obr. 24. Chanalyzer Lite – tabulka Wi-Fi sítí</i> .....	39
<i>Obr. 25. Chanalyzer Lite – tabulka s Wi-Fi kanály</i> .....	39
<i>Obr. 26. Chanalyzer Lite – síla vybraných sítí v čase</i> .....	40
<i>Obr. 27. Chanalyzer Lite – aktivita kanálů v čase</i> .....	40
<i>Obr. 28. Chanalyzer Lite – aktivita na Wi-Fi kanálech</i> .....	41
<i>Obr. 29. Chanalyzer Lite – 3D náhled aktivity Wi-Fi sítí</i> .....	42
<i>Obr. 30. Mapa stanovišť</i> .....	44
<i>Obr. 31. Vyhodnocení zabezpečení Wi-Fi sítí</i> .....	53

**SEZNAM TABULEK**

Tab. 1. Vlastnosti standardů společnosti IEEE 802.11 [13], upravil Tomek 2018 ....	13
Tab. 2. Využívané kanály v Evropě.....	30
Tab. 3. Specifikace Wi-Spy 2.4i .....	36
Tab. 4. Naměřená data, stanoviště č. 1 .....	45
Tab. 5. Naměřená data, stanoviště č. 2 .....	45
Tab. 6. Naměřená data, stanoviště č. 3 .....	45
Tab. 7. Naměřená data, stanoviště č. 4 .....	46
Tab. 8. Naměřená data, stanoviště č. 5 .....	46
Tab. 9. Naměřená data, stanoviště č. 6 .....	46
Tab. 10. Naměřená data, stanoviště č. 7 .....	46
Tab. 11. Naměřená data, stanoviště č. 8 .....	47
Tab. 12. Naměřená data, stanoviště č. 9 .....	47
Tab. 13. Naměřená data, stanoviště č. 10 .....	47
Tab. 14. Naměřená data, stanoviště č. 11 .....	48
Tab. 15. Naměřená data, stanoviště č. 12 .....	48
Tab. 16. Naměřená data, stanoviště č. 13 .....	48
Tab. 17. Naměřená data, stanoviště č. 14 .....	48
Tab. 18. Naměřená data, stanoviště č. 15 .....	49
Tab. 19. Naměřená data, stanoviště č. 16 .....	49
Tab. 20. Naměřená data, stanoviště č. 17 .....	49
Tab. 21. Naměřená data, stanoviště č. 18 .....	50
Tab. 22. Naměřená data, stanoviště č. 19 .....	50
Tab. 23. Naměřená data, stanoviště č. 20 .....	50
Tab. 24. Naměřená data, stanoviště č. 21 .....	50
Tab. 25. Naměřená data, stanoviště č. 22 .....	51
Tab. 26. Shrnutí naměřených dat .....	52

## SEZNAM PŘÍLOH

**P I:** Naměřená data wardrivingem