

Využití metod umělé inteligence při návrhu realizace bezdrátové sítě v budově

Usage of Artificial Intelligence Methods For The Design of Wireless Networks In The Building

Bc. Zdeněk Loveček

Diplomová práce
2014



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Zdeněk LOVEČEK**
Osobní číslo: **A10873**
Studijní program: **N3902 Inženýrská informatika**
Studijní obor: **Informační technologie**
Forma studia: **kombinovaná**

Téma práce: **Využití metod umělé inteligence při návrhu realizace bezdrátové sítě v budově**

Zásady pro vypracování:

1. Nastudujte možnosti návrhování a rozmísťování prvků bezdrátové sítě v budově.
2. Nastudujte možnosti metod umělé inteligence s ohledem na návrh bezdrátové sítě.
3. Zvolte různé scénáře struktury budovy a otestujte zvolené metody.
4. Provedte analýzu klasických typů návrhů s metodami návrhů pomocí umělé inteligence.

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. ŠNOREK M., JIŘINA M.: **Neuronové sítě a neuropočítače**, ČVUT, 1996, ISBN 80-01-01455-X.
2. BÍLA J.: **Umělá inteligence a neuronové sítě v aplikacích**, ČVUT, 1996, ISBN 80-01-01275-1.
3. ZELINKA I.: **Umělá inteligence I**, VUT Brno, 1998, ISBN 80-214-1163-5.
4. ZELINKA, I., OPLATKOVÁ, Z., OŠMERA, P., ŠEDA, M., VČELAŘ, F. **Evoluční výpočetní techniky – principy a aplikace**. BEN – technická literatura, Praha, 2008, ISBN 80-7300-218-3.
5. DAVIS, Harold. **Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!**. 1. vyd. Praha: Grada, 2006, 334 s. Průvodce (Grada). ISBN 80-247-1421-3.
6. PECHAČ, Pavel. **Šíření vln v zástavbě**. Praha: BEN – technická literatura, 2005, 108 s. ISBN 80-730-0186-1.
7. HORÁK, Jaroslav. **Vytváříme domácí bezdrátovou síť**. Vyd. 1. Brno: Computer Press, 2011, 293 s. ISBN 978-802-5129-777.
8. SOSINSKY, Barrie. **Mistrovství počítačové sítě**. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-802-5133-637.

Vedoucí diplomové práce:

doc. Ing. Zuzana Komínková Oplatková, Ph.D.

Ústav informatiky a umělé inteligence

Datum zadání diplomové práce:

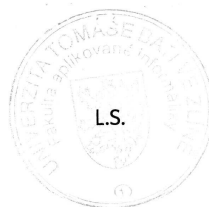
21. února 2014

Termín odevzdání diplomové práce:

20. května 2014

Ve Zlíně dne 21. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan



doc. Mgr. Roman Jašek, Ph.D.
ředitel ústavu

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/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....
podpis diplomanta

ABSTRAKT

Diplomová práce je zaměřena na problematiku umělé inteligence – algoritmu SOMA. Cílem práce je porovnat optimální rozmístění Acces pointů v budově při použití simulačního software a použitím algoritmu SOMA a Diferenciální evoluce.

V teoretické části práce je popsána problematika bezdrátových sítí, jejich struktura a funkcionality a úvod do problematiky neuronových sítí, evolučního algoritmu SOMA a DE.

Praktická část popisuje návrh bezdrátové sítě v budově a simulační software pro šíření signálu.

Klíčová slova: Standard 802.11, Evoluční algoritmus SOMA, Diferenciální evoluce.

ABSTRACT

Diploma thesis is focused on artificial intelligence – algorithm SOMA. The aim of this document is compare the optimal deployment of WiFi routers in the building using software simulation, using the algorithm SOMA and DE.

The theoretical part is describes the issue of wireless networks, its structure and functionality and introduction to neurons networks and evolutionary algorithm SOMA.

The practical part describes the design of a wireless network in building, simulation software for signal propagation.

Keywords: Standard 802.11, Evolutionary algorithm SOMA, Differential evolution.

Děkuji vedoucí mé diplomové práce Doc. Zuzaně Komínkové Oplatkové, Ph.D., za vstřícnost, věnovaný čas, rady a připomínky, kterými mne vedla k cíli.

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

OBSAH

<i>Úvod</i>	9
1. Historie bezdrátové sítě	11
2. Vývoj standardu 802.11	12
3. Základy sítí 802.11	16
3.1. Komponenty sítě	16
3.1.1 Distribuční systém	16
3.1.2 Přístupový bod (Access Point, AP).....	16
3.1.3 Bezdrátové médium	16
3.1.4 Stanice.....	17
3.2. Typy sítí	17
3.2.1 Ad hoc sítě	17
3.2.2 Infrastrukturní sítě.....	18
3.3. OSI model	20
3.3.1 Jednotlivé vrstvy ISO/OSI modelu	21
3.4. Linková vrstva a MAC podvrstva	22
3.4.1 Formát MAC rámce	23
3.4.2 Složení MAC rámce.....	23
3.5. Fyzická vrstva	24
3.6. Zabezpečení bezdrátové sítě	25
3.6.1 Změna hesla přístupu k routeru	26
3.6.2 Blokace vysílání SSID	26
3.6.3 Omezení síly vysílaného Wi-Fi signálu.....	26
3.6.4 Manuální nastavení IP adresy	26
3.6.5 Kontrola MAC adres.....	26
3.6.6 WEP	27
3.6.7 WPA.....	27
3.6.8 WPA2.....	28
4. Evoluční algoritmy	29
4.1. SOMA	29

4.1.1	Parametry algoritmu SOMA.....	29
4.1.2	Jednotlivé kroky algoritmu SOMA.....	30
4.2.1	Parametry Diferenciální evoluce	32
4.2.2	Jednotlivé kroky Diferenciální evoluce	34
5.	Popis prostředí.....	37
5.1.	Problémy se šířením signálu uvnitř budov	38
5.1.1	Vícecestné šíření signálu- odstranění problému	38
5.1.2	Ztráty průchodem přes překážky	39
5.1.3	Rušení jinými systémy.....	39
5.2.	Simulační software pro šíření signálu v budovách	39
5.2.1	Program I-Prop 1.39	39
5.2.2	Program Ekahau Site Survey 2.1	40
5.2.3	Porovnání programů I-Prop a Ekahau Site Survey	41
5.2.4	Ekahau HeatMapper	42
5.3.	Měření a simulace	43
5.3.1	Nastavení simulace v I-Prop.....	45
5.3.2	Rozmístění přístupových bodů a simulace	46
5.4.	Optimalizace rozmístění směrovacích stanic v bezdrátových sítích	48
5.4.1	Účelová funkce	48
5.4.2	Testovací část.....	49
6.	Závěr.....	56
7.	Seznam použité literatury	57
8.	Seznam použitých symbolů a zkratk	58
9.	Seznam obrázků	59
10.	Seznam tabulek	61
11.	Seznam příloh.....	63

ÚVOD

Bezdrátová síť je typ počítačové sítě, ve které je spojení mezi účastníky sítě uskutečňováno pomocí bezdrátové komunikace, nejčastěji pomocí elektromagnetických vln. Její hlavní výhodou je její nízká cena, která je mimo jiné způsobena tím, že jsou certifikovaná zařízení k dispozici ve velkých sériích. Pro návrh takové sítě v administrativní budově se využívá simulačních programů tak, aby se předcházelo místům se špatným signálem. Většina dostupných aplikací je schopna zjistit sílu signálu v daném místě. Existuje už jen pár takových, které jsou schopny provést simulaci pro více přístupových bodů v administrativní budově a méně je ještě těch, které samy dokáží v daném prostředí navrhnout rozmístění Access Pointů tak, aby byla pokryta všechna místa v budově.

Cílem mé diplomové práce je vytvořit model rozmístění Access Pointů v budově za použití umělé inteligence - algoritmu SOMA a Diferenciální evoluce tak, aby všechna místa v budově byla pokryta dostatečnou silou signálu. Ve své práci porovnám v simulačním programu I-Prop současný stav rozmístění AP s návrhem, který se vygeneruje pomocí evolučního algoritmu SOMA.

Teoretická část práce je zaměřena na obecnou problematiku bezdrátových sítí, vývoj Standardu 802.11, komponenty sítí, OSI model, Linkovou vrstvu a MAC podvrstvu a bezpečnost. Protože problematika bezdrátových sítí je rozsáhlá a není úplně předmětem této diplomové práce, je jí věnována je okrajová část. Dále jsou v této části popsány evoluční algoritmy SOMA a Diferenciální evoluce.

Praktická část se zabývá prostředím a současným stavem rozmístění AP. Dále je zde popsáno, jakým způsobem byly algoritmy testovány a vyhodnoceny. Všechny výsledky byly zpracovány do přehledných obrázků a tabulek.

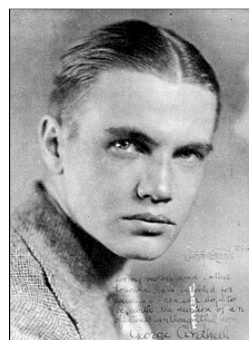
I. TEORETICKÁ ČÁST

1. HISTORIE BEZDRÁTOVÉ SÍTĚ

Počátky bezdrátového přenosu se datují do čtyřicátých let minulého století, přesněji řečeno princip přenosu dat pomocí rozprostřeného spektra, který dnešní bezdrátové sítě používají. Německá armáda experimentovala s torpédem, které mělo být řízeno na dálku za pomoci rádiového vysílání. Provedené pokusy ale ukázaly zásadní nedostatek - radiové signály bylo totiž možno jednoduše odposlouchávat. Divadelní herečka rakouského původu Hedy Lamarr (obr. 1) navrhla, že by radiové signály mohly být distribuovány náhodně v čase napříč sériemi frekvencí. Přenos na každé frekvenci by pak mohl být krátký a celkově celý datový tok by byl mnohem méně náchylný k rušení či odposlouchávání. Další problém představovala synchronizace mezi vysílajícím a přijímacím zařízením. Hudební skladatel George Antheil (vlastním jménem Georg Carl Johann Antheil) (obr. 2) tento problém vyřešil tak, že navrhl synchronizační mechanismus používající děrovou perforovanou roli papíru, podobnou té, která se používala u jeho mechanických hudebních pián řízených širokým děrovaným pruhem papíru. V roce 1942 Hedy Lamarr a George Antheil si tento vynález nechali patentovat. Vynález se do konce války nedočkal využití, protože válečné námořnictvo označilo vynález za neproveditelný a papírový pás pro mechanické piano (patent uvažoval o 88 kanálech, právě tolik má piano kláves) za těžkopádný. [9]



Obr. 1 - Hedy Lamarr



Obr. 2 - George Antheil

V šedesátých letech minulého století se vynález po inovaci (papírový pás byl nahrazen elektronikou) poprvé uplatnil v roce 1962 pod názvem *rozprostřené spektrum* a to během kubánské krize. Později ve Vietnamské válce byla nasazena bezpilotní pozorovací letadla komunikující se základnou právě touto metodou a počátkem 80. let 20. století byla technologie rozprostřeného spektra uvolněna pro civilní využití.

O důležitosti objevu svědčí i to, že Hedy Lamarr byla v roce 1997 udělena v kalifornské Pasadě výroční cena vynálezců, a to v jejích 84 letech. George Antheil se ocenění bohužel nedočkal, protože náhle zemřel v Manhattanu 12. února 1959 na srdeční infarkt.

2. VÝVOJ STANDARDU 802.11

Dnes jsou v civilním sektoru využívány dva způsoby modulace do rozprostřeného spektra. Starší metoda patentovaná Lamarr a Antheilem je označována jako **FHSS** (*frequency hopping spread spectrum = přeskakující frekvence v rozprostřeném spektru*), novější a technicky náročnější metoda je označována jako **DSSS** (*direct sequence spread spectrum = přímá sekvence v rozprostřeném spektru*). FHSS byla implementována mimo jiné v zařízeních **BreezeNET** pro pásma 2.4GHz a 3.5GHz, modulace DSSS nabízející vyšší přenosovou kapacitu dala základ technologii **WaveLAN** americké společnosti NCR. [7]

Původní zařízení WaveLAN pracovala v pásmu 902-928MHz, později se WaveLAN přesunul do pásma 2.4GHz a stal se tak základem normy IEEE 802.11b a standardem Wi-Fi. U nás se BreezeNET i WaveLAN staly populárním způsobem připojování zákazníků k Internetu. Zatímco BreezeNET se dokázal díky FHSS vyhnout jinému BreezeNETu změnou pořadí přepínaných kanálů a WaveLAN bylo možno při rušení jiným WaveLANem přepnout na jiný kanál, signál BreezeNETu neustále přeskakoval do širokého kanálu používaného WaveLANem, modulace FHSS a DSSS totiž spolu navzájem kolidovaly a antény převaděčů od sebe musely být vzdáleny alespoň několik metrů.

Ke každé bezdrátové síti musí mít provozovatel patřičnou licenci pro vysílání v určité frekvenci. Této frekvenci se říká licencované pásmo. Frekvencí není nekonečné množství, proto tato pásma jsou zpoplatněna vysokou částkou. Majitelé licencí si samozřejmě svá pásma chrání, aby v nich nikdo jiný nevysílal. Protože rádiové vysílání mají i některé přístroje v domácnosti (např. mikrovlnná trouba, mobilní telefon), vzniklo takzvané bezlicenční pásmo **ISM** (2,4GHz), neboli pásmo vyhrazené pro průmyslové, vědecké a lékařské potřeby (Industrial Scientific and Medical). [11]

Samotné bezdrátové sítě tak, jak je známe dnes, spatřily světlo světa v roce 1997, kdy byl organizací **IEEE** (*Institute of Electrical and Electronics Engineers*, je mezinárodní nezisková organizace, jejíž hlavní zaměření spočívá ve vývoji průmyslových standardů) vydán první standard bezdrátových sítí pracujících v pásmu ISM pod označením **802.11**. Tato bezdrátová síť nabízela rychlost až 2Mb/s. O dva roky později (1999) tuto specifikaci rozšířila IEEE o dvě kvalitnější specifikace známé pod označením **802.11b** – tedy o definici bezdrátové sítě pracující v pásmu **2,4GHz** rychlostí až **11Mb/s** s použitou modulací DSSS a **802.11a**, bezdrátovou síť pracující v novém pásmu **5GHz** o rychlosti až **54Mb/s**. Frekvenci 2,4GHz totiž začalo mezitím využívat až příliš mnoho zařízení, jejichž

výčet obsahuje jak mikrovlnné trouby, tak i mobilní telefony používající technologii Bluetooth. Standard využívá modulace **OFDM** (*Orthogonal Frequency Division Multiplexing* - Orthogonální frekvenční multiplex). O čtyři roky později (2003) byl vyvinut standard nový, označovaný jako **802.11g**, který využívá opět modulaci **OFDM**, avšak rovněž i **DSSS**, a to právě z důvodu zpětné kompatibility se starším **802.11b**. Standard pracuje ve stejném frekvenčním pásmu jako norma "b" a využívá rychlostí do **54Mb/s** včetně těch, které byly převzaty z původního 802.11b a dokonce i prapůvodního 802.11). Dnes je využíván ještě jeden standard **802.11n** (2009). Norma též zlepšuje odolnost proti rušení, a to za použití technologie chytrých antén **MIMO** (*Multiple Input Multiple Output*). Ta však až tak nová není, přišly s ní již před více než 40 lety Bellovy laboratoře, avšak používána masově nikdy nebyla. **MIMO** má však velikou výhodu. Pracuje totiž na té nejnižší síťové vrstvě (fyzické) podle **ISO/OSI** modelu a lze ji tak využít bez ohledu na protokoly vyšších vrstev. Maximální propustnost i rychlost se zvyšuje jednoduše tím, že se navýší počet připojených antén. Přesný počet antén stanoven nikde není. Použití antén je pouze omezeno na maximální počet **16** pro venkovní provoz a až **4** pro provoz v bytové zástavbě. [8]

RYCHLOST	POČET ANTÉN
až 600 Mb/s	4X4 MIMO
až 450Mb/s	3X3 MIMO
až 300Mb/s	2X2 MIMO

Tabulka 1: Přenosová rychlost 802.11n v závislosti na počtu antén

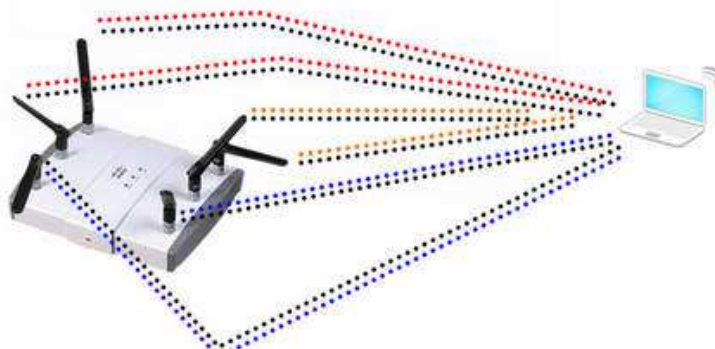
V letošním roce 2014 se čeká oficiálního schválení standardu **802.11ac**, nazývaného též Wi-Fi páté generace (5G Wi-Fi) nebo gigabitová Wi-Fi síť. Už teď přichází první zařízení s plnou podporou specifikace, tzn. fáze „draft“, která by se měla od finální verze lišit jen minimálně, prakticky zanedbatelně. Jakékoliv změny, které mezitím nastanou, se budou řešit aktualizací firmwaru. Stejně jako u standardu **802.11n** bude rychlost zařízení odvozena od počtu antén, u jedné antény na obou stranách začne rychlost na **433Mb/s** (šířka kanálu 80MHz) a může být až **3,47Gb/s** při osmi anténách. Standard 802.11ac komunikuje výhradně v pásmu 5GHz, nebude žádná 2,4GHz verze. Je však zaručena zpětná kompatibilita, takže čip bude schopný pracovat i na 2,4GHz, ale pouze na starších standardech a s upřednostněním 5GHz pásma, pokud to bude druhá strana umět. Na rozdíl od 5GHz pásma u 802.11n, který používal šířku kanálu 20/40MHz (nejběžnější je

20MHz), používá 802.11ac šířku od 20 až do 160MHz, nejběžnější by měl být kanál 80MHz. [11]

Komunikace je oddělena na streamy, kterých bude podporováno až osm, s tím, že v počáteční fázi se bude pro jedno zařízení využívat nejvýše tři. Každý stream nabídne maximální datovou propustnost 433Mb/s, tři streamy zvládnou přenést až 1,3Gb/s. Mobilní zařízení, jako je chytrý telefon nebo tablet, dokáže pracovat jen s jedním streamem, u notebooků, televizorů nebo lepších USB adaptérů bychom se mohli setkat s podporou tří streamů.

S více uživateli zároveň připojenými k Wi-Fi byl často problém. Základna mohla v určitou dobu komunikovat jen s jedním zařízením bez ohledu na počet použitelných streamů, takže při komunikaci více zařízení se musela střídat. Nový standard již povinně podporuje **MU-MIMO** (*Multi User - Multiple Input Multiple Output*), který umožňuje vícestreamové základně komunikovat s několika zařízeními současně v jednom momentě, každé zařízení bude na vlastním streamu (či více streamech). Bude-li mít základna tři streamy, notebook v dosahu také tři a mobil jeden, bude jeden stream využívat pro mobilní telefon a zbylé dva pro notebook. Pokud by byly k základně připojeny tři jednostreamové smartphony, obslouží třístreamová základna všechny tři, aniž by jeden ovlivňoval rychlost druhého.

U 802.11ac je nedílnou součástí technologie **Beamforming** (obr. 3), která funguje tak, že je fáze signálu některé z vysílacích antén přizpůsobena prostředí, výsledný signál je proto v cíli mnohem silnější, jelikož je dán součtem všech příchozích signálů. [12]



Obr. 3 - Beamforming

Jako první se zařízeními připravenými na nový standard přišla společnost Netgear. Prvním modelem je router R6300 (obr. 4) pracující s šířkou pásma 80MHz (propustnost je tedy

maximálně 433MHz na jeden stream) se třemi 802.11ac streamy (až 1,3Gb/s) a nejrychlejším standardem 802.11n (2x400Mb/s).



Obr. 4 – Netgear R6300

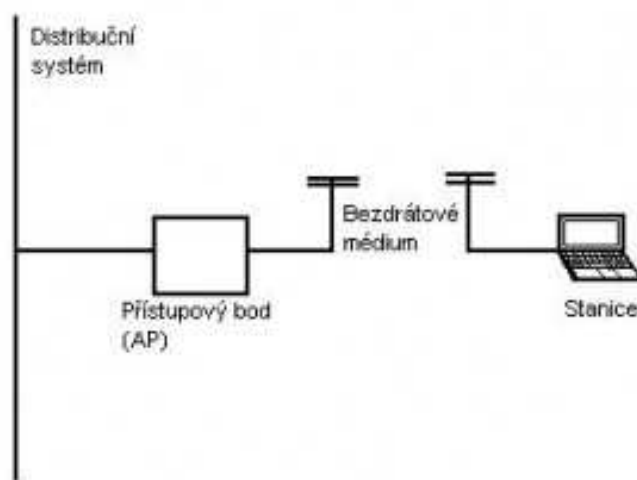
Existuje ještě rychlejší bezdrátový standard – **IEEE 802.11ad**, který už ale není Wi-Fi, ale síť, které se říká **WiGig**. Je určena pouze pro krátké vzdálenosti (v rámci místnosti, zhruba do 10m), pracuje na šířce pásma 60GHz a dosahuje maximální rychlosti 7Gb/s.

3. ZÁKLADY SÍTÍ 802.11

3.1. Komponenty sítě

Každá 802.11 síť (obr. 5) obsahuje čtyři hlavní druhy fyzických komponent. [9] Jsou to:

- Distribuční systém.
- Přístupový bod (Access Point).
- Bezdrátové médium.
- Stanice.



Obr. 5 – Komponenty sítě 802.11

3.1.1 Distribuční systém

Distribuční systém je logická komponenta, která směřuje data na určitou stanici. Většinou je systém řešen jako síťový most (bridge) s distribučním médiem, kterým jsou informace přenášeny. Médium je většinou ethernetový kabel.

3.1.2 Přístupový bod (Access Point, AP)

Je to nejdůležitější část Wi-Fi sítě. Právě AP přemostuje spojení mezi kabelovou a bezdrátovou sítí. Access point také nabízí mnoho jiných funkcí, jako routování, směrování portů, ale hlavně také právě zabezpečení bezdrátové sítě.

3.1.3 Bezdrátové médium

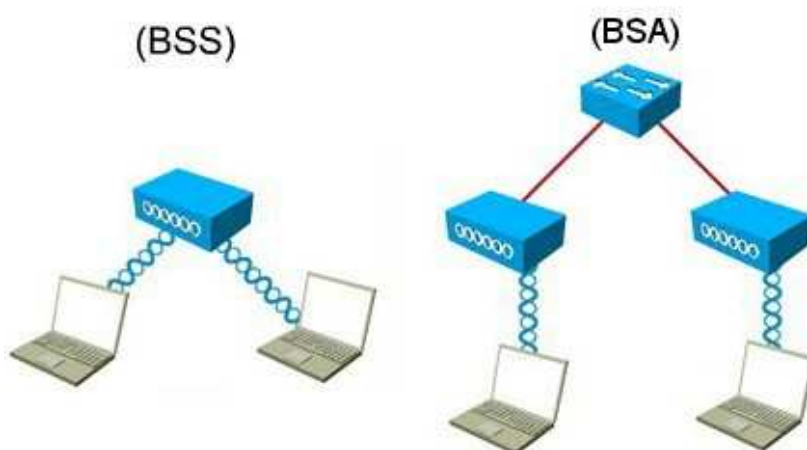
Bezdrátové médium je nosičem dat při přesunu dat od stanice ke stanici ve wifi standartu 802.11. Jsou to právě dvě frekvence: 2,4GHz a 5 GHz.

3.1.4 Stanice

Stanicí může být jakékoli zařízení s Wi-Fi (počítač, notebook, mobilní telefon, PDA). Stanice nemusí být mobilní (přenosná). Wi-fi síť se realizuje i mezi stolními počítači, pokud je například nejsou spojeny ethernetovými kabely.

3.2. Typy sítí

Základní stavební blok 802.11 sítě označujeme jako **Basic Service Set (BSS)** (obr. 6), tedy *základní soubor služeb*. Jde o skupinu stanic, které spolu komunikují. Tato komunikace probíhá v takzvaném **Basic Service Area (BSA)** (obr. 6), tedy území dosahu těchto stanic. Pokud se stanice nachází v BSA, může komunikovat s dalšími členy BSS. [9]



Obr. 6 – BSS, BSA

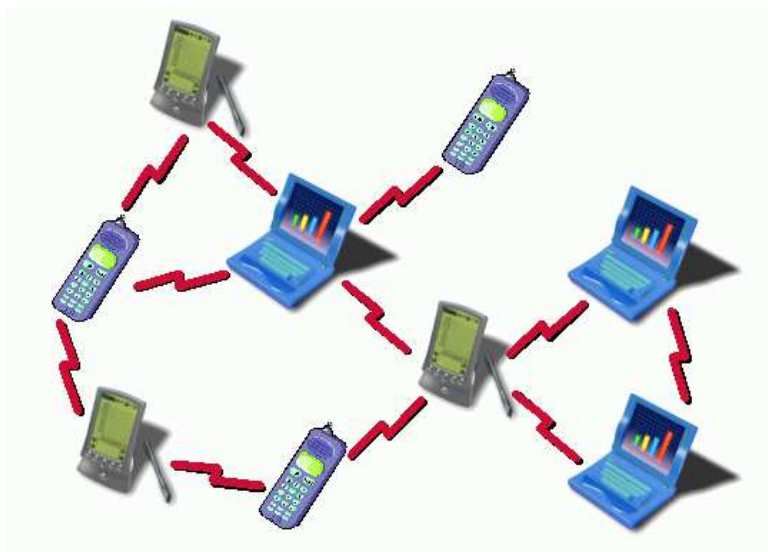
Rozlišujeme dva hlavní typy sítí podle toho, jak probíhá komunikace mezi členy BSS:

- Ad.hoc síť.
- Infrastrukturní.

3.2.1 Ad hoc síť

V tomto typu sítě spolu stanice komunikují přímo, nezávisle na prostředníkovi. Nejčastějším použitím je propojení několika počítačů na krátký čas, například pro jednorázovou výměnu dat nebo při takzvané LAN party. Stanice musí být ve vzájemném rádiovém dosahu, proto sítě ad-hoc nejsou vhodné pro rozsáhlejší prostory a členitější sítě

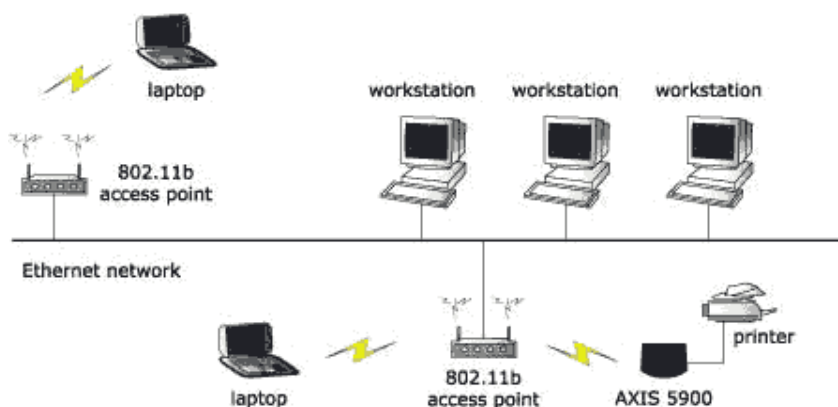
a vzájemná komunikace představuje větší nároky na klientskou stanici, která musí udržovat spojení s každou stanicí, s níž právě komunikuje (obr. 7).



Obr. 7 – Ad-hoc síť

3.2.2 Infrastrukturní síť

Infrastrukturní síť (obr. 8) se takto nazývají proto, že mají svoji přesně vymezenou infrastrukturu, neboť roli spojovacího článku zde přijímá síťová komponenta zvaná přístupový bod (*Access Point – AP*). AP je rozhraní mezi bezdrátovou a drátovou sítí a plní funkci datového mostu. Přístupový bod je schopen komunikovat s více než jednou stanicí a proto může propojovat i bezdrátové stanice, které se nalézají v jeho dosahu. Infrastrukturní síť nabízí centrální správu.

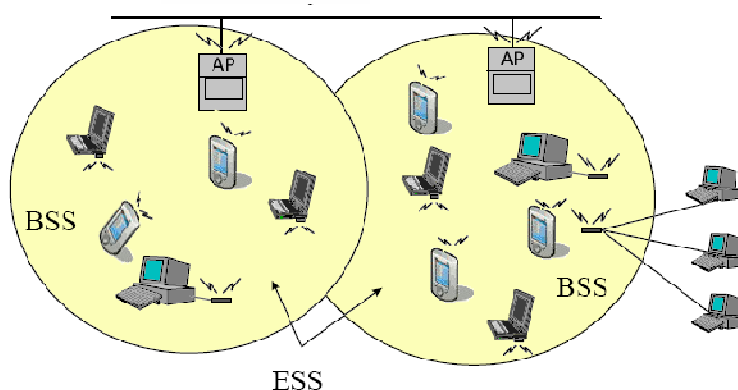


Obr. 8 – Infrastrukturní síť

V síti se musí stanice asociovat s přístupovým bodem, jinak vzájemné spojení není možné. Asociační proces vždy iniciuje mobilní stanice a přístupový bod připojení k sobě umožní, nebo zamítne. Pro stanici je asociace *exkluzivní*, což znamená, že nemůže být asociována k více přístupovým bodům. Díky tomu není možné jednu mobilní stanici připojit na více přístupových bodů, i když je v jejich dosahu.

Na straně přístupového bodu toto omezení není a standard nepředepisuje, kolik stanic smí přístupový bod asociovat. AP může být asociován s větším množstvím stanic (typicky 254), avšak přenosová rychlost se dělí mezi stanice. Pokud připojíme 254 stanic k AP s rychlostí 11 Mb/s (reálně 5 Mb/s), bude výsledná reálná průměrná rychlost $5 * 1024 / 254 = 20$ kb/s, což je málo.

Standard 802.11 dovoluje vytvoření větších sítí propojením BSS do takzvaných Rozšířených oblastí služeb – *Extend Service Set (ESS)* (obr. 9).



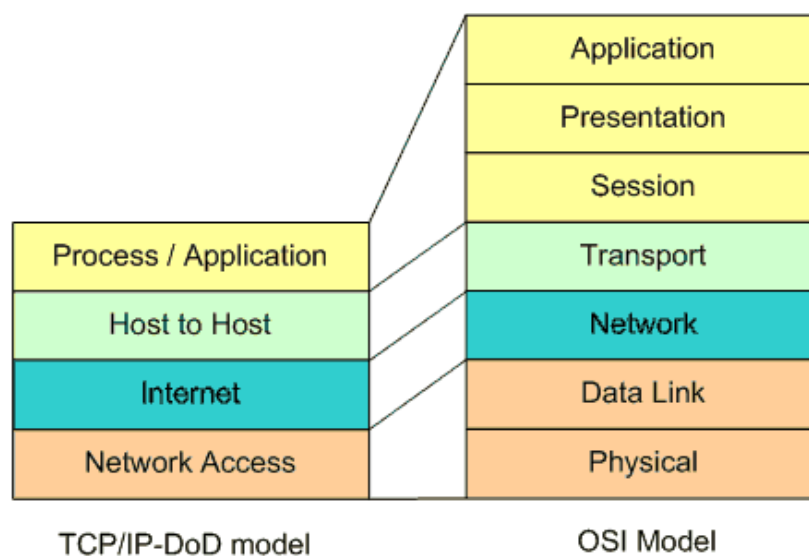
Obr. 9 – Rozšířená oblast služeb (ESS)

Stanice uvnitř ESS mohou mezi sebou komunikovat, ačkoliv jsou v rozdílných BSS. ESS vytvoříme propojením jednotlivých BSS přes páteřní síť. Standard 802.11 nepředepisuje, jakého typu páteřní síť musí být, pouze upřesňuje, jaké služby musí poskytovat. Při vytváření ESS je ale důležité pamatovat na to, že páteřní síť musí být v jedné doménové vrstvě.

3.3. OSI model

OSI model (obr. 10) je termín pro *Open Systems Interconnection Basic Reference Model*. Jedná se o doporučený model definovaný organizací **ISO** (International Standards Organization) v roce 1983, který popisuje síťové komunikace a protokoly použité pro komunikaci mezi počítači. Model je dělen do sedmi vrstev, při komunikaci se provádí *zapouzdření* - *encapsulate* na straně odesílatele a *rozbalování* na straně příjemce. Začíná se sedmou vrstvou, ta se zabalí do šesté vrstvy, atd. Tento model byl vytvořen proto, aby se standardizovala komunikace a hardware i software různých výrobců mohl vzájemně komunikovat. [13]

Přestože popis OSI modelu vznikl již před řadou let a považuje se za základ pro síťové technologie, nebyl nikdy přesně realizován. Obdobou OSI modelu je model **TCP/IP** (obr. 10), u kterého můžeme říci, že vychází z OSI modelu, ale upravuje jej, aby byl více flexibilní. Podle *OSI modelu* je vždy možno komunikovat pouze s vrstvou nad nebo pod, a všechny vrstvy musí být v komunikaci obsaženy, což v řadě praktických úloh přináší zbytečnou zátěž (časovou i datovou).



Obr. 10 – OSI a TCP/IP model

Nižší vrstvy relačního modelu OSI (fyzická, linková, síťová, transportní) jsou zaměřeny na předávání dat mezi dvěma uzly počítačové sítě. Vyšší vrstvy (relační, prezentační, aplikační) jsou pak již zaměřeny na potřeby síťových aplikací. Přitom využívají přenosové možnosti transportní vrstvy a k nim přidávají služby, které jsou užitečné pro většinu aplikací.

3.3.1 Jednotlivé vrstvy ISO/OSI modelu

- **Physical layer** (*fyzická vrstva*) – umožňuje komunikaci na nejnižší hardwarové úrovni, v podstatě řeší vlastní propojení. Zabývá se kabely, přenosovými médii, napěťovými a jinými fyzikálními hodnotami signálu. Příklad: 100BaseT, RS-232, 802.11g.
- **Data-link layer** (*linková vrstva*) – zajišťuje přenos jednotlivých bitů mezi dvěma uzlovými počítači, mezi kterými existuje přímé spojení. Linková vrstva navazuje na fyzickou vrstvu v tom, že využívá těchto spojení pro přenos větších bloků dat, které se označují jako *rámce* (frames). Přenos těchto rámců pak nabízí vyšší (sít'ové) vrstvě jako službu. Linková vrstva se dělí na horní subvrstvu zvanou **Logical Link Control** (LLC) a dolní subvrstvu zvanou **Media Access Control** (MAC). Mezi hlavní úkoly linkové vrstvy patří: synchronizace rámců (rozpoznání začátku i konce), zajištění spolehlivosti (detekce i korekce chyb), řízení toku dat (ochrana proti zahlcení), řešení konfliktů při vícenásobném přístupu ke sdílenému médiu. Příklad: Ethernet, Token Ring.
- **Network layer** (*sít'ová vrstva*) – úkolem vrstvy je najít vhodné spojení prostřednictvím uzlů a tak doručit *pakety* až k cílovému uzlu. Seřazuje přenášené rámce, stará se o nastavení parametrů přenosu linky, oznamuje neopravitelné chyby. Formátuje fyzické rámce, opatřuje je fyzickou adresou a poskytuje synchronizaci pro fyzickou vrstvu. Příklad: IP, ARP.
- **Transport layer** (*transportní vrstva*) – poskytuje efektivní přenosové služby své bezprostředně vyšší (tj. relační) vrstvě. Tyto služby přitom mohou mít spojovaný (connection-oriented) i nespojovaný (connectionless) charakter.
- **Session layer** (*relační vrstva*) - je spojení mezi dvěma uzly na úrovni bezprostředně vyšší, než je transportní vrstva. Hlavním úkolem je navazování, udržování a rušení relací a zajištění pravidelného střídání uzlů při vysílání. Příklad: NetBIOS.
- **Presentation layer** (*prezentační vrstva*) – zajišťuje správné předávání dat mezi počítači tak, aby byla zajištěna jejich správná konverze. Různé počítače totiž používají různou reprezentaci dat, např. kódování znaků (ASCII, EBCDIC), formátování čísel, šifrování, komprese dat a jiné. Příklad: Mpeg.

- **Application layer (aplikační vrstva)** - umožňuje aplikacím přístup do počítačové sítě na bázi ISO/OSI modelu. Funguje jako brána mezi aplikacemi běžícími v různých uzlech, které si vzájemně vyměňují informace. Aplikační vrstva obsahuje pouze jádro aplikací, které má smysl standardizovat (např. přenosové mechanismy elektronické pošty). Ostatní části aplikací (typicky uživatelská rozhraní) byly posunuty nad aplikační vrstvu. Příklad: FTP.

Standard 802.11 definuje pouze dvě nejnižší vrstvy OSI, tedy *fyzickou* a *linkovou*. Všechny ostatní vrstvy nechává standard 802.11 nedotčené. Linková vrstva, respektive její podvrstva označovaná jako **MAC** (Media Access Control), představuje soubor pravidel určujících jak přistupovat k prostředkům pro přenos dat. Samotné detaily o přenosu dat jsou ponechány na fyzické vrstvě **PHY**.

3.4. Linková vrstva a MAC podvrstva

MAC podvrstva slouží jako rozhraní mezi fyzickou vrstvou a hostitelským zařízením a také vytváří podporu ad-hoc sítě i infrastrukturního zapojení sítě.

Pro MAC podvrstvy jsou důležité dvě hlavní vlastnosti:

- Cyclic Redundancy Check (CRC) – cyklický kontrolní součet.
- Fragmentace paketů.

Každý přenášený paket je opatřen připojeným kontrolním součtem CRC. Díky tomu je možné zjistit, zda paket nebyl během přenosu poškozen nebo změněn. Funkce fragmentace paketů zase rozděluje pakety do menších částí a přenáší je postupně. Oproti kabelovému Ethernetu je totiž výrazně vyšší možnost chyby během přenosu paketu a opakovaný přenos celého paketu by síť zbytečně zdržoval. Pokud je přenášena jen jeho část, síť ušetří mnoho kapacity.

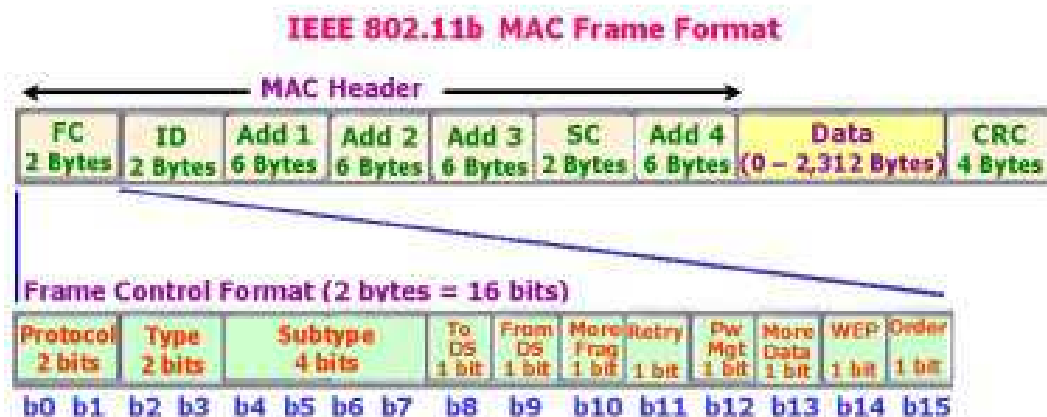
3.4.1 Formát MAC rámce

MAC rámec se skládá z **hlavičky** (header), které sestavuje informace o přenášených datech a **těla rámce** (frame body) obsahující samotná přenášená data a kontrolní součet CRC. [9]

3.4.2 Složení MAC rámce

MAC rámec se skládá z těchto částí (obr. 11):

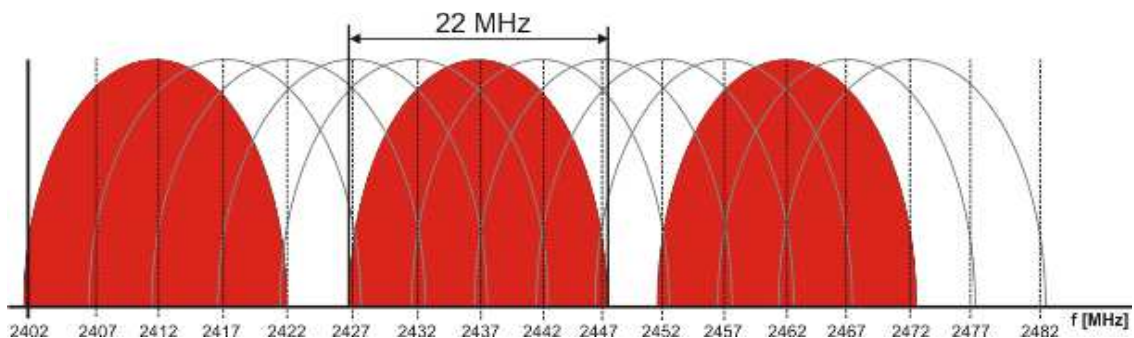
- **Frame Control (FC)** – obsahuje informace o verzi protokolu a typu rámce (řídící, datový a kontrolní).
- **Duration/ID (ID)**
 - Station ID je identifikátor stanice používaný pro funkci úspory energie.
 - Duration Value je délka trvání rámce použitelná pro výpočet rezervace přenosového média.
- **Address field 1-4** – jsou čtyři adresní pole obsahující adresy zdroje, cíle, přenašeče a příjemce v závislosti na poli Frame Control,
- **Sequence Control (SC)** – používá se pro defragmentaci a likvidaci duplikátních rámců.
- **Cyclic Redundancy Check (CRC)** – je cyklický kontrolní součet, který zjišťuje, zda byl paket během přenosu poškozen nebo změněn.



Obr. 11 – MAC rámec

3.5. Fyzická vrstva

Zařízení Wi-Fi lze provozovat, jak již bylo uvedeno, v tzv. ISM pásmech. ISM pásma jsou celosvětově rozšířená bezlicenční frekvenční pásma, která se nacházejí na frekvencích 900MHz, 2,4 až 2,48GHz a 5,1 až 5,8GHz. V České republice vymezuje provoz generální licence *ČTÚ VO-R/12/08.2005-34*. [7]



Obr. 12 – Rozprostření kanálů v ISM pásmu 2,4 GHz

Z obrázku 12 je patrné, že v celém pásmu 2,4GHz se nacházejí pouze tři nepřekrývající se kanály. Povolený vyzářený výkon (EIRP) celého vysílacího řetězce (vysílač + anténní svod + anténa) je maximálně **100mW (20dBm)**. Pro Českou republiku je v pásmu **2,4GHz** definováno **13 kanálů** o šířce **22MHz**. Rozstup mezi středy kanálů je pouhých 5MHz.

Pásmo 5GHz je rozděleno do tří účelově odlišených subpásem. Šířka kanálu pro toto pásmo byla stanovena na 20 MHz. První subpásmo je definováno mezi frekvencemi **5,125 až 5,25GHz**. Je určeno pro použití uvnitř budov a maximální dovolený vyzářený výkon je **200mW (23dBm)**. Druhé subpásmo se nachází mezi frekvencemi **5,25 až 5,35GHz**. V tomto subpásmu se nacházejí čtyři nezávislé kanály, na kterých lze vysílat ve venkovním prostředí. Maximální dovolený vyzářený výkon je stanoven na **200mW**, ale pouze tehdy, pokud je přenosový systém vybaven automatickou regulací výkonu. Pokud není v zařízení automatická regulace výkonu přítomna, je nutné výkon omezit na **100mW**. Poslední subpásmo určeno pro venkovní použití je definováno ve frekvenčním rozsahu **5,47 až 5,725GHz**. V tomto subpásmu se nachází 11 nezávislých kanálů, na kterých lze vysílat výkonem až **1W (30dBm)**. Platí zde ovšem stejné omezení jako v předchozím případě. Pokud není tato podmínka splněna, je nutné výkon o polovinu snížit, a to na hodnotu **500mW (27dBm)**.

Standard 802.11 umožňuje na rozdíl od jeho nástupců přenos také pomocí *infračervených vln* (IR). Tento způsob přenosu se však příliš nerozšířil. Hlavní příčinou byl malý dosah, nemožnost překlenout překážky a nízká přenosová rychlost, která nepřesáhla **2Mbit/s**.

Ve všech standardech 802.11 je fyzická vrstva rozdělena do dvou podvrstev:

- **PLCP (*Physical Layer Convergence Procedure*)** – v této podvrstvě se k datovým rámcům **MAC** (Medium Access Control) podvrstvy přidávají informace o použitém přenosovém mechanismu a modulaci. Díky této podvrstvě je přenášený datový rámec nezávislý na typu fyzické vrstvy. Do této podvrstvy je implementována rovněž funkce **CCA** (Clear Channel Assessment), která poskytuje odezvu pro MAC vrstvu o připravenosti přenosového média.
- **PMD (*Physical Medium Dependent*)** – tato podvrstva je zodpovědná za přenos dat mezi jednotlivými vysílači a přijímači. Z podvrstvy PLCP jsou data v závislosti na použitém přenosovém mechanismu ve vysílači vysílána do bezdrátového prostředí, kde jsou na straně přijímače pomocí PMD přijímána a předávána podvrstvě PLCP.

3.6. Zabezpečení bezdrátové sítě

V dnešní době používá většina domácností pro připojení na Internet Wi-Fi router. Často se stává, že si vlastník routeru se zabezpečením moc hlavu neláme a většinou nechává zvolené „tovární“ nastavení. Stává se tím nedobrovolně poskytovatelem internetového připojení pro další osoby. [8]

Bezpečnost bezdrátových Wi-Fi sítí můžeme rozdělit do dvou hlavních skupin:

- **Šifrování** - zabezpečení přenášených dat před odposlechem.
- **Autorizace** - řízení přístupu oprávněných uživatelů.

Způsoby zabezpečení Wi-Fi sítí

3.6.1 Změna hesla přístupu k routeru

Přihlašovací jméno mají téměř všichni výrobci stejné – „admin“, heslo se sice liší, ale i začínající hacker ví, že výrobce ZyXEL používá „1234“, Netgear „password“ a D-Link ve svých routerech heslo přednastavené nemá. Proto je bezpodmínečně nutné přístupové heslo na router změnit.

3.6.2 Blokace vysílání SSID

Zablokováním identifikátoru SSID se sice porušuje standard, ale jedná se o nejjednodušší zabezpečení. Daná síť se nezobrazí v seznamu dostupných bezdrátových sítí, protože nepřijímají broadcasty se SSID. Pro připojení musí uživatel znát název sítě.

3.6.3 Omezení síly vysílaného Wi-Fi signálu

Pokud na routeru v malém objektu nastavíme zbytečně vysokou sílu signálu, riskujeme, že síť bude viditelná i mimo tento objekt. Obecně platí pravidlo, že síť by neměla přesahovat hranici objektu. V praxi je ovšem většinou toto pravidlo složité dodržet, hlavně v bytové zástavbě.

3.6.4 Manuální nastavení IP adresy

Jedna z prvních ochran přístupu na AP (*Access Point*) je zamezení automatického přidělování IP adresy, masky, brány a DNS (*Domain Name System*), tzv. **DHCP** (*Dynamic Host Configuration Protocol*) serveru. Pro útočníka není toto zabezpečení nepřekonatelné, např. pomocí programu Wireshark může vysledovat provoz sítě a tím zjistit potřebné nastavení. Existuje ovšem program *fake IP*, který náhodně vysílá stovky IP a tím útočnickovi výrazně stěžuje odchyťování potřebného nastavení.

3.6.5 Kontrola MAC adres

MAC adresa je unikátní identifikace každého síťového zařízení. V routeru můžeme manuálně nastavit, kterým zařízením je dovolen přístup, a kterým ne. Pro zkušenějšího útočníka není filtrování MAC adresy překážkou, protože např. pomocí programu

Wireshark může vysledovat provoz sítě a tím zjistit potřebnou MAC adresu. Změna MAC se na útočnickově stanici změní, např. příkazem *macchanger* (Linux).

3.6.6 WEP

WEP (*Wireless Equivalent Privacy*) je označení pro zabezpečení bezdrátové sítě na základě standardu IEEE 802.11 z roku 1997. WEP pracuje na linkové vrstvě ISO-OSI modelu, kde šifruje pakety pomocí *proudové šifry RC4*. Existuje ve verzi 64 bitů, který používá 40 bitový klíč s 24 bitovým inicializačním vektorem a delší 128 bitový klíč, který používá 104 bitový klíč s 24 bitovým inicializačním vektorem.

K šifrování se používá RC4. Data se zpracovávají po jednotlivých bitech a pro kontrolu integrity se používá metody **CRC-32**. Šifrování probíhá za použití klíče, který je složen z uživatelského klíče (hesla) a inicializačního vektoru. Nejprve se za pomoci CRC-32 spočítá kontrolní součet k ověření integrity (*Integrity Check Value*). Z inicializačního vektoru a uživatelského klíče se pomocí šifry RC4 spočítá šifrovací klíč, který musí mít stejnou velikost jako zpráva s kontrolním součtem. Dále je mezi zprávou a šifrovacím klíčem proveden logický součet XOR a nakonec výsledné zprávy je připojen inicializační vektor, který slouží pro dešifrování zprávy.

Pro neúplnost standardu a dalším vadám v implementaci byl WEP v roce 2001 prolomen. Stačil pouze pasivní odposlech bezdrátového provozu a za pomoci příslušného programu získat šifrovací klíč. Později došlo k vylepšení původního zabezpečení. **WEP2** rozšiřuje inicializační vektory a zesiluje 128 bitové šifrování. WEP2 má ovšem stejné bezpečnostní problémy jako WEP, jen k prolomení šifry je třeba odchytit více IV paketů.

3.6.7 WPA

WPA (*Wi-Fi Protected Access*) obecně vychází ze standardu **IEEE 802.11i** (WPA2). WPA vznikl v roce 2002 ze standardu WEP jako rychlá reakce na nedostatečné zabezpečení. Důležitým cílem WPA bylo použít již vyráběný hardware, který podporoval zabezpečení WEP a pouhou aktualizací (firmware, software) umožnit využití nového zabezpečení. WPA stejně jako WEP k šifrování používá *proudovou šifru RC4* s 128 bitovým klíčem a 48 bitovým inicializačním vektorem. Navíc je implementovaný *protokol TKIP* (*Temporal Key Integrity Protocol*), který zavedl dynamickou správu šifrovacích

klíčů, které jsou mezi účastníkem a routerem přenášeny na začátku komunikace, ale i během ní, čímž brání útočníkovi v útoku opakovaním. TKIP mění klíč pro každý odeslaný paket a tím je nemožné odposlechnout dostatek paketů stejného šifrovacího klíče. Pro kontrolu integrity dat se používá **MAC** (*Message Authentication Code*), konkrétně algoritmus nazvaný *Michael*, který je zde nazýván **MIC** (*Message Integrity Code*). MIC probíhá na základě hashovací funkce, která využívá dvojnásobné délky IV, než WEP. Ke každému rámci přidává digitální podpis, který se vypočítává z datové části paketu, zdrojové a cílové MAC adresy, pořadového čísla rámce a náhodné hodnoty. V případě kolize integritní kontroly dojde k automatické výměně klíčů, neboť toto chování je vyhodnoceno jako útočné.

Autentizace účastníka je pro WPA navržena buď pro použití předsdílené fráze **PSK** (*Pre-shared key*) nebo pro použití s autentizačním serverem (typicky **RADIUS** - *Remote Authentication Dial In User Service*, česky - *Uživatelská vytáčená služba pro vzdálenou autentizaci*) pomocí protokolu IEEE 802.1X.

ZDNet (*business technology news website*) dne 18. 6. 2010 vyhlásil, že **WEP a TKIP budou brzy pro jejich nedostatečné zabezpečení zakázány ve Wi-Fi zařízeních.**

3.6.8 WPA2

WPA2 je také známý pod označením IEEE 802.11i, který byl schválen 24. 6. 2004. WPA2 je dodatek ke standardu IEEE 802.11 a jeho předchůdce WPA implementuje pouze třetí návrh tohoto standardu, tedy pouze část tohoto standardu. WPA2 používá **blokovou šifru AES** (*Advanced Encryption Standard*), zatímco dřívější WEP a WPA používají **proudovou šifru RC4**. Data jsou šifrována symetrickým klíčem po blocích o velikosti 128 bitů. Pro autentizaci dat se používá protokol **EAP** (*Extensible Authentication Protocol*) a **autentizační server**. Kontrola integrity dat je prováděna pomocí protokolu **CCMP** (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*), který poskytuje utajení, integritu a autentizaci. Autentizace účastníka je pro WPA2 navrženo buď PSK nebo 802.1X (RADIUS server).

4. EVOLUČNÍ ALGORITMY

4.1. SOMA

SOMA algoritmus patří také do skupiny memetických či hejnových algoritmů. Potomci se nevytvářejí křížením jako u jiných evolučních algoritmů, ale filozofie algoritmu je založena na pohybu inteligentních jedinců, tj. migraci jedinců. Tito jedinci spolupracují při řešení společného problému. Jedinci prohledávají prostor a hledají např. potravu. Evoluční cyklus se tedy nenazývá generace, ale *migrace*. Nejedná se o vývoj nových jedinců, ale o přesun původních jedinců na nové pozice. Příkladem takového chování jsou např. mravenci, včely, predátoři ve smečce hledající potravu, apod. Vlastnost samo-organizace u algoritmu SOMA plyne z faktu, že se jedinci ovlivňují navzájem během hledání lepšího řešení, což mnohdy vede k tomu, že v prostoru možných řešení vznikají skupiny jedinců, které se během putování přes prohledávaný prostor rozpadají či spojují. [1]

4.1.1 Parametry algoritmu SOMA

Běh algoritmu SOMA je ovlivňován speciální množinou parametrů, které lze rozdělit na parametry *řídící* a *ukončovací*. Řídící parametry jsou takové parametry, které mají vliv na kvalitu běhu algoritmu, zatímco ukončovací parametry představují předem nadefinované podmínky, které běh algoritmu ukončují. Všechny tyto parametry musí být zvoleny uživatelem před začátkem samotného algoritmu. Parametry a jejich doporučené hodnoty pro SOMA algoritmus popisuje následující tabulka. [1]

<i>Parametr</i>	<i>Doporučený rozsah</i>	<i>Poznámka</i>
PathLength	[1,1; 5>]	Řídící parametr
Step	[0,11; PathLength]	Řídící parametr
PRT	[0; 1]	Řídící parametr
D	Ovlivněno daným problémem	Počet argumentů účelové funkce
PopSize	[10; definuje uživatel]	Řídící parametr
Migrace	[10; definuje uživatel]	Ukončovací parametr
MinDiv	[± libovolný; definuje uživatel]	Ukončovací parametr

Tabulka 2: Parametry algoritmu SOMA

PathLength – určuje, jak daleko se aktivní jedinec zastaví od vedoucího jedince.

Step – určuje velikost skoku jedince. Pokud není tvar účelové funkce známý, doporučuje se nastavit jeho hodnotu na 0,11. Parametr Step nesmí být celočíselným násobkem parametru PathLength – jinak by došlo ke snížení diverzibility populace a proces by tak mohl rychleji skončit v lokálním extrému.

PRT– tzv. *pertubace*. Podle tohoto parametru se tvoří pertubační vektor, který ovlivňuje, zda se aktivní jedinec bude pohybovat přímo k vedoucímu jedinci či ne.

D – je počet optimalizovaných proměnných.

PopSize – je řídicí parametr, který určuje počet jedinců v populaci.

Migrace – určuje, kolikrát se populace změní.

MinDiv– určuje maximální možný rozdíl mezi nejhorším a nejlepším jedincem v populaci.

4.1.2 Jednotlivé kroky algoritmu SOMA

- *Definice parametrů*

Před samotným spuštěním algoritmu je nutné nejprve definovat veškeré potřebné parametry – řídicí a ukončovací parametry (Specimen, Step, PathLength, MinDiv, Popsize, PRT a Migrace). Dalším důležitým krokem, je nadefinovat účelovou funkci, která reprezentuje optimalizovaný problém. Řešením pak je nalezení jejího nejlépe globálního extrému, tedy optimální hodnoty parametrů.

- *Tvorba populace*

V tomto kroku vytvoříme počáteční populaci náhodným vygenerováním jedince. S využitím parametru Specimen a generátoru čísel je pro každý parametr jedince generováno náhodné číslo (jeho hodnota je dána rozsahem Specimenu).

- *Migrační kola – migrace*

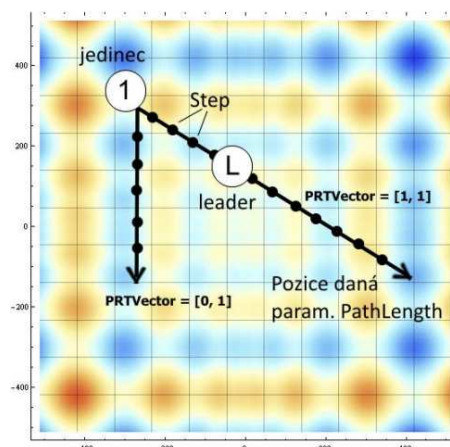
Každého jedince ohodnotíme účelovou funkcí a určíme mezi jedinci Leadera. V tuto chvíli dochází k migraci ostatních jedinců směrem k Leaderovi po zvolených krocích (parametr Step). Znovu dochází k ohodnocení jedinců účelovou funkcí, a pokud se u některých jedinců změní hodnota k lepšímu – jedinec si ji zapamatuje. Po skončení migračního kola se všichni jedinci posunou na novou, nejlépe ohodnocenou pozici. Leader zůstává na místě. Než daný jedinec započne svou cestu směrem k Leaderovi, je vygenerován prázdný PRT Vector o dimenzi D včetně vygenerované sekvence náhodných čísel z intervalu $\langle 0,1 \rangle$ pro každý optimalizovaný parametr. Tato náhodná čísla jsou porovnána s parametrem PRT. Jestliže je n-té vygenerované číslo větší nežli PRT parametr, pak je n-tý parametr PRT Vectoru nastaven na 0 a v opačném případě na 1. Parametry jedince, které jsou takto nastaveny na 0, se nepřepočítávají (tj. jsou zmrazeny), tím se snižuje počet stupňů volnosti pohybu jedince. Tento proces nahrazuje operátor mutace, jež obvykle u evolučních algoritmů probíhá. Díky tomu se rapidně zvyšuje robustnost SOMA algoritmu ve smyslu nalezení globálního extrému.

- *Zjištění stavu ukončovacích parametrů*

Nyní zkontrolujeme, zda je rozdíl mezi Leaderem a nejhorším jedincem menší než MinDiv. Stejně tak ověříme, zda došlo k naplnění počtu migračních kol – parametr Migrace. Pokud není splněna ani jedna podmínka, algoritmus se vrací do předcházejícího kroku a pokračuje, jinak se algoritmus zastaví.

- *Stop*

Získáváme nejlepšího nalezeného jedince (řešení) po ukončení posledního migračního kola.



Obr. 13 – Funkce PRT

4.1.3 Strategie SOMA

V dnešní době existuje již několik různých variací algoritmu SOMA. Pro jejich obecné označení se používá výraz *strategie*, kterou lze rozdělit na: [4]

- *AllToOne*

Všichni jedinci kromě vůdce putují za vůdcem.

- *AllToAll*

V každém migračním kole se vůdcem stávají postupně všichni jedinci a ostatní putují za nimi. Po dokončení migrace aktuálního jedince se daný jedinec vrátí na pozici, kde byl nalezen nejlepší extrém. Tato strategie je náročná na výpočet.

- *AllToAllAdaptive*

Strategie totožná s AllToAll s tím rozdílem, že se aktuální migrující jedinec přesune na novou pozici nalezenou na jeho cestě ihned, nikoli až po migracích všech ostatních jedincův populaci.

- *AllToOneRand*

Strategie, kde opět existuje Leader a jedinci se snaží k němu přiblížit. Leader však není vybírán podle nejlepšího ohodnocení, ale náhodným výběrem. Zde je tedy možná určitá modifikace algoritmu, kdy Leader bude vybírán daným algoritmem.

4.2. Diferenciální evoluce

Diferenciální evoluce je postup k heuristickému hledání minima multimodálních funkcí, který navrhli R. Storn a K. Price koncem 90. let 20. století. Experimentální výsledky i zkušenosti z četných aplikací ukazují, že často konverguje rychleji než jiné stochastické algoritmy pro globální optimalizaci. [1]

4.2.1 Parametry Diferenciální evoluce

Parametry a jejich doporučené hodnoty algoritmu pro Diferenciální evoluci popisuje následující tabulka. [1]

<i>Parametr</i>	<i>Interval</i>	<i>Doporučený rozsah</i>	<i>Poznámka</i>
NP	[10D, 100D]	10D	Jestliže je fce vysoce multimodální – velikost populace 100D
F	[0, 2]	0,3 - 0,9	Mutační konstanta
CR	[0, 1]	0;8 – 0,9	Práh křížení $CR \ll 1$, jestliže je fce separabilní a $CR \approx 1$, jestli je neseperabilní
Generations	Uživatel		Počet kol šlechtění

Tabulka 3: Parametry Diferenciální evoluce

Vysvětlení parametrů v tabulce:

CR – jedná se o práh křížení. V případě, že se jedná o funkci, která je separabilní, pak je doporučeno nastavit tento parametr na hodnoty blízké 0. V opačném případě jsou výhodné hodnoty, které se blíží k 1. V případě, že se CR nastaví na 0, dojde k tomu, že se mutace nedostane do zkušebního jedince a vývoj evoluce se pak zastaví. V případě, že CR bude nastaven na 1, bude zkušební jedinec tvořen pouze ze tří náhodně vybraných rodičů - jedinců z populace, se diferenciální evoluce se bude spíše podobat náhodnému hledání nežli evolučnímu algoritmu. Je proto vhodné, aby CR nikdy nenabývalo těchto hodnot.

D – dimenze problému. Jde o počet argumentů účelové funkce. Parametr je dán řešeným problémem a zle ho měnit pouze reformulací problému.

NP – jedná se o parametr udávající velikost populace, který by neměl být menší než 4.

F – jedná se o mutační konstantu.

Generations – udává počet evolučních cyklů, tzv. generací, během nichž se celá populace vyvíjí.

4.2.2 Jednotlivé kroky Diferenciální evoluce

- **Definice parametrů**

Před samotným spuštěním algoritmu je nutné nejprve definovat veškeré potřebné parametry – mutační konstanta F , práh křížení CR , počet jedinců v populaci NP , rozměr jedince D . Dále je nutné nadefinovat prototyp jedince – Specimen, nebo-li z jakých typů čísel se budou jedinci skládat.

- **Tvorba populace**

Populace se tvoří vygenerováním množiny jedinců (matice) podle prototypového (Specimen) vektoru. U každého jedince se musí počítat s jedním prvkem navíc a tím je hodnota účelové funkce.

- **Započetí kola migrace**

Během každé generace se provádí ještě cyklus, který zabezpečuje postupné evoluční šlechtění každého jedince z populace. V tomto cyklu se postupně vybírají všichni jedinci z celé populace a pro každého jedince je proveden následující evoluční cyklus.

- **Evoluční cyklus**

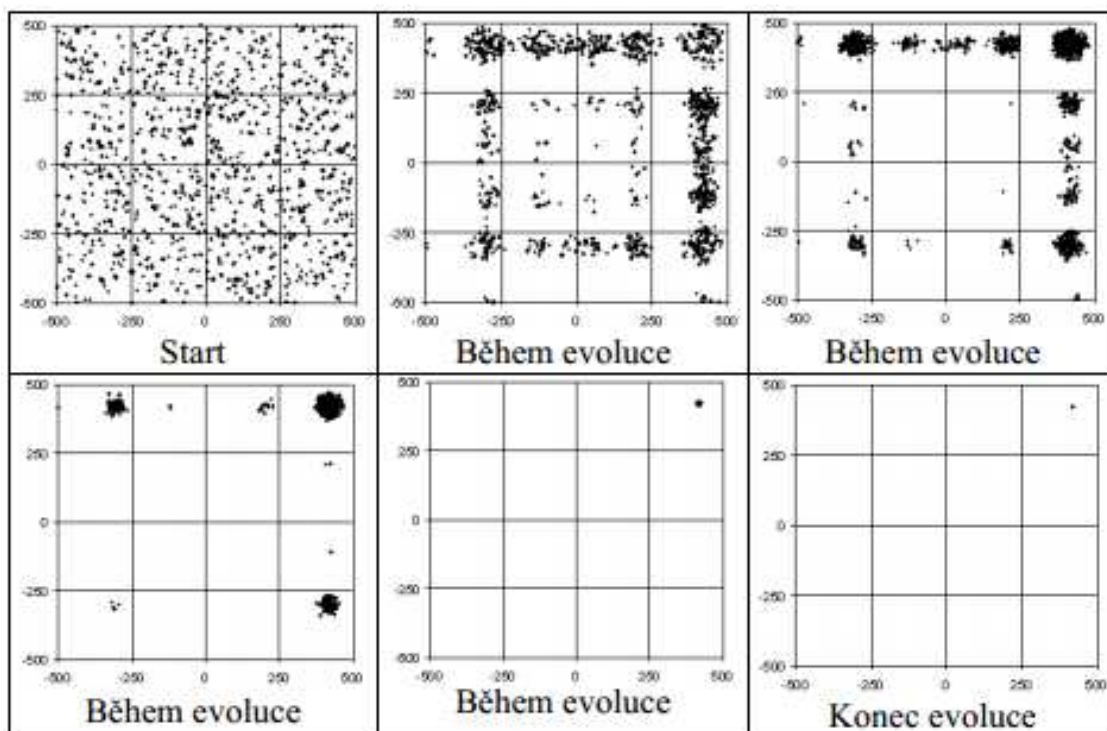
V tomto cyklu se náhodně zvolí tři další různí jedinci z populace. První dva se od sebe odečtou a získá se tak tzv. *diferenční vektor*. Ten se vynásobí mutační konstantou F , která zmutuje a získá *váhovaný diferenční vektor*. Ten se přičte k třetímu jedinci a získá se tzv. *šumový vektor*. Poté se připraví tzv. *zkušební vektor* a ze šumového vektoru se bere postupně jeden prvek za druhým (první z obou, druhý z obou, ...) a pro takto vybranou každou dvojici se generuje náhodné číslo v intervalu $\langle 0-1 \rangle$ a porovnává se s konstantou CR . Pokud je toto číslo menší než CR , pak se do příslušné pozice v tzv. *zkušebním vektoru* umístí prvek z vektoru šumového a v opačném případě z vektoru cílového. Tím je zajištěno, že se do nové generace dostanou jedinci s lepšími vlastnostmi.

- **Testování naplnění ukončovacích parametrů**

Diferenciální evoluce je ukončena pouze tehdy, provede-li se uživatelem zadaný počet generací. Jiný ukončovací parametr tento algoritmus ve své základní verzi nemá.

- *Vyhodnocení*

Během každé generace se uchovává hodnota účelové funkce nejlepšího jedince. Tyto hodnoty lze pak vykreslit do grafu, který zachycuje historii vývoje průběhu evolučního procesu. Celý proces se opakuje, dokud není vyčerpán zadaný počet generací. [1]



Obr. 14 – Konvergence populace do globálního extrému na funkci při NP=20, F=0,5, CR=1,0

II. PRAKTICKÁ ČÁST

5. POPIS PROSTŘEDÍ

Pro realizaci svého záměru jsem si vybral prostory firmy IBM, ve které již třetím rokem pracuji. Zajímalo mě, jakým způsobem je řešena bezdrátová Wi-Fi síť na ploše jednoho patra, jaké pokrytí z hlediska signálu je dosaženo v odlehlejších místech a v tzv. quiet rooms, které jsou nově odděleny cihlovou zdí tloušťky 150mm a dveřní výplní s voštinovou výplní. Jednotlivá pracovní místa jsou typu open space, což je pro šíření signálu příznivější. Celé patro má rozměry 55x55m a jeho půdorys je ve tvaru písmene U.



Obr. 15 – Celkový pohled na budovu



Obr. 16 – Interiér budovy

5.1. Problémy se šířením signálu uvnitř budov

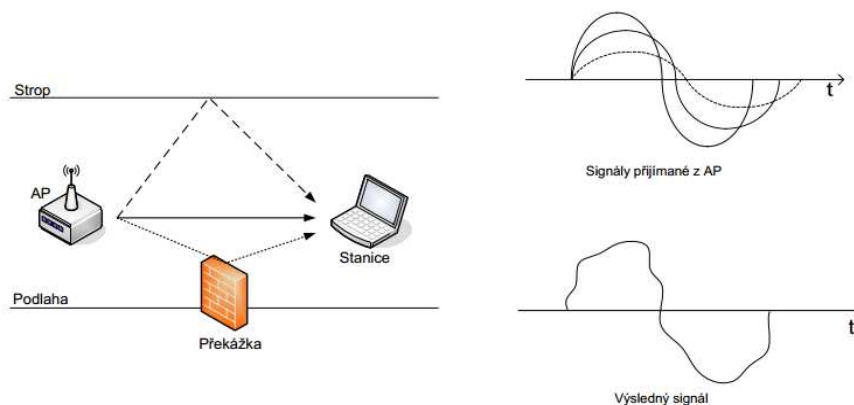
- Vícecestné šíření signálu (vícecestné interference).
- Ztráty průchodem přes překážky (zdi, podlaží).
- Rušení jinými systémy.

5.1.1 Vícecestné šíření signálu- odstranění problému

Pokud rádiová vlna narazí na překážku, pak se část energie odrazí, část se absorbuje a zbytek oslabené vlny prochází překážkou. Například kovové materiály odráží veškerou energii vlny, naopak voda velkou část energie absorbuje. Odraz je také závislý na úhlu dopadu, tloušťce a elektrických vlastnostech materiálu. Při použití všesměrových antén (orb. 17) se signál šíří všemi směry a odráží se od stěn, stropů a předmětů. Každý odražený signál má jinou dráhu, tudíž i jinou dobu šíření (dochází k posunutí fáze a útlumu signálu). Rádiový signál je vlnění, které se v každém bodě skládá z protínajících se signálů. Například u standardu IEEE 802.11b nesmí zpoždění odražené vlny překročit 500 ns. Vícecestné šíření je hlavně ve vnitřních prostorách, kdy do přijímací antény dorazí odražený signál se zpožděním od přímého signálu. Problém s interferencí se řeší pomocí dvou antén, k příjmu je vybrána ta, která má lepší signál. K vysílání se používá jen jedna anténa. [6]

Způsoby odstranění problému:

- Vhodné rozmístění stanic.
- Použití vhodných antén (sektorové, směrové).
- OFDM modulace.



Obr. 17 – Vícecestné šíření signálu

5.1.2 Ztráty průchodem přes překážky

Překážky mohou být pohyblivé (pohyb osob) nebo stacionární (stěny, různé předměty). Útlumy lze zjistit pomocí měření a následného výpočtu. Z výsledné hodnoty se odečte útlum volného prostoru mezi vysílači. Výsledný útlum je ovlivněn tloušťkou a materiálem překážky, kdy kov vlny odráží a voda vlny absorbuje. Útlum narůstá se zvětšující se frekvencí. [12] Velikost útlumu překážkou lze spočítat dle následujícího vztahu:

$$L = 10 \cdot \log\left(\frac{P_2}{P_1}\right), \text{ kde}$$

L – ztráty vlivem překážek [dB],

P_1, P_2 – výkon vyslaný a přijatý [W].

5.1.3 Rušení jinými systémy

Rušení jinými systémy je způsobeno:

- Nekvalitní Wi-Fi hardware (přístupové body, klientské adaptéry).
- Špatně provedený anténní svod.
- Nekvalitně odrušené okolní přístroje (mikrovlnné trouby, atd. ...).
- Jiné rušení.

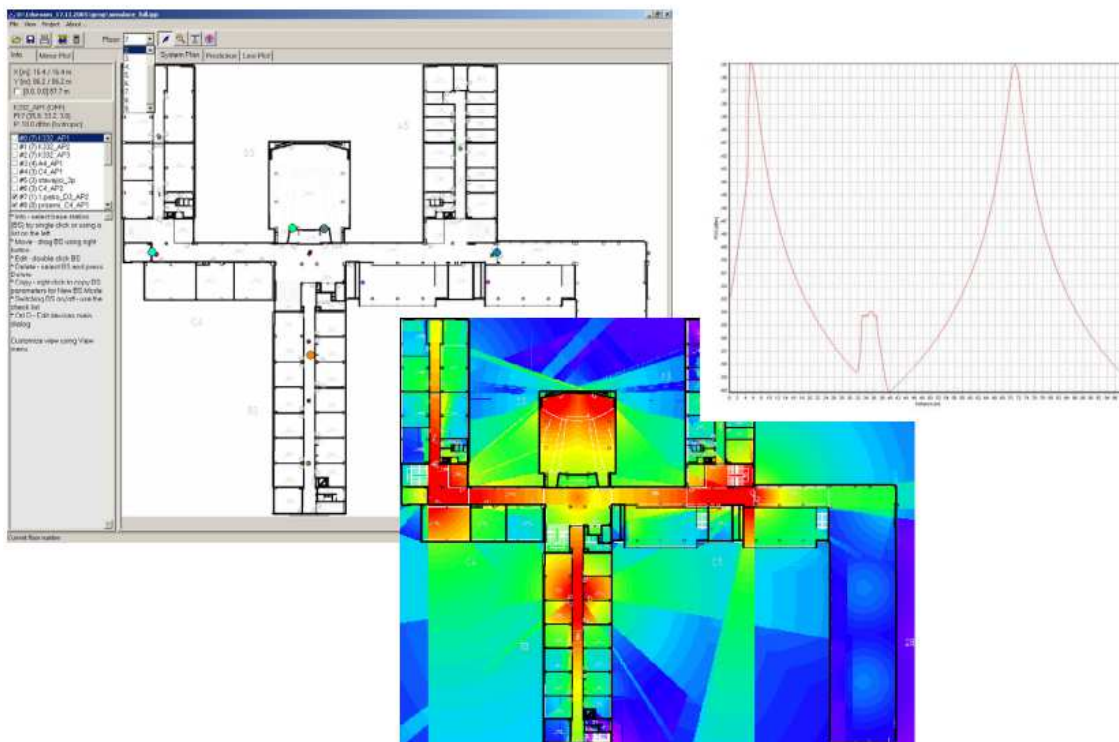
5.2. Simulační software pro šíření signálu v budovách

V současné době se nejčastěji pro simulaci a testování šíření Wi-Fi signálu v budovách používají programy Ekahau Site Survey a Ekahau Heatmapper od firmy Ekahau (www.ekahau.com). Zmínit musím ale ještě český program I-Prop, u kterého byl ovšem vývoj již ukončen.

5.2.1 Program I-Prop 1.39

- Softwarový nástroj pro interaktivní plánování bezdrátových systémů uvnitř vícepodlažních objektů.
- Software je postaven na modelech „One Slope“ a „Multi Wall“.
- Vyznačuje se jednoduchým ovládním.

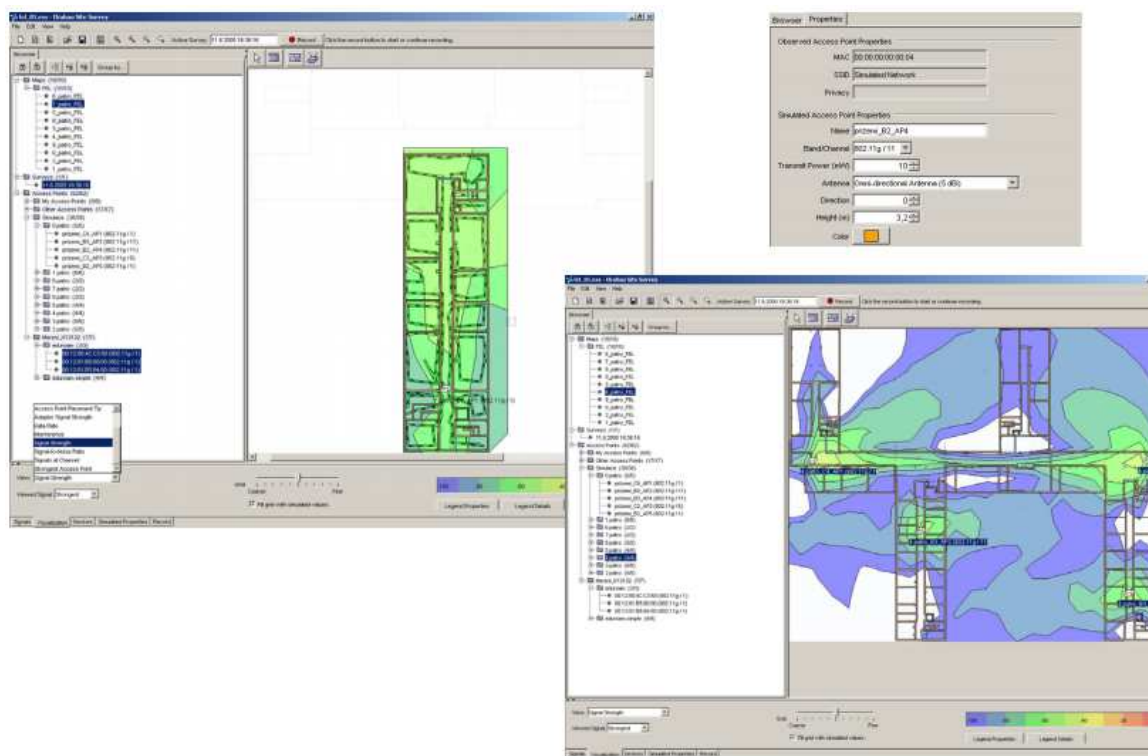
- Software je možno použít pro plánování sítí GSM, WiFi a Wimax.
- Výsledky simulací lze exportovat jako obrázky.



Obr. 18 – Ukázka práce v programu I-Prop

5.2.2 Program Ekahau Site Survey 2.1

- Jedná se o kompletní softwarový nástroj pro návrh a následné měření Wi-Fi sítí.
- Jsou podporovány standardy IEEE 802.11a/b/g/n.
- Program umožňuje provádět predikci v rámci jednoho podlaží.
- Uživatel si může nakonfigurovat vlastní překážky a antény.
- Programem lze provádět i samotné měření signálu.
- Program může spolupracovat se systémem GPS.
- Všechny výsledky měření a simulace jsou zobrazovány graficky.
- Ze všech měření a simulací lze vygenerovat přehledné reporty.



Obr. 19 – Ukázka práce v programu Ekahau Site Survey

5.2.3 Porovnání programů I-Prop a Ekahau Site Survey

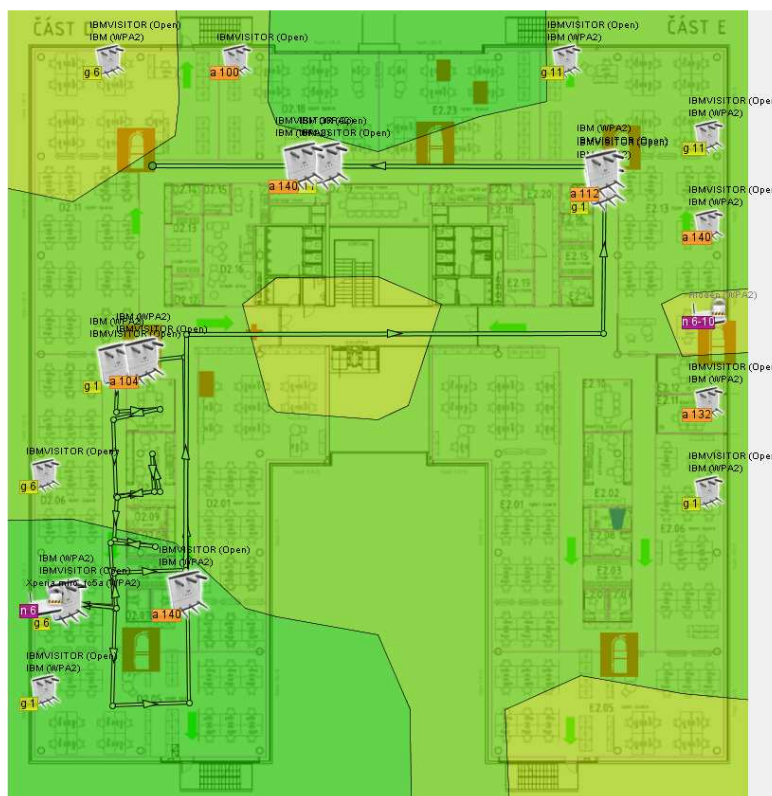
I-Prop 1.39	Ekahau Site Survey 2.1
+ Jednoduchá obsluha	+ Intuitivní ovládání
+ Vícepodlažní predikce	+ Přehledný grafický výstup
+ Použití pro velký rozsah frekvencí	+ Možnost vytvářet reporty
+ Malá velikost programu	+ Možnost definovat vlastní antény a překážky
-Velká časová náročnost při výpočtech	-Lze použít jen pro jedno patro
-Méně přehledný grafický výstup	-Určeno pouze pro Wi-Fi (2,4 a 5,5GHz)
-Možnost definovat pouze čtyři typy překážek	-Náročnost na systém

Tabulka 4: Porovnání programů I-Prop a Ekahau

5.2.4 Ekahau HeatMapper

Jedná se o aplikaci, která dokáže vytvořit pěknou a přehlednou mapu pokrytí bytu, kanceláře či jiného místa Wi-Fi sítí. Rozdíl mezi programy Ekahau Site Survey a Ekahau HeatMapper je ten, že HeatMapper slouží pro testování pokrytí signálu v daném prostředí bez možnosti předchozí simulace. Program je možno bezplatně stáhnout ze stránek výrobce. V praxi testování síly signálu probíhá tak, že se do programu importuje mapa budovy (nožné soubory pro import *.jpg, *.bmp, *.wbmp, *.png, *.gif, *.svg), a po přihlášení se do Wi-Fi sítě se v mapě budovy vyznačí trasa, po které se koná pohyb. Program sám v daném prostředí vyhledává Access Pointy. Po projití zvolené trasy program přehledně ukáže sílu signálu ve všech částech podlaží. Síla signálu je přehledně barevně rozlišena, podobně jako u termovize. Zelená místa znázorňují nejsilnější pokrytí a červená nejslabší. Testování síly signálu jsem pomocí tohoto programu provedl v budově firmy (obr. 20).

Daný výsledek testování reflektuje aktuální stav síly a rozmístění Wi-Fi AP v budově. Z obrázku je patrné, že všechna místa podlaží jsou bezdrátovým signálem pokryta. Z výsledného měření je také patrné, že u větších zasedacích místností je navíc k dispozici připojení k návštěvnické síti. Tato verze programu bohužel neumí vybrat konkrétní bezdrátovou síť, jejíž sílu signálu chceme otestovat na konkrétním prostředí, ale vždy se zobrazují všechny dostupné bezdrátové sítě v dané oblasti.



Obr. 20 – Výsledek měření síly signálu v prostorách firmy

5.3. Měření a simulace

Aby bylo možné přesně provést simulaci v simulačním programu I-Prop, musíme změřit útlumy stavebních materiálů. Jednotlivé výsledky měření jsem převzal z experimentů, které probíhaly VŠB Technické univerzitě v Ostravě v budově na Krásném poli učebně KrP203 [10]. Předmětem měření bylo zjistit útlumy stavebních materiálů – cihlových příček šíře 150mm, dřevěných dveří s voštinovou výplní, železobetonového stropu tloušťky 450mm a nosníků šíře 300mm. Kolektiv autorů pro simulaci použil tyto přístroje:

- První sestava se skládala z routeru Cisco Aironet 1242 nastaveného na vysílací výkon -1dBm, ke kterému byla připojena směrová anténa ISM14 (AS4-14) se ziskem 14dBi. Mezi anténou a vysílačem byl pigtail s útlumem 2dB, 2 konektory s útlumem 2dB a půl metru koaxiálního kabelu s celkovým útlumem 0,11dB. Celkový vysílací výkon byl 9dBm. Výpočet vysílacího výkonu EIRP:

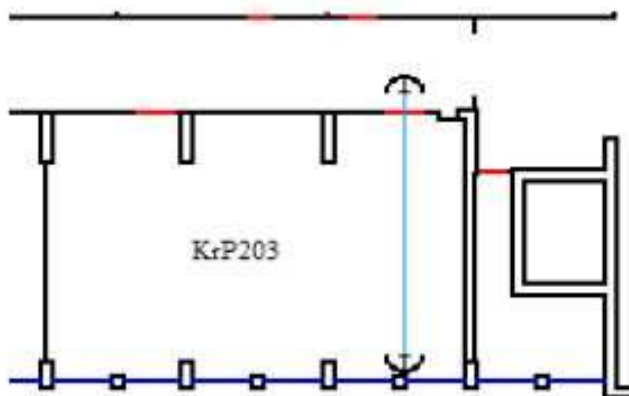
$$\begin{aligned} EIRP &= P_t + G_t - L_t \\ EIRP &= -1 + 14 - 4,1 \\ EIRP &= 9dBm \end{aligned}$$

kde P_t – výstupní výkon Wi-Fi karty [dBm], G_t – zisk vysílací antény [dBi], L_t – ztráty anténního svodu a konektorů na vysílací straně [dB]

- Jako druhé zařízení byla použita Wi-Fi karta Cisco AIR LMC350 nastavena na vysílací výkon 0dBm, ke které byla připojena směrová anténa Yagi XP se ziskem 16dBi. Mezi anténou a vysílačem byl 1 pigtail s útlumem 2dB, 3 konektory s útlumem 3dB a 3 metry koaxiálního kabelu s celkovým útlumem 1,47dB. Celkový vysílací výkon byl 9,5dBm. Výpočet vysílacího výkonu EIRP:

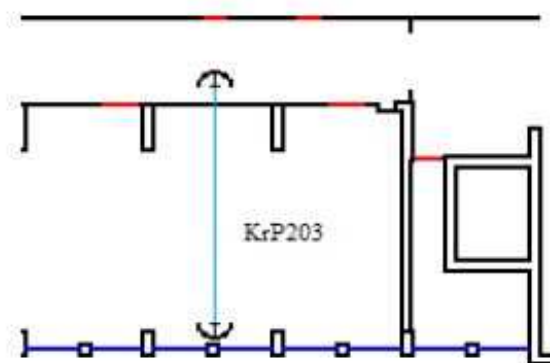
$$\begin{aligned} EIRP &= P_t + G_t - L_t \\ EIRP &= 0 + 16 - 5,5 \\ EIRP &= 9,5dBm \end{aligned}$$

U měření útlumu dveří byla jedna anténa umístěna naproti dveřnímu otvoru ve vzdálenosti 7 m a na chodbě 10 cm od vstupních dveří byla umístěna druhá anténa, dle (obr. 21). Nejdříve byla změřena úroveň signálu při otevřených dveřích a po té při zavřených dveřích. Pro minimalizaci chyb se toto měření se provedlo 5 krát. Naměřený útlum se na routeru pohyboval od 1 do 3dB a na Wi-Fi kartě byl naměřen útlum od 1 do 2dB. Proto byl útlum při simulaci v programu I-Prop zvolen 2dB. [10]



Obr. 21 – Rozmístění antén pro měření útlumu dveří

U měření útlumu cihlové zdi tloušťky 150mm byla nejprve změřena úroveň signálu ve dveřním otvoru, kdy jedna anténa byla umístěna naproti otvoru pro dveře ve vzdálenosti 7m a na chodbě 10cm od vstupních dveří byla umístěna druhá anténa (obr. 22). Pak byly antény přeneseny o stejnou vzdálenost do místa, kde překážku tvořila cihlová zeď. Takto proběhly čtyři měření bez překážky a s překážkou. Naměřený útlum se pohyboval v rozmezí od 5 do 7 dB. Proto byl útlum při simulaci v programu I-Prop zvolen 7dB. [10]



Obr. 22 – Rozmístění antén pro měření útlumu cihlové zdi 150mm

Měření pro železobetonový nosník 300mm a železobetonový strop 450mm zde uvádět nebudu, protože ve své simulaci nebudu tyto útlumy potřebovat.

5.3.1 Nastavení simulace v I-Prop

V simulačním programu jsem nejprve nakreslil schéma patra budovy. Program nabízí na výběr pouze čtyři druhy stěn (nelze přidat další), proto jsem zvolil tyto stavební materiály včetně definovaných útlumů:

<i>Stavební materiál</i>	<i>Útlum [dB]</i>
Vnější okna	12
Cihlové příčky 150mm	7
Vnitřní skleněné příčky	4
Dveřní výplň s voštinovou výplní	2

Tabulka 5: Nastavení parametrů pro simulaci

V místě šachet pro schodiště byl vyříznut otvor v podlaze, pro simulaci bylo zvoleno *Multi-Wall* modelování. [10] Tento model pro výpočet potřebuje přesné rozmístění jednotlivých příček na patrech s jejich útlumy a útlumy volného prostředí. Pro simulaci vícepatrových budov potřebuje také útlumy podlah. Tento model má dobrý poměr náročnosti na vstupy a složitosti na výpočet, ale není na rozdíl od *One-Slope modelu* [10] možnost simulovat vlnovodný efekt v dlouhých zahnutých chodbách. Celkové ztráty šíření jsou dány vztahem:

$$L_0 = 20 \cdot \log\left(\frac{4\pi d}{\lambda}\right) + \sum i k_{wi} L_{wi} + k_f \left(\frac{k_f + 2}{k_f + 1} - b\right)$$

L_0 – celkový útlum [dB]

D – vzdálenost [m]

λ - vlnová délka [m]

K_{wi} – počet příček, které promítají spojnicí mezi vysílačem a přijímačem

L_{wi} – činitel útlumu pro příčky [dB]

K_f – počet podlaží, které protínají spojnicí přijímač vysílač

L_f – činitel útlumu pro podlaží

b – konstanta nelinearity útlumu průchodem skrz více podlaží

Pro cihlové zdi tloušťky 150mm byl nastaven útlum na základě měření na hodnotu 7dB, pro dveřní výplň s voštinovou výplní 2dB. Pro vnější okna, která tvoří skelet budovy, byl

nastaven útlum 12dB, protože se jedná o tvrzené sklo potažené hliníkovou fólií. Pro vnitřní skleněné příčky byl zvolen útlum 4dB. Ostatní parametry, které program nabízí, zůstaly nastaveny v základním nastavení (obr 23).

Type	Attn.[dB]	Description
0.	7	Cihlove pricky 150mm
1.	12	Vnější okna
2.	2	Dvere
3.	4	Vnitřni slenene pricky 10mm

Loss at 1m [dB]: 38

Propagation index: 2

Offset [dB]: 0

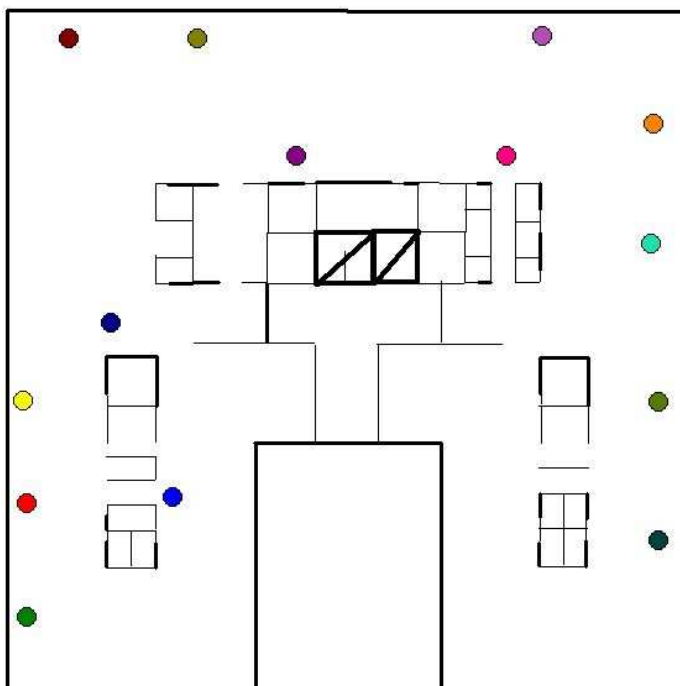
Adjacent floors loss [dB]: 18.3

Multi-floor param. 'b': 0.46

Obr. 23 – Nastavení parametrů pro simulaci

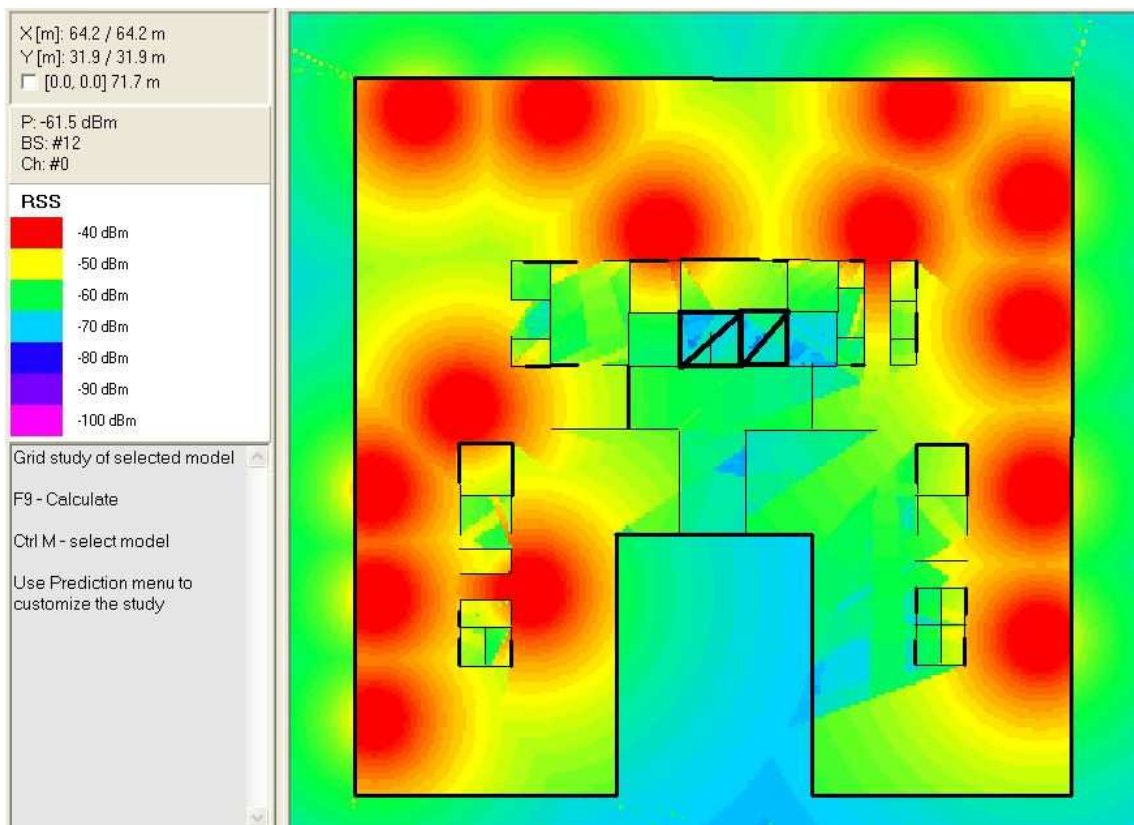
5.3.2 Rozmístění přístupových bodů a simulace

Přístupové body byly rozmístěny na místa podle skutečného stavu a to vždy ve výšce 2,5m, vysílací výkon EIRP byl nastaven na 6dB s frekvencí 2,412GHz a se všesměrovou anténou (obr 24).



Obr. 24 – Přehled rozmístění přístupových bodů – současný stav

Ve výsledcích simulace (obr. 25) je zřejmé malé pokrytí levé části pravé strany budovy, kde se nacházejí pracovní stoly pro zaměstnance. Úroveň signálu se zde pohybuje kolem 70dBm, což už je na hraně pro příjem signálu s méně kvalitními Wi-Fi kartami. V minulosti se v této části budovy nacházely samostatné místnosti se servery, proto při budování bezdrátové sítě nebylo do této části potřeba projektovat připojení. Druhým aspektem při budování bezdrátové sítě bylo bezproblémové pokrytí signálem quiet roomy, které se nacházejí ve střední části každé z částí patra. Z výsledků simulace je patrné, že všechny tyto prostory jsou signálem dostatečně pokryté. Všechny pracovní stoly jsou sice opatřeny UTP kabelem pro připojení k síti, pokud se ovšem zaměstnanec z důvodu meetingu pohybuje po celém patře, je lepší používat bezdrátové připojení.



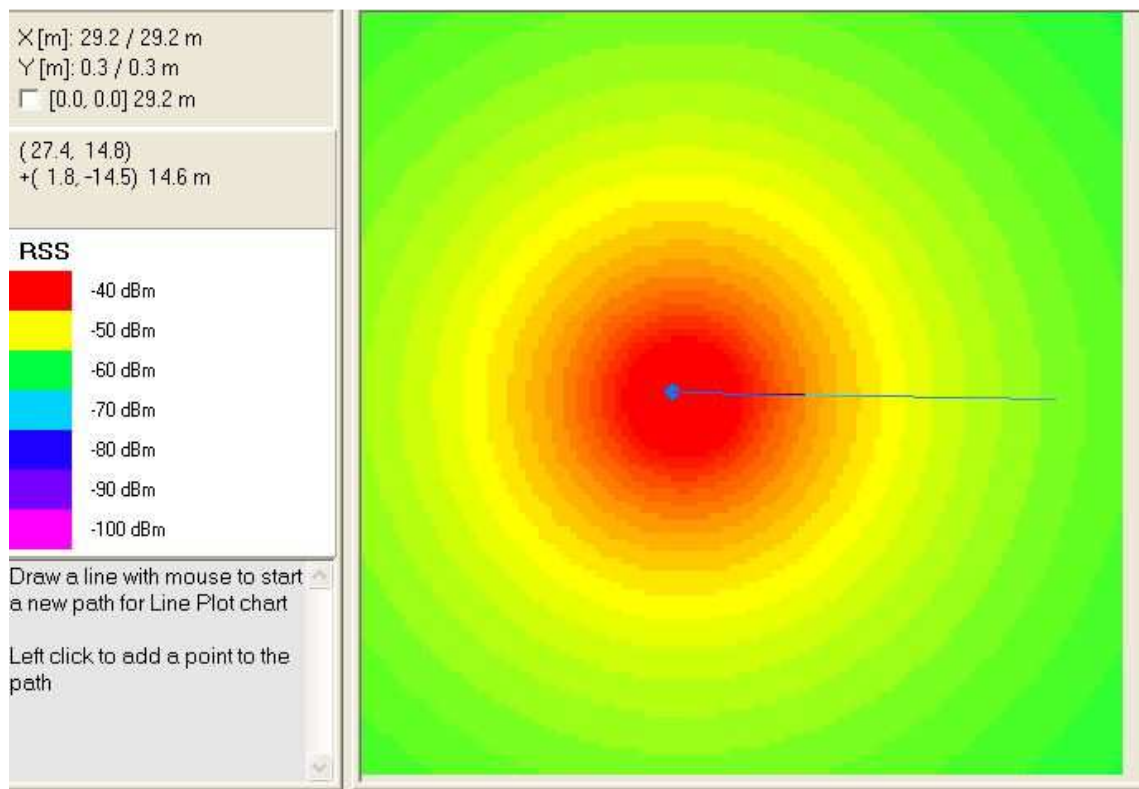
Obr. 25 – Úroveň signálu v jednotlivých částech patra

5.4. Optimalizace rozmístění směrovacích stanic v bezdrátových sítích

Celá praktická část byla prováděna v prostředí Wolfram Mathematica 9.0. Pro zpracování algoritmu bylo důležité, aby byla oddělena část, ve které se provádí ohodnocení účelové funkce od části, která provádí vlastní algoritmus.

5.4.1 Účelová funkce

Na účelovou funkci je možné nahlížet jako na geometrický problém, v jehož rámci se hledá nejnižší (minimum) či nejvyšší (maximum) pozice na ploše ležící v $N+1$ rozměrném prostoru. Při řešení mého úkolu – navrhnout počet AP v budově, jsem vycházel z poznatku, že vzdálenost přípojného zařízení a Access Pointu by neměla přesáhnout 15m. Útlum v této vzdálenosti je cca 60dB (obr. 26).



Obr. 26 – Úroveň útlumu signálu ve vzdálenosti 15m

V účelové funkci jsem ovšem nastavil poloměr dosahu signálu na 10m. Dále jsem musel matematicky vyřešit problematiku, kdy signál procházel okrajem budovy, tzn. tuto přechýlující plochu odečíst od celkového obsahu budovy.

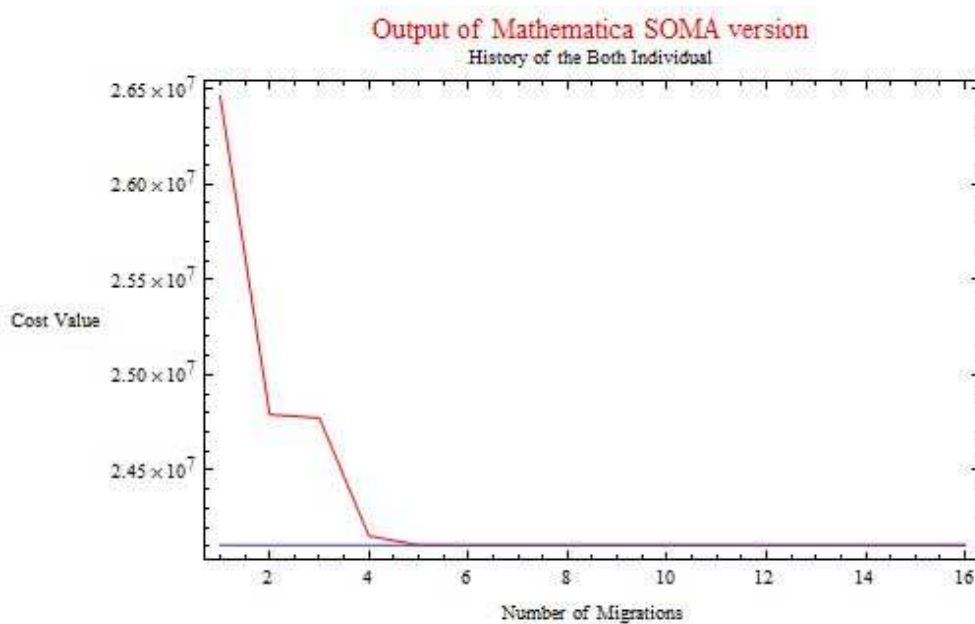
5.4.2 Testovací část

Pro celé testování jsem použil stejné následující nastavení parametrů pro algoritmy SOMA a DE:

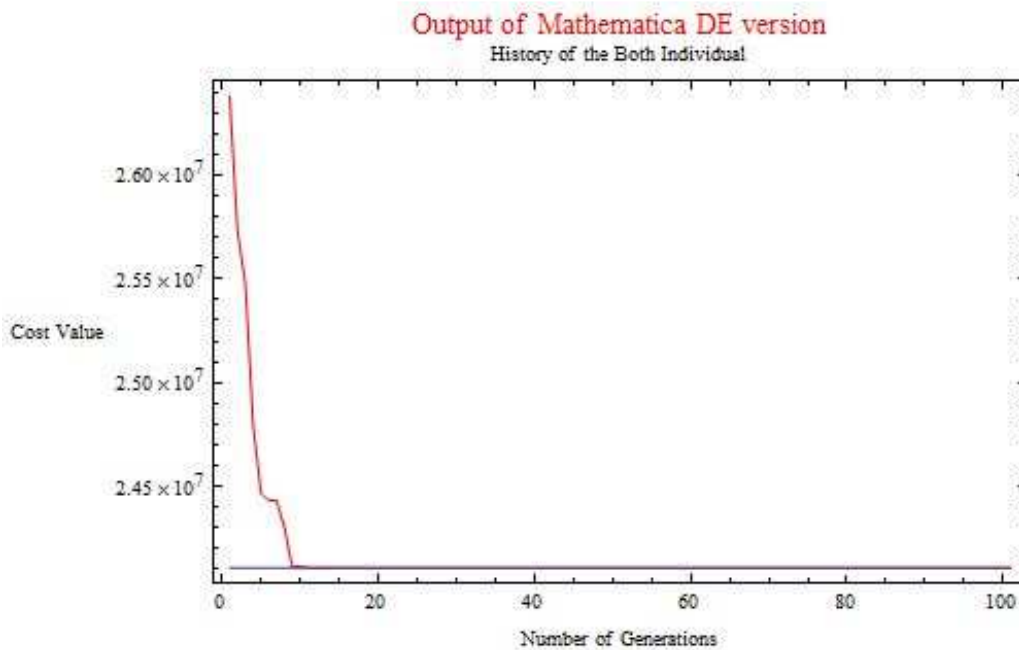
<i>Algoritmus SOMA</i>		<i>Algoritmus DE</i>	
<i>Parametr</i>	<i>Hodnota</i>	<i>Parametr</i>	<i>Hodnota</i>
PopSize	20	NP	20
Migrations	15	Generations	100
Step	0,11	F	0,8
PathLength	3	Cr	0,8
PRT	0,1		
MinDiv	-1		

Tabulka 6: Nastavení parametrů algoritmu SOMA a DE

Pro testování je také vhodné vytvořit graf z historie algoritmu, jak se vyvíjelo umístění nejlepšího jedince. Celý proces se mnohokrát zopakuje a všechny historie se vkládají do jednoho grafu. V grafu potom můžeme vidět, od kterého evolučního cyklu se všechny opakování ustálily na extrému funkce.



Obr. 27 – Histogram algoritmu SOMA



Obr. 28 – Histogram algoritmu DE

Na obrázcích 27 a 28 vidíme porovnání dvou řešení, kde červená čára znázorňuje nejpomalejší postup při hledání extrému a modrá čára nejrychlejší postup při hledání extrému. U obou algoritmů shodně vidíme, že nejpomalejší běh algoritmu začínal na hodnotě $2,65 \times 10^7$ a ke globálnímu extrému se u algoritmu SOMA dostal po 5ti a algoritmus DE po 10ti evolučních kolech. Algoritmy shodně našly extrém pro leadere již na začátku.

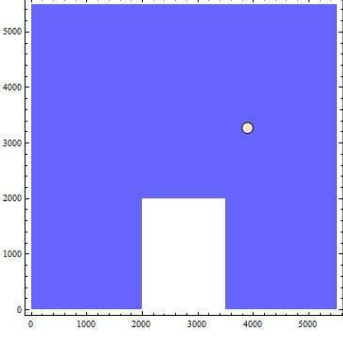
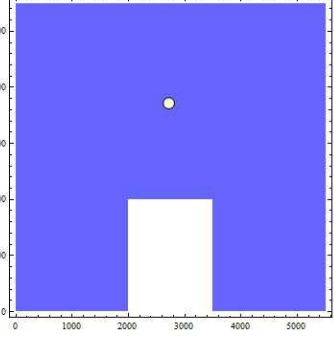
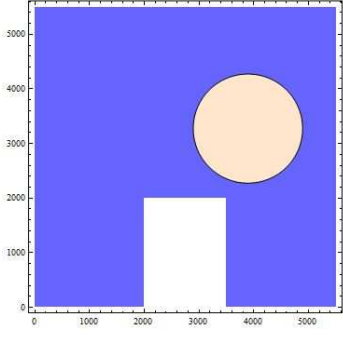
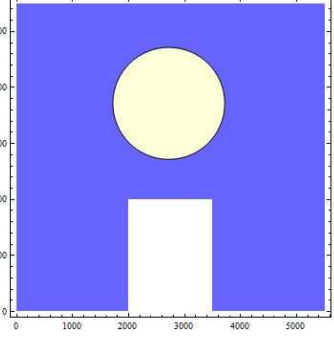
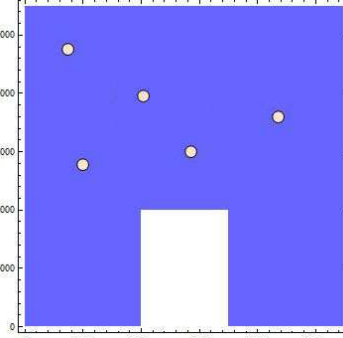
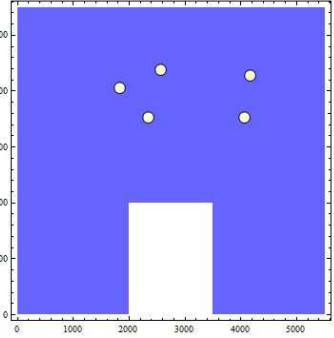
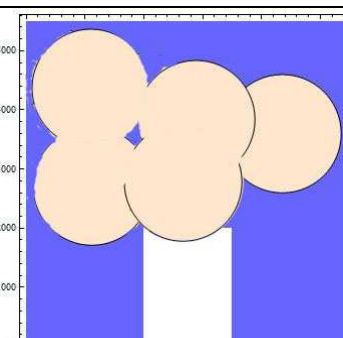
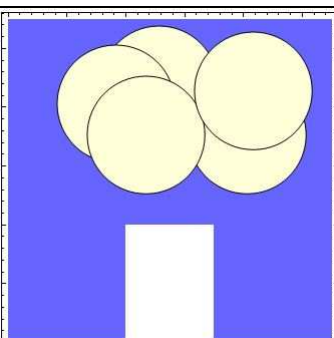
Další veličinou, kterou zjišťujeme při testování, je čas. Potřebujeme, aby algoritmus byl co nejrychlejší při hledání globálního extrému. Délku trvání algoritmu ovlivňují všechny počáteční podmínky, jako je dimenze a složitost účelové funkce, nastavení řídicích a ukončovacích parametrů algoritmu. Porovnání časové náročnosti algoritmu SOMA a DE pro hledání optimálního rozmístění AP nejlépe zobrazuje následující tabulka:

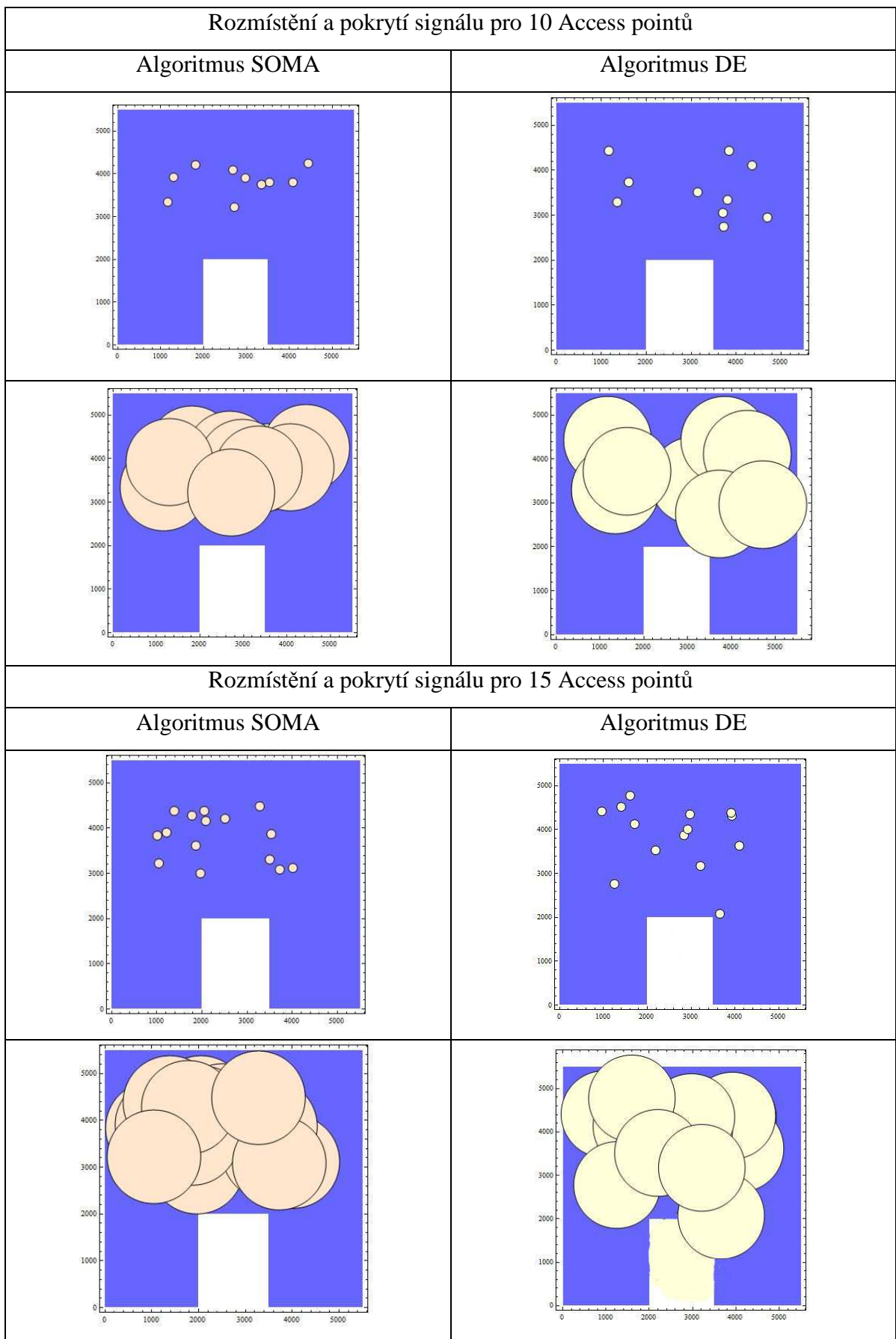
<i>Algoritmus SOMA</i>		<i>Algoritmus DE</i>	
<i>Počet AP</i>	<i>Čas</i>	<i>Počet AP</i>	<i>Čas</i>
1	52 sec	1	19 sec
5	3 min 7 sec	5	1 min 15 sec
10	11 min 19 sec	10	2 min 48 sec
15	25 min 48 sec	15	4 min 12 sec
20	33 min 43 sec	20	5 min, 38 sec
25	47 min 31 sec	25	6 min 51 sec
30	1 hod 2 min 29 sec	30	10 min 5 sec

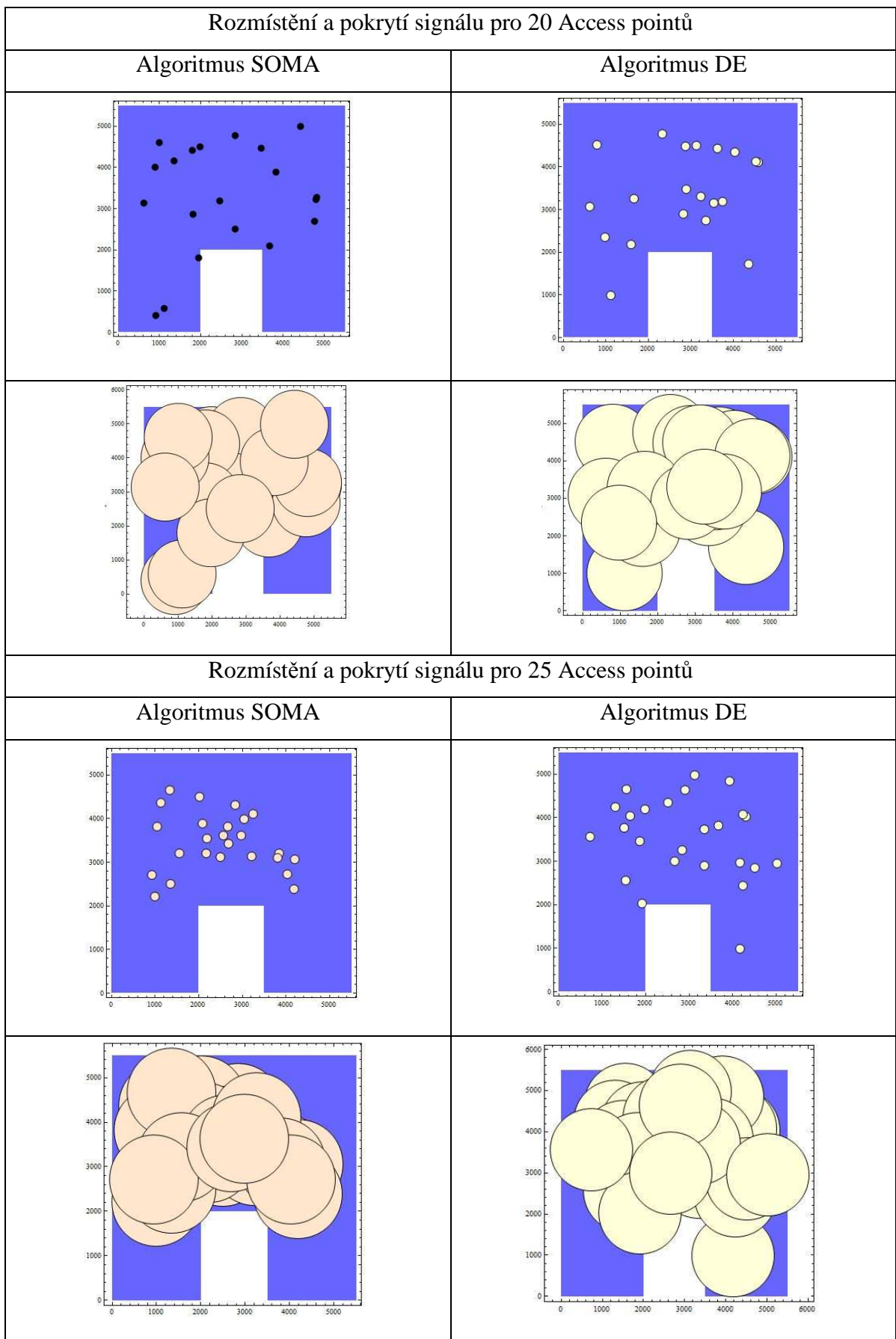
Tabulka 7: Porovnání časové náročnosti algoritmů SOMA a DE

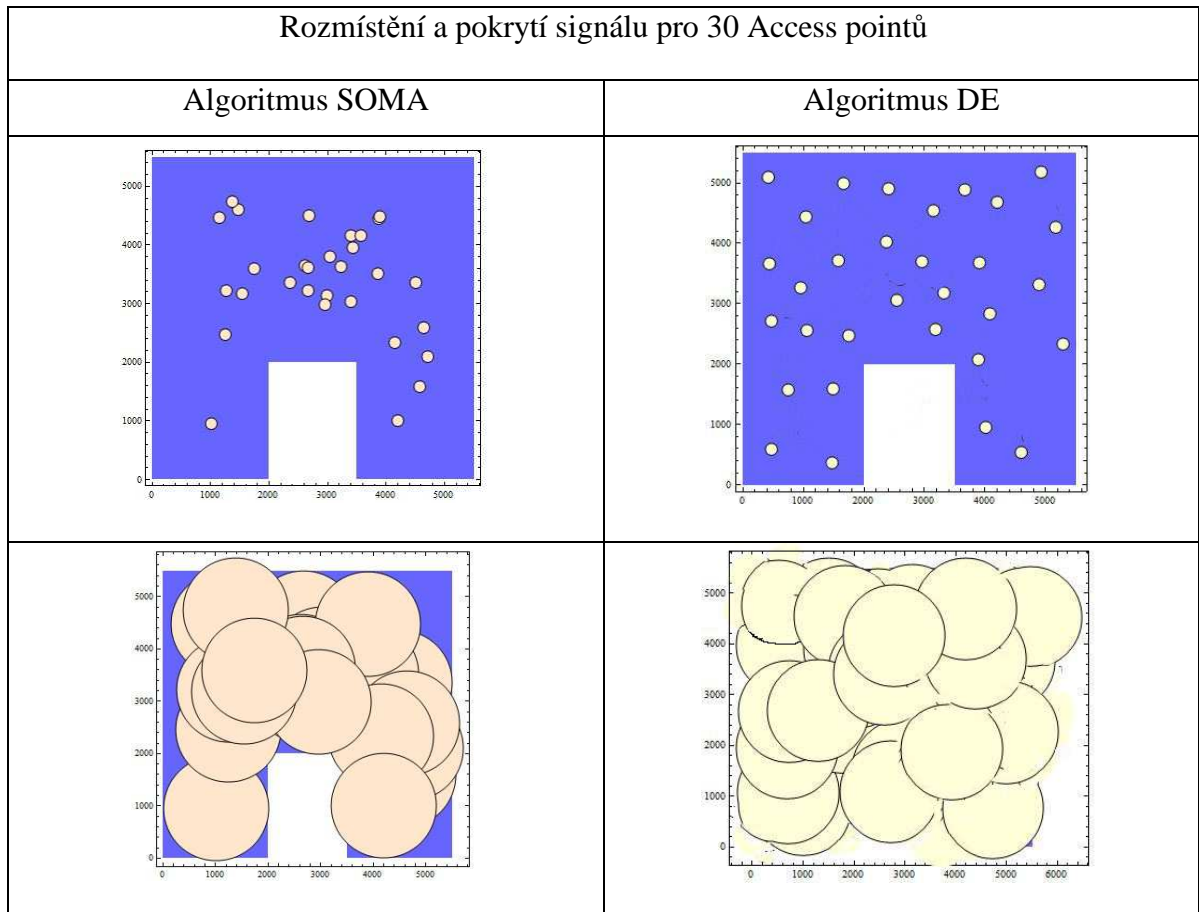
Mohu tedy konstatovat, že algoritmus Diferenciální evoluce je průměrně 6x rychlejší, než algoritmus SOMA.

Na následujících obrázcích je vidět rozmístění AP pro přesně daný počet AP (1, 5, 10, 15, 20, 25 a 30) při použití algoritmů SOMA a DE. Z obrázků je dále patrné, že při navolení rozložení 30 AP je budova dostatečně pokryta bezdrátovým signálem. Pomocí programu I-Prop jsem si toto tvrzení ověřil a zjistil jsem, že útlum signálu v administrativní části budovy byl maximálně 50dB. Jen v technických místnostech je útlum signálu do 60dB, ale tyto místnosti nejsou primárně určeny pro připojení na Wi-Fi síť. Z jednotlivých obrázků je také patrné, že oba algoritmy umisťovaly AP na podobná místa, ovšem algoritmus DE byl jednoznačně rychlejší.

Rozmístění a pokrytí signálu pro 1 Access point	
Algoritmus SOMA	Algoritmus DE
 <p>A 5000x5000 coordinate system with a white rectangular obstacle at the bottom center (approx. x=2000-3500, y=0-2000). A single small white dot representing an access point is located at approximately (3800, 3300).</p>	 <p>A 5000x5000 coordinate system with a white rectangular obstacle at the bottom center. A single small white dot representing an access point is located at approximately (2800, 3700).</p>
 <p>The same 5000x5000 coordinate system with the obstacle. A large orange circle representing the coverage area of the access point is centered at approximately (3800, 3300).</p>	 <p>The same 5000x5000 coordinate system with the obstacle. A large yellow circle representing the coverage area of the access point is centered at approximately (2800, 3700).</p>
Rozmístění a pokrytí signálu pro 5 Access pointů	
Algoritmus SOMA	Algoritmus DE
 <p>A 5000x5000 coordinate system with the obstacle. Five small white dots representing access points are scattered in the upper half of the area.</p>	 <p>A 5000x5000 coordinate system with the obstacle. Five small white dots representing access points are scattered in the upper half of the area, in a different configuration from the SOMA algorithm.</p>
 <p>The same 5000x5000 coordinate system with the obstacle. Five overlapping orange circles represent the coverage areas of the five access points.</p>	 <p>The same 5000x5000 coordinate system with the obstacle. Five overlapping yellow circles represent the coverage areas of the five access points.</p>







Tabulka 8: Rozmístění a pokrytí Wi-Fi signálu na základě algoritmu SOMA a DE



Obr. 29 – Výsledná úroveň signálu v jednotlivých částech patra

6. ZÁVĚR

Tato diplomová práce se zabývala optimálním rozmístěním Access Pointů v administrativní budově. V programu I-Prop byl nasimulován současný stav, při kterém jsem zjistil, že jsou v budově místa s útlumem signálu až 70dB, což pro pracovní stanice s méně výkonnou Wi-Fi kartou může představovat výpadky v připojení. Pro porovnání jsem zvolil dva evoluční algoritmy – SOMA a Diferenciální evoluci. Tyto algoritmy jsem získal od vedoucí mé práce. V nich byla v programu Mathematica naprogramovaná programová část. Mým úkolem bylo vytvořit účelovou funkci. Testováním jsem zjistil, že dosavadní počet 16 AP v budově je pro kvalitní příjem signálu nedostačující. Podle evolučních algoritmů by měl být optimální počet Access Pointů roven číslu 30. V takovém případě je útlum signálu v administrativní části budovy maximálně 50dB. Při umístění menšího počtu AP v budově než navrhovaného počtu 30, dojde ke zvýšení útlumu, což sice nemusí vést k technickým problémům, ale pro zajištění stabilního připojení může být nedostatečné.

Práci je v budoucnu možné rozšířit o problematiku optimalizace Access Pointů. U dosavadního způsobu se musí manuálně zkoušet počet AP, než signálem pokryjí celý prostor.

7. SEZNAM POUŽITÉ LITERATURY

- [1] ZELINKA, Ivan ... [et al.] *Evoluční výpočetní techniky: principy a aplikace*. 1. české vyd. Praha: BEN, 2009, 534 s. ISBN 978-80-7300-218-3.
- [2] ZELINKA, Ivan. *Umělá inteligence I: Neuronové sítě a genetické algoritmy*. 1. vyd. Brno: VUT v Brně, 1998, 126 s. ISBN 80-214-1163-5.
- [3] ŠNOREK, Miroslav. *Neuronové sítě a neuropočítače*. Vyd. 1. Praha: ČVUT, 1996, 124 s. ISBN 80-010-1455-X.
- [4] MAŘÍK, Vladimír. *Umělá intelligence I.díl*. Praha: Academia, 2000, 264 s. ISBN 80-200-0496-3.
- [5] BÍLA, Jiří. *Umělá inteligence a neuronové sítě v aplikacích*. Vyd. 1. Praha: Vydavatelství ČVUT, 1995, 115 s. ISBN 80-010-1275-1.
- [6] PECHAČ, Pavel. *Šíření vln v zástavbě*. Praha: BEN - technická literatura, 2005, 108 s. ISBN 80-730-0186-1.
- [7] DAVIS, Harold. *Průvodce úplného začátečníka pro Wi-Fi bezdrátové sítě: není zapotřebí žádných předchozích zkušeností!*. 1. vyd. Praha: Grada, 2006, 334 s. Průvodce (Grada). ISBN 80-247-1421-3.
- [8] HORÁK, Jaroslav. *Vytváříme domácí bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2011, 293 s. ISBN 978-80-251-2977-7.
- [9] SOSINSKY, Barrie A. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-80-251-3363-7.
- [10] LÁTAL, Jan ... [et al.]. *Simulace a plánování vnitřního pokrytí budov dle standardu IEEE 802.11 v prostředí ssoftwarové aplikace I-Prop -1 část*. Praha, 2011.
- [11] TRČÁLEK, Antonín. Gigabit vzduchem. *Computer*. 2012, č. 12, s. 2.
- [12] SCHMIDT, Christoph a Patrik KHUDHUR. Stavíme stometrovou síť bez drátů. *Chip*. 2012, č. 10, s. 2.
- [13] Počítačové sítě - Model ISO/OSI. *Site.the.cz* [online]. 2010 [cit. 2014-05-18]. Dostupné z: <http://site.the.cz/index.php?id=4%20http://www.samuraj-cz.com/clanek/osi-model/>

8. SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
AP	Access Point
BSA	Basic Service Area
BSS	Basic Service Set
CRC	Cyclic Redundancy Chec
DE	Diferenciální evoluce
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSSS	Direct sequence spread spectrum
EIRP	Equivalent Isotropically Radiated Power
ESS	Extend Service Set
FHSS	Frequency hopping spread spectrum
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, scientific and medical
ISO	International Standards Organization
MAC	Media Access Control
MIC	Message Integrity Code
MIMO	Multiple Input Multiple Output
MU-MIMO	Multi User - Multiple Input Multiple Output
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection Basic Reference Model
PSK	Pre-shared key
RADIUS	Remote Authentication Dial In User Service
TKIP	Temporal Key Integrity Protocol

9. SEZNAM OBRÁZKŮ

Obrázek 1 - Hedy Lamarr	11
Obrázek 2 - George Antheil	11
Obrázek 3 - Beamformin	14
Obrázek 4 – Netgear R6300	15
Obrázek 5 – Komponenty sítě 802.11	16
Obrázek 6 – BSS, BSA	17
Obrázek 7 – Ad-hoc síť	18
Obrázek 8 – Infrastrukturní síť	18
Obrázek 9 – Rozšířená oblast služeb (ESS)	19
Obrázek 10 – OSI a TCP/IP model	20
Obrázek 11 – MAC rámeček	23
Obrázek 12 – Rozprostření kanálů v ISM pásmu 2,4 GHz	24
Obrázek 13 – Funkce PRT	31
Obrázek 14 – Konvergence populace do globálního extrému na funkci při NP=20, F=0,5, CR=1,0	35
Obrázek 15 – Celkový pohled na budovu	37
Obrázek 16 – Interiér budovy	37
Obrázek 17 – Vícecestné šíření signálu	38
Obrázek 18 – Ukázka práce v programu I-Prop	40
Obrázek 19 – Ukázka práce v programu Ekahau Site Survey	41
Obrázek 20 – Výsledek měření síly signálu v prostorách firmy	42
Obrázek 21 – Rozmístění antén pro měření útlumu dveří	44
Obrázek 22 – Rozmístění antén pro měření útlumu cihlové zdi 150mm	44
Obrázek 23 – Nastavení parametrů pro simulaci	46
Obrázek 24 – Přehled rozmístění přístupových bodů – současný stav	46

Obrázek 25 – Úroveň signálu v jednotlivých částech patra	47
Obrázek 26 – Úroveň útlumu signálu ve vzdálenosti 15m.....	48
Obrázek 27 – Histogram algoritmu SOMA.....	49
Obrázek 28 – Histogram algoritmu DE.....	50
Obrázek 29 – Výsledná úroveň signálu v jednotlivých částech patra	55

10. SEZNAM TABULEK

Tabulka 1 - Přenosová rychlost 802.11n v závislosti na počtu antén	13
Tabulka 2 - Parametry algoritmu SOMA	29
Tabulka 3 - Parametry Diferenciální evoluce	33
Tabulka 4 - Porovnání programů I-Prop a Ekaheu zatím	41
Tabulka 5 - Nastavení parametrů pro simulaci	45
Tabulka 6 - Nastavení parametrů algoritmu SOMA a DE.....	49
Tabulka 7 - Porovnání časové náročnosti algoritmů SOMA a DE	51
Tabulka 8 - Rozmístění a pokrytí Wi-Fi signálu na základě algoritmu SOMA a DE	52-55

11. SEZNAM PŘÍLOH

Příloha P1 - CD obsahující vlastní práci a zdrojové kódy.....	63
---	----

Příloha P1 - CD obsahující vlastní práci a zdrojové kódy