

Česká zemědělská univerzita v Praze

Technická fakulta



**Monitoring pohybu osob v uzavřeném objektu  
pomocí Wi-Fi technologie**

diplomová práce

Vedoucí diplomové práce:

Ing. Zdeněk Votruba, Ph.D.

Autor:

Bc. Martin Olmr

PRAHA 2017

## ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Martin Olmr

Informační a řídicí technika v agropotravinářském komplexu

Název práce

**Monitoring pohybu osob v uzavřeném objektu pomocí WiFi technologie**

Název anglicky

**Monitoring the movement of people in an enclosed building via WiFi technology**

---

### Cíle práce

Cílem práce je návrh technologie a její praktické ověření pro on-line monitoring osob v uzavřených objektech (nemocnice, LDN,...). Technologie bude postavena na WiFi triangulaci a vyhodnocována vlastním navrženým prostředkem. V praktické části bude ověřena spolehlivost, přesnost a ekonomické srovnání s alternativními technologiemi.

### Metodika

1. Literární rešerše
2. Popis stávajících řešení používaných ve světě
3. Popis navržené technologie včetně diskuse
4. Metodika triangulace a koncepce řešení
5. Praktické řešení včetně základních testů
6. Ověření v poloprovozních podmínkách
7. Vyhodnocení a doporučení pro další výzkum/provoz

## **Doporučený rozsah práce**

50 – 60 stran textu včetně příloh

## **Klíčová slova**

WiFi, monitoring pohybu, asistivita, bezpečnost, programování

---

## **Doporučené zdroje informací**

Dufková, J.: Sociologie životního stylu, BEN, 2010, 978-80-7380-123-6  
Gaddi: eHealth, Care and Quality of Life, 2013, Springer, 8847052521  
Mach, J.: Lékař a právo, GRADA, 2010, 978-80-247-3683-9  
Pecháč, P.: Šíření vln v zástavbě, BEN, 2006, 80-7300-186-1  
Procházka, M.: Antény – encyklopedická příručka, BEN, 205, 80-7300-166-7  
Zandl, P.: Bezdrátové sítě WiFi, Computer Press, 2003, 80-7226-632-2

---

## **Předběžný termín obhajoby**

2016/17 LS – TF

## **Vedoucí práce**

Ing. Zdeněk Votruba, Ph.D.

## **Garantující pracoviště**

Katedra technologických zařízení staveb

Elektronicky schváleno dne 3. 2. 2016

**doc. Ing. Jan Malaťák, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 2. 3. 2016

**prof. Ing. Vladimír Jurča, CSc.**

Děkan

V Praze dne 05. 03. 2017

## Čestné prohlášení

*Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením Ing. Zdeňka Votruby, Ph.D. a uvedl v seznamu všechny použité literární a odborné zdroje.*

*Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů a to i bez ohledu na výsledek obhajoby.*

*Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.*

*Jsem si vědom, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.*

V Praze dne .....

.....  
Bc. Martin Olmr

## Poděkování

*Tímto bych chtěl poděkovat vedoucímu mé práce Ing. Zdeňku Votrubovi, Ph.D. za cenné rady a věcné připomínky při jejím zpracování.*

**Abstrakt:** Cílem práce je návrh technologie a její praktické ověření pro on-line monitoring osob v uzavřených objektech (nemocnice, LDN). Technologie bude postavena na Wi-Fi triangulaci a vyhodnocována vlastním navrženým prostředkem. V praktické části bude ověřena spolehlivost, přesnost a ekonomické srovnání s alternativními technologiemi.

**Klíčová slova:** Wi-Fi, monitoring pohybu, asistivita, bezpečnost, programování

## **Monitoring the movement of people in an enclosed building via Wi-Fi technology**

**Abstract:** The aim of this work is to design technology and its practical verification for online monitoring of people in closed buildings (hospitals, hospices). The technology will be based on Wi-Fi triangulation and an evaluated self-designed device. The practical part will verify the reliability, accuracy and economic comparison with alternative technologies.

**Keywords:** Wi-Fi, motion tracking, assistance, security, programming

# Obsah

1	Úvod .....	1
2	Cíl práce .....	2
3	Metodika práce .....	3
4	Bezdrátový přenos.....	5
4.1	Princip elektromagnetického pole.....	5
4.2	Maxwellovy rovnice .....	6
4.2.1	I. Maxwellova rovnice .....	6
4.2.2	II. Maxwellova rovnice .....	6
4.2.3	III. Maxwellova rovnice .....	7
4.2.4	IV. Maxwellova rovnice .....	7
4.3	Elektromagnetické vlnění .....	8
4.3.1	Vlnová délka .....	8
4.3.2	Amplituda.....	9
4.3.3	Frekvence .....	10
4.4	Frekvence a jejich rozdělení.....	11
4.5	Vysílání a příjem signálu.....	12
4.5.1	Vysílání přenosového signálu.....	13
4.5.2	Příjem přenosového signálu.....	13
4.6	Antény.....	14
4.6.1	Základní vlastnosti antén .....	14
4.6.2	Základní typy konstrukce antén .....	16
4.7	Rušení signálu .....	18
5	Technologie Wi-Fi.....	20
5.1	Protokoly standardu IEEE 802.11.....	20
5.2	Zařízení sítě Wi-Fi.....	21
5.2.1	Access Point.....	21
5.2.2	Repeater .....	21
5.2.3	Klient .....	21
5.3	Zabezpečení .....	22

5.3.1	WEP .....	22
5.3.2	WPA, WPA 2 .....	22
5.3.3	Protokol IEEE 802.1X .....	22
5.3.4	Filtrování MAC adres .....	23
5.3.5	Vypnutí vysílání SSID .....	23
5.4	Rušení signálu Wi-Fi .....	23
6	Triangulace .....	25
6.1	Proximity .....	25
6.2	Trilaterace .....	26
6.3	Analýza prostoru .....	27
6.4	Indikace síly signálu.....	27
6.5	Doba přenosu.....	27
6.6	Časový rozdíl přenosu .....	27
6.7	Směrové antény .....	27
6.8	Překrytí signálů.....	28
6.9	Aproximace bodu v trojúhelníku .....	29
7	Stávající řešení používané ve světě .....	30
7.1	Accuware.....	30
7.2	Ekahau.....	32
7.3	Infsoft .....	32
7.4	Mapspeople .....	33
8	Koncepce řešení .....	34
9	Praktické řešení .....	36
9.1	Návrh a sestavení hardware .....	36
9.1.1	Programovatelné Wi-Fi moduly .....	36
9.1.2	Potřebné komponenty pro zprovoznění modulu .....	40
9.1.3	Sestavení komponent.....	41
9.1.4	Programování Wi-Fi modulu .....	43
9.1.5	Testování funkčnosti .....	47
9.2	Vytvoření software.....	53
9.2.1	Návrh software.....	54
9.2.2	Programování software.....	55



9.2.3	Mapa síly signálu a algoritmus určování polohy klienta .....	64
9.3	Základní testy .....	68
9.3.1	Test komunikace Server – Klient .....	68
9.3.2	Test výpočtu map signálu .....	69
9.3.3	Test určování polohy klienta .....	71
10	Ověření v poloprovozních podmínkách .....	74
10.1	Porovnání výsledků s již dostupnými technologiemi .....	80
10.2	Ekonomické vyhodnocení .....	81
11	Závěr .....	82
12	Závěrečná doporučení .....	84
	Seznam zdrojů .....	85
	Seznam obrázků .....	87
	Seznam tabulek .....	88
	Seznam rovnic .....	89
	Seznam grafů .....	89
	Seznam příloh .....	89

## Seznam použitých zkratk

AES	Advanced encryption standard, šifrování přístupu do Wi-Fi sítě
AP	Access Point
ČTÚ	Český telekomunikační úřad
DVB-T	Digitální pozemní televizní vysílání
ID	Identifikátor
LAN	Local area network
MAC	Media Access Control
PAN	Personal area network
PSK	Pre-shared key, modulace s fázovým klíčováním, autentizace do sítě Wi-Fi
SSID	Service Set Identifier
WAN	World area network
WEP	Wired Equivalent Privacy, zabezpečení sítě Wi-Fi
Wi-Fi	Bezdrátová počítačová síť
WPA	Wi-Fi protected access, zabezpečení sítě Wi-Fi
WPF	Windows Presentation Foundation

# 1 Úvod

Nejen rádia, televize, telefony, počítače, ale i některé automobily, ledničky, pračky a spousta dalších dnes již běžně používaných věcí využívá bezdrátových přenosů dat.

V úplných počátcích za dob Heinricha Rudolfa Hertze či Guglielmo Marconiho jsme využívali analogového bezdrátového přenosu pomocí rádiových vln. Nejdříve se zvonilo zvonkem na druhé straně místnosti, poté se telegrafovalo přes Atlantický oceán a postupným zdokonalováním bezdrátových přenosů jsme se dostali až do dnešní doby digitalizace a bezdrátových přenosů.

Pokud se zaměříme na digitální bezdrátové počítačové sítě, určitě nám neunikne technologie Wi-Fi. Je to nejpoužívanější technologie pro bezdrátovou počítačovou síť a na její signál narazíme na každém rohu.

Pomocí Wi-Fi přistupujeme z našich počítačů a mobilních telefonů na internet, tedy využíváme ji k přenosu dat. To je samozřejmě správně, tato technologie je k tomu určena, ale můžeme ji využít i k jiným potřebám. Například odborníci z Massachusetts Institute of Technology (MIT) pomocí narušení Wi-Fi signálu detekují pohyb až 8 osob v prostoru najednou.

Pomocí Wi-Fi signálu lze také určovat polohu objektu v otevřeném a uzavřeném prostoru. Právě návržení vlastní technologie určování polohy v uzavřeném prostoru pomocí Wi-Fi signálu a její otestování v poloprovozních podmínkách je náplní této diplomové práce.

## 2 Cíl práce

Hlavním cílem této diplomové práce je návrh technologie monitorující pohyb osob v uzavřeném prostoru pomocí signálu Wi-Fi. Navržená technologie bude následně otestována v poloprovozních podmínkách. Dílčími cíli této práce pak je:

- vytvořit přehled řešené problematiky,
- provést návrh technologie,
- zkonstruovat hardware z dostupných komponentů,
- naprogramovat počítačovou aplikaci pro monitorování pohybu klienta na základě navržené technologie určování polohy,
- otestovat výslednou technologii v poloprovozních podmínkách,
- zhodnotit funkčnost, přesnost a použitelnost technologie.

### 3 Metodika práce

Teoretická část se zaměří na bezdrátové přenosy z pohledu fyzikálních vlastností, čímž bude navázáno na mou bakalářskou práci Analýza bezdrátových přenosů pro datovou komunikaci z pohledu fyzikálních vlastností. Bude zmíněn způsob využití frekvenčních pásem a regulace Českým telekomunikačním úřadem. Detailně bude popsána technologie Wi-Fi, včetně zabezpečení a rušení signálu. Dále se práce zaměří na triangulaci a početní metody pro výpočet polohy bodu v prostoru. Na závěr teoretické části se seznámí s aktuálně dostupnými technologiemi pro určování polohy pomocí Wi-Fi a uvede jejich výhody a nevýhody. Při psaní teoretické části bude čerpáno z nastudované odborné literatury a využito již dosažených znalostí získaných při psaní bakalářské práce v této oblasti.

V praktické části se navrhne a sestaví hardware, jenž bude monitorovat sílu signálu dostupných Access Pointů v okolí a tyto informace prostřednictvím Wi-Fi sítě odesílat na monitorovací stanici. Při navrhování hardware se bude využívat komponentů dostupných pro vývojovou desku Arduino, přičemž bude rozhodnuto mezi použitím Wi-Fi modulu Wifi Shield V2.2 a ESP 8266. Sestavený hardware bude napájen pomocí baterií a sestaven v co nejmenších rozměrech.

Se sestaveným hardwarem se provedou základní testy. Cílem těchto testů bude prověřit vlastnosti Wi-Fi signálu, především pak vliv rušení konstrukčními prvky stavby a osobami na tento signál. Na základě získaných dat bude vytvořen algoritmus pro určování polohy klienta (vytvořeného hardware). Tento algoritmus bude součástí WPF (Windows Presentation Foundation) aplikace vytvořené v jazyce C# pro operační systém Windows. Ta bude s klientem komunikovat pomocí TCP/IP (IPv4) protokolu, přičemž TCP/IP server bude umístěn ve vytvořené aplikaci a bude umožňovat připojení až 16 klientů zároveň. Součástí aplikace bude uživatelské rozhraní, jež bude zobrazovat seznam připojených klientů, mapu monitorovaného prostoru a aktuální určenou polohu jednotlivých klientů.

Navržený algoritmus, vytvořenou aplikaci a zkonstruovaný hardware, bude podroben testování v testovacím bytě. Cílem tohoto testování bude upravovat algoritmus tak, aby bylo dosaženo co nejpřesnějšího určování polohy klienta a vytvořená technologie byla připravena k dalšímu testování v poloprovozních podmínkách.

Pro otestování technologie budou k dispozici prostory Technické fakulty České zemědělské univerzity v Praze, konkrétně místnosti 218/I, 219/I, 220/I a chodba. Katedrou technologických zařízení staveb bude zapůjčeno pět Access Pointů TP-link TL-WA701ND, jež poslouží k pokrytí monitorovaného prostoru Wi-Fi signálem. Do těchto prostor bude aplikována vytvořená technologie a budou zde vytvořeny poloprovozní podmínky. Následně bude provedeno důkladné testování určování polohy v klíčových místech monitorovaného prostoru. Na základě získaných dat se určí přesnost, spolehlivost a slabiny vytvořené technologie.

Na závěr se provede porovnání vlastností navržené technologie s již existujícími technologiemi, finanční analýza navržené technologie a stanovena závěrečná doporučení.

## 4 Bezdrátový přenos

Bezdrátová datová komunikace může probíhat prostřednictvím ultrazvuku, optiky nebo elektromagnetických vln. Technologie Wi-Fi využívá elektromagnetických vln v pásmu mikrovln. Proto se tato diplomová práce zaměřuje pouze na přenos prostřednictvím elektromagnetického vlnění. [1] [2]

### 4.1 Princip elektromagnetického pole

Kolem elektrických vodičů, jimiž protéká elektrický proud, vzniká magnetické pole. Rozlišujeme pole stacionární a nestacionární. [2]

Stacionární magnetické pole se ve všech místech prostoru, v němž se nachází, s časem nemění. Je nejčastěji tvořeno permanentními magnety nebo nepohybujícími se vodiči, kterými prochází konstantní elektrický proud. Nestacionární magnetické pole je naopak proměnlivé v čase. To vzniká pohybujícím se vodičem nebo vodičem s časově proměnným elektrickým proudem. [2]

Elektrické pole je prostor, ve kterém působí elektrické síly. Pro vznik elektrického pole je zapotřebí elektrického náboje nebo časově proměnného magnetického pole. [2]

Časové změny elektrického pole vyvolávají vznik magnetického pole a naopak časově proměnné magnetické pole vyvolává vznik elektrického pole. Takové pole nazýváme proměnné elektromagnetické pole. [2]

## 4.2 Maxwellovy rovnice

J. C. Maxwell předpověděl a matematicky popsal vztah mezi elektřinou a magnetizmem. Svými výpočty předpověděl existenci elektromagnetického vlnění. [1] [2]

### 4.2.1 I. Maxwellova rovnice

První rovnice nám říká, že zdrojem vírového magnetického pole je vodivý elektrický proud nebo časově proměnné elektrické pole. [1] [2]

#### **Integrální tvar**

$$\oint_{C(S)} \mathbf{H} \cdot d\mathbf{l} = \iint_S \left( \mathbf{j} + \frac{\partial \mathbf{D}}{\partial t} \right) \cdot d\mathbf{S} \quad (4.1)$$

#### **Diferenciální tvar**

$$\text{rot } \mathbf{H} = \nabla \times \mathbf{H} = \mathbf{j} + \frac{\partial \mathbf{D}}{\partial t} \quad (4.2)$$

H..... intenzita elektromagnetického pole

$\mathbf{j} + \frac{\partial \mathbf{D}}{\partial t}$  ..... plošná hustota elektrického proudu a posuvného proudu

### 4.2.2 II. Maxwellova rovnice

Druhá rovnice říká, že zdrojem vírového elektrického pole je časově proměnné magnetické pole. Jedná se o vyjádření Faradayova indukčního zákona. [1] [2]

#### **Integrální tvar**

$$\oint_{C(S)} \mathbf{E} \cdot d\mathbf{l} = - \iint_S \left( \mathbf{j} + \frac{\partial \mathbf{B}}{\partial t} \right) \cdot d\mathbf{S} \quad (4.3)$$



### Diferenciální tvar

$$\operatorname{rot} E = \nabla \times E = -\frac{\partial B}{\partial t} \quad (4.4)$$

E ..... intenzita elektrického pole

B ..... magnetická indukce

#### 4.2.3 III. Maxwellova rovnice

Celkový tok elektrické intenzity libovolnou uzavřenou plochou je úměrný celkovému náboji Q, který uzavírá. [1] [2]

### Integrální tvar

$$\oint_{S(V)} D \cdot dS = \iiint_V \rho^* dV = Q \quad (4.5)$$

### Diferenciální tvar

$$\operatorname{div} D = \nabla \cdot D = \rho^* \quad (4.6)$$

D ..... elektrická indukce

#### 4.2.4 IV. Maxwellova rovnice

Vyjadřuje princip kontinuity magnetických indukčních čar. To znamená, že jsou uzavřené. [1] [2]

### Integrální tvar

$$\oint_{S(V)} B \cdot dS = 0 \quad (4.7)$$

### Diferenciální tvar

$$\operatorname{div} B = \nabla \cdot B = 0 \quad (4.8)$$

B ..... magnetická indukce

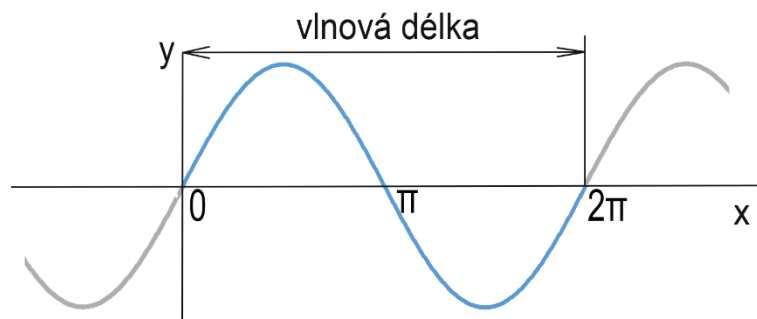
### 4.3 Elektromagnetické vlnění

Elektromagnetické vlnění, často označované také jako elektromagnetické záření, vzniká časovými změnami intenzity elektrického pole  $\partial E / \partial t$  a intenzity magnetického pole  $\partial H / \partial t$ . Tyto časové změny nezůstávají lokalizovány na místě, v němž k nim dochází, ale šíří se prostorem jako vlnění. [1] [2]

Elektromagnetické vlnění je charakterizováno vlnovou délkou, amplitudou a frekvencí neboli kmitočtem. [1] [2]

#### 4.3.1 Vlnová délka

Elektromagnetické vlnění je periodické. Vlnovou délkou rozumíme přímočarou vzdálenost, kterou vlna urazí za jednu periodu, tedy v intervalu  $\langle 0; 2\pi \rangle$  (viz obr. 4.1). Vlnovou délku označujeme řeckým písmenem  $\lambda$  a uvádíme v délkových jednotkách např. metrech. [1] [2]



Obr. 4.1 Vlnová délka [1]

Šíření elektromagnetických vln prostorem závisí na vlnové délce. U dlouhých a středně dlouhých vln dochází k ohybu podél zemského povrchu. Tohoto jevu využíváme při vysílání signálu za rozměrné překážky. Ve výšce přibližně 60 km nad zemským povrchem se nachází vrstva atmosféry tzv. ionosféra. Ta pro elektromagnetické vlnění představuje „vodivou“ plochu. Vlnění se v této vrstvě odráží a v závislosti na aktuálních atmosférických

podmínkách lze dosáhnout vyslání elektromagnetického vlnění na značnou vzdálenost. [1]  
[2] [3]

Vlnovou délku lze vypočítat jako podíl rychlosti šíření vlny, tedy rychlosti světla, a frekvence (viz rovnice 4.9). [1] [3]

$$\lambda = \frac{c}{f} \quad (4.9)$$

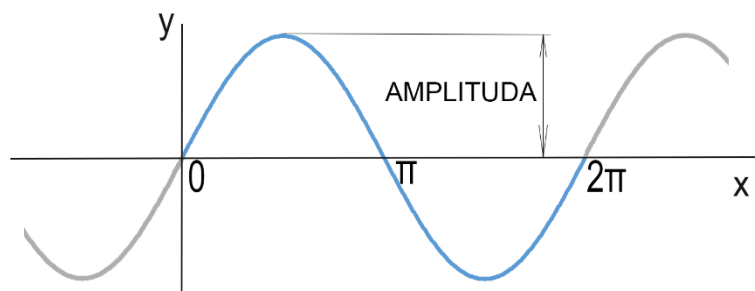
$c$ ..... rychlost světla (300 000 km/s) [km/s]

$f$ ..... frekvence [Hz]

$\lambda$ ..... vlnová délka [m]

#### 4.3.2 Amplituda

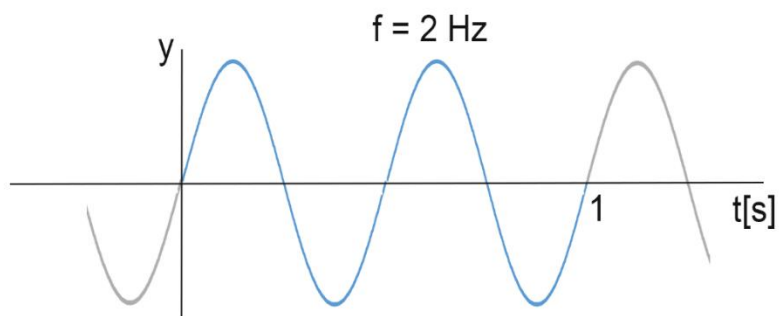
Amplituda je absolutní hodnota největší výchylky (viz obr. 4.2). Této hodnoty je dosaženo jednou kladně a jednou záporně během jedné periody. Amplituda může být konstantní, nebo může docházet k rezonanci či tlumení. K rezonanci dochází složením dvou a více periodických dějů, čímž amplituda narůstá a může tak dosáhnout výrazně vyšších hodnot než původní amplituda. Tlumením ztrácí vlna energii a amplituda se zmenšuje. [1]  
[2] [3]



Obr. 4.2 Amplituda [1]

### 4.3.3 Frekvence

Počet period (kmitů) za sekundu nazýváme frekvence (viz obr. 4.3). Frekvence je převrácenou hodnotou periody (viz rovnice 4.10) a vyjadřujeme ji měrnou jednotkou hertz  $\text{Hz} = \text{s}^{-1}$ . [1] [2]



Obr. 4.3 Frekvence [1]

Závislost frekvence a periody určuje vztah: [1] [2]

$$f = \frac{1}{T} \quad (4.10)$$

f ..... frekvence [Hz]

T ..... perioda [s]

Vztah závislosti frekvence a vlnové délky: [1] [2]

$$f \cdot \lambda = c \quad (4.11)$$

f ..... frekvence [Hz]

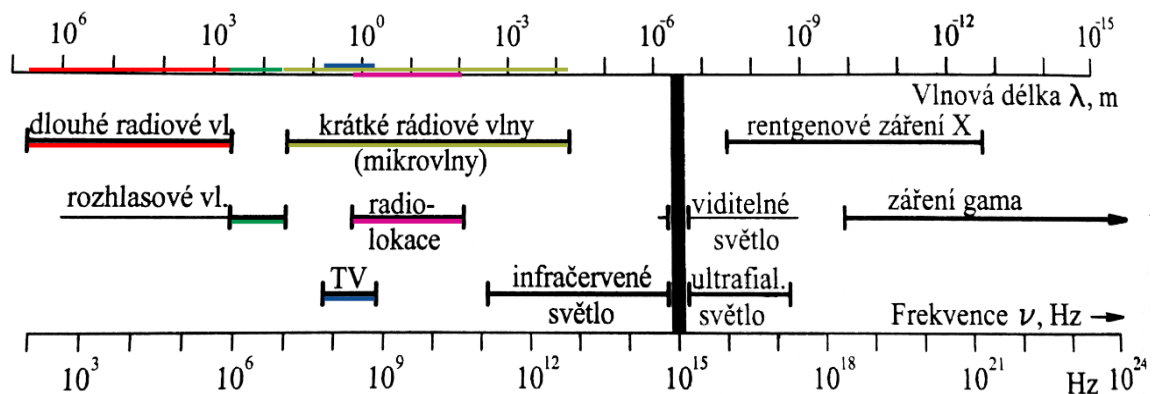
$\lambda$  ..... vlnová délka [m]

c ..... rychlost šíření vlny [ $\text{m} \cdot \text{s}^{-1}$ ]

#### 4.4 Frekvence a jejich rozdělení

Elektromagnetické vlnění se šíří vakuem rychlostí  $2,997 \cdot 10^8 \text{ m} \cdot \text{s}^{-1}$ . Základy fyziky vychází z předpokladu, že se jedná o nejvyšší rychlost, kterou se může energie šířit prostorem. Tuto rychlost nazýváme rychlost světla. Je-li vlnová délka elektromagnetického vlnění v rozmezí od  $0,78 \cdot 10^{-6} \text{ m}$  do  $0,36 \cdot 10^{-6} \text{ m}$ , jedná se o viditelné záření (světlo). [1] [2]

Pro účely bezdrátové datové komunikace využíváme vlnové délky větší než  $10^{-3} \text{ m}$ , viz obr. 4.4. Podmínky využívání frekvenčního spektra a jeho rozdělení má ve správě na území České republiky Český telekomunikační úřad (ČTÚ). Tyto podmínky mají zajistit ochranu před vzájemným ovlivňováním jednotlivých přenosů. [1] [2] [4]



Obr. 4.4 Spektrum elektromagnetického vlnění [1] [2]

Frekvenční spektrum je ČTÚ rozděleno na kmitočtová pásma. Rozlišujeme pásma licencovaná a nelicencovaná. Při dodržení stanovených podmínek ČTÚ, můžeme na nelicencovaných pásmech využívat vlastní zařízení. Jednou z hlavních podmínek ČTÚ na nelicencovaných pásmech je omezování vyzářeného výkonu vysílačem. Vysílání v licencovaném frekvenčním pásmu vyžaduje zakoupení licence pro využívání pásma u ČTÚ. Rozdělení kmitočtů a podmínky jejich používání jsou uvedeny ve všeobecném oprávnění č. VO-R/10/05.2014-3, jež je dostupné na stránkách Českého telekomunikačního úřadu. V tab. 4.1 rozdělení frekvencí podle způsobu využití je uveden přehled rozdělení frekvencí podle způsobu využití. [1] [4]

Tab. 4.1 Rozdělení frekvencí podle způsobu využití [5] [4] [1]

Námořní a letecká navigace	3-30 kHz
Rozhlas (dlouhé vlny), časové signály, navigace	30-300 kHz
Rozhlas (střední vlny)	300-3000 kHz
Amatérské rádio a krátkovlnné vysílání	3-30 MHz
Rozhlas (krátké vlny)	30-300 kHz
Televizní vysílání, mobilní telefony, WI-FI	300-3000 MHz
Mikrovlnná zařízení, radary	3-30 GHz
Radioastronomie, Vysokorychlostní přenos dat	30-300 GHz

V této diplomové práci je využito technologie Wi-Fi, jež je nejčastěji provozována na frekvencích 2,4 GHz a 5 GHz. Tato frekvenční pásma jsou nelicencovaná. V generální licenci GL-30/2000 vydanou ČTÚ je pro pásmo 2,4 GHz povolen max. vyzařovaný výkon 100 mW. Pro Wi-Fi provozované v pásmu 5 GHz je povoleno dosáhnout maximálního výkonu 200 mW. Vysílač Wi-Fi musí být umístěn ve vnitřních prostorech budovy. [4] [5] [1]

#### 4.5 Vysílání a příjem signálu

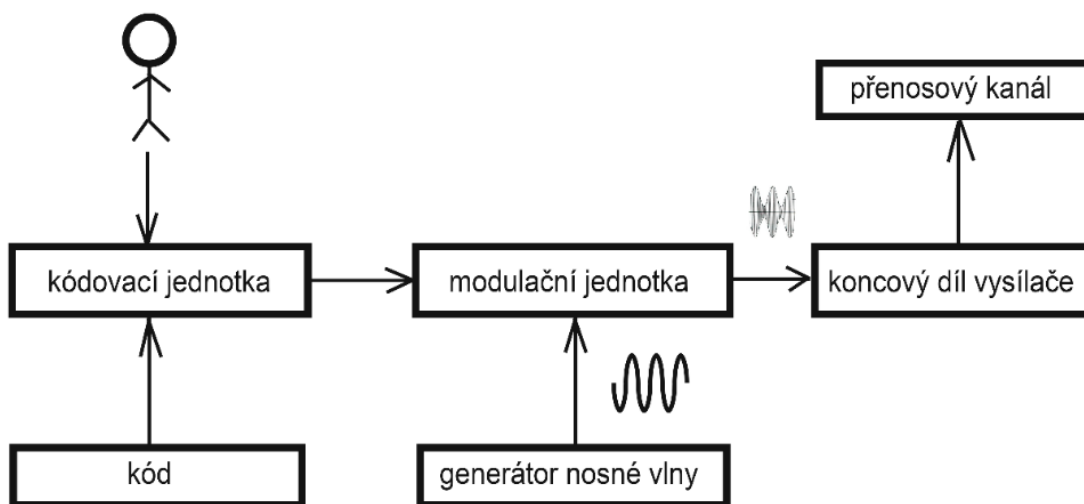
Principem bezdrátové datové komunikace je přenos dat mezi vysílačem a přijímačem (viz obr. 4.5). V případě komunikace prostřednictvím elektromagnetických vln je zapotřebí pomocí vysílače vyzářit elektromagnetickou vlnu do prostoru prostřednictvím antény a anténou přijímače tuto elektromagnetickou vlnu zachytit. Pro efektivní vyzáření elektromagnetické vlny je zapotřebí, aby délka antény byla polovinou nebo čtvrtinou vlnové délky elektromagnetické vlny. [6] [1] [2]



Obr. 4.5 Přenos signálu [1]

#### 4.5.1 Vysílání přenosového signálu

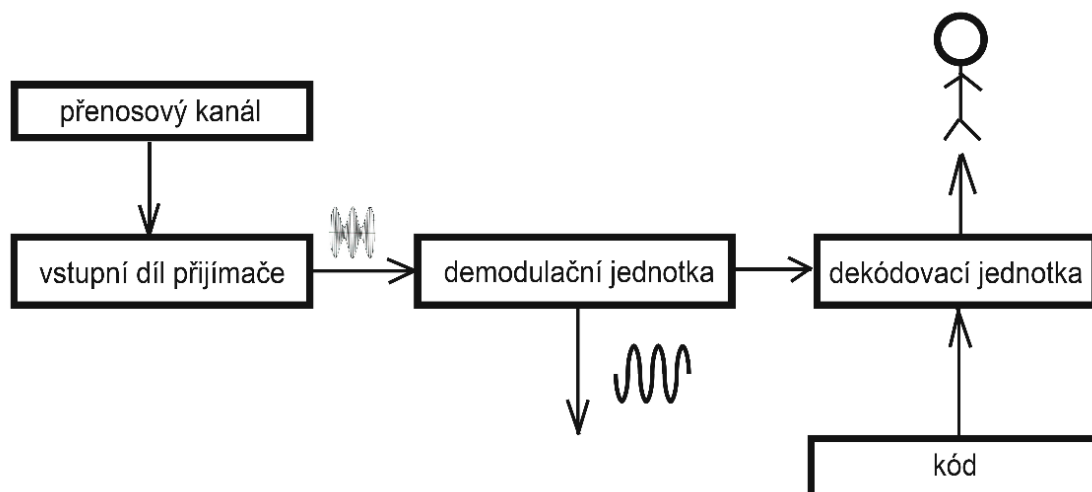
Data přenášíme prostřednictvím elektromagnetické vlny. Abychom tedy mohli data odeslat, musíme je nejdříve umístit na elektromagnetickou vlnu. Tento proces se nazývá modulace. Generátorem se vytváří elektromagnetická vlna, do níž je následně modulací zakódována přenášená informace (viz obr. 4.6). Rozlišujeme modulaci amplitudovou (AM), frekvenční (FM) a fázovou. [6] [1]



Obr. 4.6 Schéma vytvoření přenosového signálu [6] [1]

#### 4.5.2 Příjem přenosového signálu

Elektromagnetická vlna je při cestě mezi vysílačem a přijímačem ovlivňována rušením. Proto po zachycení elektromagnetické vlny anténou přijímače získáváme vlnu, jež s jistou pravděpodobností odpovídá vzoru na straně vysílače. Tzv. demodulací získáme zakódovanou zprávu z nosné vlny (viz obr. 4.7). Abychom byli schopni zprávu z nosné vlny demodulovat, musíme znát typ modulace, kterým byla zpráva modulována na nosnou vlnu.



Obr. 4.7 Schéma zpracování signálu [6] [1]

## 4.6 Antény

Elektromagnetické vlnění vytváříme pomocí pasivního zařízení nazývaného anténa, jež převádí elektrický proud na elektromagnetické vlnění a naopak. [7] [1]

### 4.6.1 Základní vlastnosti antén

Základní vlastnosti závisí na typu konstrukce a velikosti antény. Jsou to frekvenční rozsah, zisk, impedance, polarizace a směrovost. [7] [1]

#### 4.6.1.1 Frekvenční rozsah

Frekvenční rozsah je dán úbytkem síly signálu o 3dB od středního kmitočtu a představuje pracovní rozsah frekvence antény, s níž je schopna pracovat. Délka antény je zpravidla rovna polovině vlnové délky, jež je vypočtena ze střední hodnoty frekvenčního rozsahu. [7] [1] [8]



#### 4.6.1.2 Zisk antény

Zisk antény vyjadřuje, kolikrát je zvýhodněn určitý směr oproti dipólu (osy). Udává se na logaritmické stupnici v decibelech. [7] [1] [8]

#### 4.6.1.3 Impedance

Impedance je zdánlivý odpor na pracovním kmitočtu antény. Ten musí být totožný se vstupním odporem přijímače či s odporem koncového stupně vysílače. V případě, že tyto odpory nejsou shodné, dojde k tzv. stojatému vlnění, jež může způsobit poškození elektrického zařízení. [7] [1] [8]

#### 4.6.1.4 Polarizace

Polarizace antény stanovuje rovinu, v níž je vysílána elektromagnetická vlna. Nejčastěji se vysílá v horizontální či vertikální polarizaci. U parabolických antén se setkáváme i s kruhovou a eliptickou polarizací, přičemž závisí na směru otáčení. [7] [1] [8]

#### 4.6.1.5 Směrnost

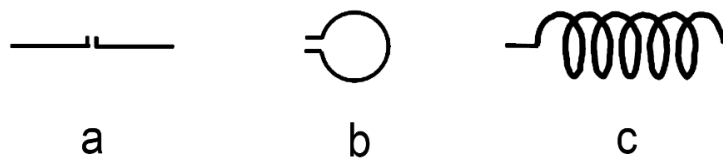
Úhel, v němž je možné efektivně vysílat a přijímat signál, označujeme jako směrnost. Hranice tohoto úhlu jsou dány poklesem signálu, přičemž na hranici tohoto úhlu je síla signálu maximálně o 3dB nižší oproti maximu. Dle směrnosti dělíme antény na směrové a všesměrové. [7] [1] [8]

#### 4.6.2 Základní typy konstrukce antén

Mezi nejpoužívanější typy konstrukcí antén patří drátové, plošné, parabolické, čočkové a anténní řady.

##### 4.6.2.1 Drátové antény

Při přenosu na větších vlnových délkách, např. rádio, RC modely, se setkáváme s drátovou konstrukcí antény. U této konstrukce se využívá vyzařování vodičů, přičemž délka vodiče je větší než jeho průměr. Drátové antény se tvarují do přímého vodiče, smyčky, či šroubovice (obr. 4.8). [7] [1] [8]



Obr. 4.8 Drátové antény - a) přímý vodič, b) smyčka, c) šroubovice [7] [1]

##### 4.6.2.2 Plošné antény

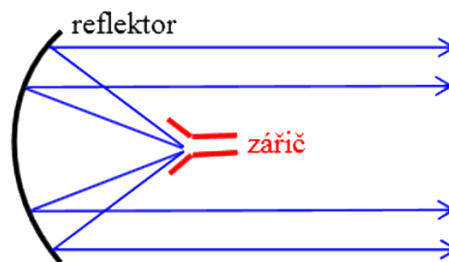
U mobilních sítí GSM či DVB-T televizního vysílání se využívá plošných antén (viz obr. 4.9). K vyzařování dochází výstupní plochou antény, jež může mít také tvar štěrbin, trychtýře apod. [7] [1] [8]



Obr. 4.9 Plošná anténa [8]

#### 4.6.2.3 Parabolické antény

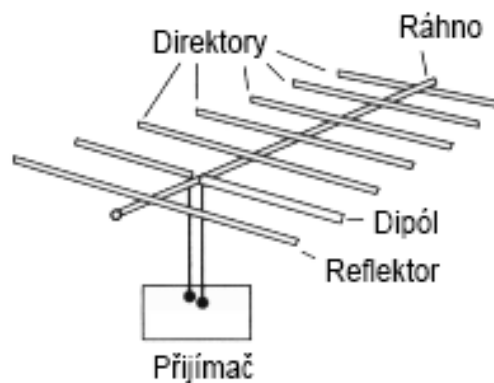
Nejúčinnějším typem konstrukce antény je parabolická anténa, jež se skládá z reflektoru a zářiče (viz obr. 4.10). Reflektor bývá ve tvaru paraboloidu, v jehož ohnisku je umístěn zářič. Ten vyzařuje elektromagnetické vlny směrem k reflektoru, jenž odrazem tyto vlny usměrňuje požadovaných směrem. [8] [1]



Obr. 4.10 Parabolická anténa [8] [1]

#### 4.6.2.4 Anténní řady

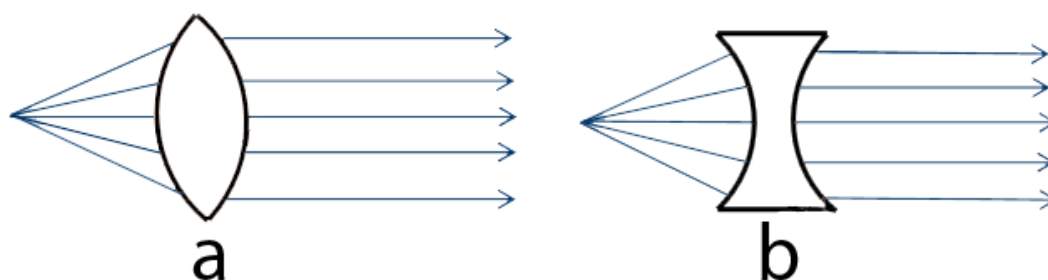
Tento typ antény reprezentuje Yagiho anténní řada (viz obr. 4.11). Ta se skládá z reflektoru, direktorů a dipólu (zářiče). Dipólem je vyzařován vlastní signál, jenž je usměrňován pomocí reflektoru. Tento signál je zachytáván direktory společně s přijímaným signálem, přičemž dojde ke spojení těchto signálů a tím i k zesílení přijímaného signálu. [8] [1]



Obr. 4.11 Yagiho anténní řada [8]

#### 4.6.2.5 Anténní čočky

U anténních čoček dochází k usměrnění elektromagnetického záření vyzářeného zářičem pomocí čočky (viz obr. 4.12). Ta může být konvexního, konkávního či rovinného tvaru. Pro správné fungování musí být zářič umístěn v ohnisku čočky. Na rozdíl od parabolických antén lze anténní čočky zkonstruovat menší při zachování podobných vlastností. [8] [1]



Obr. 4.12 Anténní čočky – a) konvexní, b) konkávní [8] [1]

#### 4.7 Rušení signálu

Při procházení elektromagnetické vlny prostorem dochází k jejímu rušení. To je způsobeno okolními vlivy, např. počasím, sluneční erupcí, fyzickými překážkami, vysíláním na podobné vlnové délce, elektrickým vedením apod. Rušení se projevuje chybami v přenesených datech, např. šum v obrazu televizního vysílání, snížení přenosové rychlosti apod. [1]

Průchodnost elektromagnetické vlny fyzickou překážkou je závislá především na vlnové délce a velikosti překážky. Pokud je vlnová délka menší než velikost překážky, dojde k odražení vlny. Zda vlna projde překážkou, však nezávisí pouze na velikosti překážky, ale i na materiálu překážky. Například vlna o vlnové délce 6 cm (kmitočet 5 GHz) prochází kapkami deště s malým rušením, zatímco vlna o vlnové délce 12,5 cm (kmitočet 2,4 GHz) téměř není schopna kapkami deště proniknout. [1]

Rušení způsobují i některá elektronická zařízení, jež vyzařují elektromagnetické záření, např. frekvenční měniče, špatně stíněná kabeláž apod. Jelikož jsou bezdrátové přenosy v dnešní době hojně využívané, dochází ke vzniku rušení označovaném jako „elektro-smog“. Zaměříme-li se na technologii Wi-Fi, narazíme v hustě obydlených oblastech na problém, kdy jsme schopni zachytit i více než patnáct Wi-Fi sítí na kmitočtu 2,4GHz v jeden okamžik. Vzhledem k tomu, že u této technologie se na frekvenci 2,4GHz využívá v České republice třinácti kanálů, jež se navzájem překrývají, dochází k potkávání více signálů na jednom kanále a vzájemnému rušení signálů. [1]

Abychom dosáhli ideální přenosu, je naším cílem odstranit veškeré rušení signálu. V praxi však nejsme schopni toto rušení zcela odstranit, snažíme se jej tedy minimalizovat, např. použitím stíněné kabeláže, odstraněním překážek, přemístěním vysílače, zesílením signálu apod. [1]

## 5 Technologie Wi-Fi

Standard IEEE 802.11 známý pod označením Wireless Fidelity, zkráceně Wi-Fi reprezentuje technologii bezdrátové sítě. Nejčastěji se používá v sítích LAN (Local Area Network), setkáme se s ní však i u sítí PAN (Personal Area Network) a WAN (World Area Network). Wi-Fi se používá jak ve vnitřních, tak i venkovních prostorech. [1] [9]

### 5.1 Protokoly standardu IEEE 802.11

Standard IEEE 802.11 se dělí na protokoly, které jsou označovány malými písmeny. Jednotlivé protokoly se liší především maximální přenosovou rychlostí. V České republice jsou volně zpřístupněny Českým telekomunikačním úřadem (ČTU) frekvence 2,4 GHz a 5 GHz. Použití protokolů, které používají jiné frekvence, je podmíněno udělením licence od Českého telekomunikačního úřadu. V následující tabulce vidíme seznam a porovnání protokolů. [1] [9]

Tab. 5.1 Protokoly standardu IEEE 802.11 [9]

Protokol	Vydáno	Frekvence	Šířka pásma	Maximální přenosová rychlost	Licence pásma
802.11a	1999	3,7 GHz	20 MHz	54 Mbit/s	Licencované
		5,0 GHz			Volné
802.11b	1999	2,4 GHz	22 MHz	11 Mbit/s	Volné
802.11g	2003	2,4 GHz	20 MHz	54 Mbit/s	Volné
802.11n	2009	2,4 GHz	20 MHz	72 Mbit/s	Volné
		5,0 GHz	40 MHz	150 Mbit/s	
802.11ad	2012	60 GHz	2 160 MHz	6 750 Mbit/s	Licencované
802.11ac	2013	5,0 GHz	20 MHz	97 Mbit/s	Volné
			40 MHz	200 Mbit/s	
			80 MHz	433 Mbit/s	
			160 MHz	867 Mbit/s	

Nejpoužívanějším protokolem je 802.11g, který zajišťuje dobrý poměr mezi kvalitou signálu, dosahem signálu a přenosovou rychlostí. Tento protokol je nahrazován rychlejším protokolem 802.11n a postupně přichází ke slovu nejnovější protokol 802.11ac.

## 5.2 Zařízení sítě Wi-Fi

Nejčastěji se Wi-Fi používá u sítí typu server-client, lze jej však využít i u sítí peer-to-peer (klient – klient) s označením Ad-hoc. V případě sítě typu server-client se klienti připojují na přístupový bod (AP - Access Point). [1] [9]

### 5.2.1 Access Point

Access Point (AP) je zařízení, které vysílá Wi-Fi signál dle nastavených a dostupných protokolů. K identifikaci Access Pointu dochází pomocí SSID (Service Set Identifier), které obsahuje název bezdrátové sítě. Více AP může vysílat stejné SSID, v tomto případě jsou AP rozlišeny pomocí MAC (Media Access Control), což je jednoznačný identifikátor síťového zařízení. [1] [9]

### 5.2.2 Repeater

Repeater (opakovač) je zařízení, které umožní zvýšit dosah Wi-Fi signálu vysílaného Access Pointem. Jak název napovídá, opakovač přijme signál z Access Pointu a znovu ho vyšle. Tím posílí signál a zvýší dosah. [1] [9]

### 5.2.3 Klient

Klient je zařízení umožňující příjem Wi-Fi signálu a připojení do sítě. Jedná se např. o počítačové karty, USB Wi-Fi, Wi-Fi moduly v telefonech apod. [1] [9]

## 5.3 Zabezpečení

Wi-Fi sítě dělíme na veřejné a privátní. Na veřejnou Wi-Fi síť narazíme nejčastěji v restauracích, obchodech a dalších veřejně přístupných místech. Častěji však zachytíme signál privátní (zabezpečené) sítě. Do privátní sítě se může připojit pouze ten, kdo k tomu má oprávnění. [1] [9]

### 5.3.1 WEP

Připojení do sítě je podmíněno zadáním hesla, WEP klíče. Těchto klíčů lze specifikovat více najednou a většinou dosahují délky třinácti znaků. Po připojení do sítě je tento klíč přenášen s každým paketem. Zachytáváním paketů lze tento klíč odhalit do několika minut. Z tohoto důvodu se použití tohoto šifrování nedoporučuje. [1] [9]

### 5.3.2 WPA, WPA 2

WPA (Wi-Fi Protected Access) technologie je nástupcem WEP klíčů. WPA odstraňuje nedostatky šifrování WEP tak, že tyto klíče dynamicky mění. Klient se do sítě připojuje pomocí hesla, stejně jako u šifrování WEP. Rozdíl je však v tom, že u WPA je autentizace do sítě prováděna pomocí PSK (Pre-Shared Key), kdy obě strany komunikují na základě dlouhé heslové fráze. [1] [9]

Několik posledních let se setkáváme také s šifrováním WPA 2, ve kterém neprobíhá šifrování pomocí PSK, ale pomocí kvalitnějšího šifrování AES (Advanced Encryption Standard). Nevýhodou proti WPA jsou větší nároky na výkon zařízení. [1] [9]

### 5.3.3 Protokol IEEE 802.1X

Protokol IEEE 802.1X specifikuje připojování klientů do sítě pomocí identických přihlašovacích údajů. Přihlašovací údaje jsou ověřeny Radius serverem, tedy třetí stranou. Většinou spolu s přihlašovacími údaji dojde i k ověření certifikátu, který musí být instalován



v klientské stanici. Toto zabezpečení je v porovnání s ostatními způsoby zabezpečení poměrně složité, zajišťuje však vysoké zabezpečení. [1] [9]

#### 5.3.4 Filtrování MAC adres

Každé síťové zařízení má svou identickou fyzikální adresu MAC (Media Access Control). Většina Access Pointů nám umožňuje povolit připojení zařízení do sítě na základě seznamu povolených MAC adres. Filtr lze použít i opačným způsobem, tedy specifikovat zařízení, které se naopak do sítě připojit nemohou. Pomocí šikovných nástrojů lze u většiny zařízení tuto MAC adresu změnit. Proto nelze považovat tuto ochranu sítě za bezpečnou. [1] [9]

#### 5.3.5 Vypnutí vysílání SSID

Každá síť Wi-Fi je identifikována pomocí SSID (Service Set Identifier), který představuje název sítě. Při vyhledávání Wi-Fi sítí v dosahu se nám v seznamu zobrazují právě názvy sítě, tedy SSID. Access Pointy nám umožňují vysílání SSID vypnout, skrýt síť. Síť, která nevysílá své SSID, je skrytá a připojit se k ní mohou pouze zařízení, které o existenci této sítě vědí. Úroveň tohoto zabezpečení je velmi nízká. [1] [9]

### 5.4 Rušení signálu Wi-Fi

Pro volné používání však jsou k dispozici nelicencované frekvence 2,4 GHz a 5 GHz. Frekvenci 2,4 GHz však nevyužívá pouze technologie Wi-Fi, ale i mnohé další technologie např. Bluetooth, mikrovlnné trouby, RC modely apod. Velké zatížení tohoto pásma způsobuje časté rušení přenosů. Především v hustě obydlené oblasti se přenos dat prostřednictvím Wi-Fi na frekvenci 2,4 GHz stává téměř nemožným. [10]

Wi-Fi signál je také ovlivňován fyzickými překážkami. Největší rušení způsobují překážky z kovu, betonu a sádky. Velké rušení způsobuje také mramor, cihla a voda. Jelikož se lidské tělo skládá přibližně ze 70% z vody, dochází k rušení signálu Wi-Fi i pohybem osob

v prostoru. To má za následek snížení přenosové rychlosti vlivem navýšení počtu chyb při přenosu dat. [10]

Minimalizaci rušení signálu provádíme především odstraněním překážek, lepším umístěním Access Pointů, změnou kanálu či přechodem na frekvenci 5 GHz, která není prozatím tolik využívána. [10]

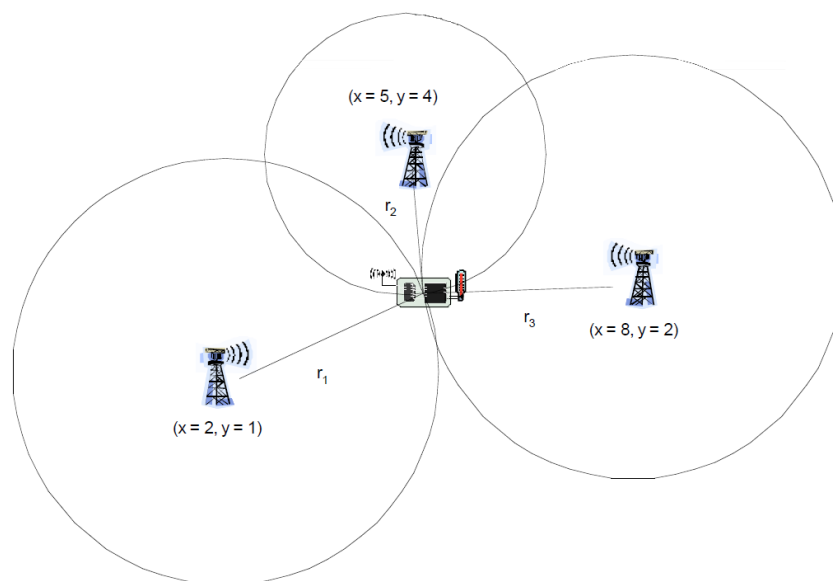
## 6 Triangulace

Určování polohy a vzdálenosti bodu pomocí trigonometrického výpočtu nazýváme Triangulace. Tento pojem zahrnuje mnoho výpočetních metod závislých na způsobu získávání vstupních dat. Tato práce je zaměřena na základní metody výpočtu polohy pomocí bezdrátových přenosů. Mezi tyto metody patří: [11]

- Proximity,
- Trilaterace,
- Analýza prostoru,
- Indikace síly signálu,
- Doba přenosu,
- Časový rozdíl přenosu,
- Směrové antény,
- Překrytí signálů,
- Aproximace bodu v trojúhelníku.

### 6.1 Proximity

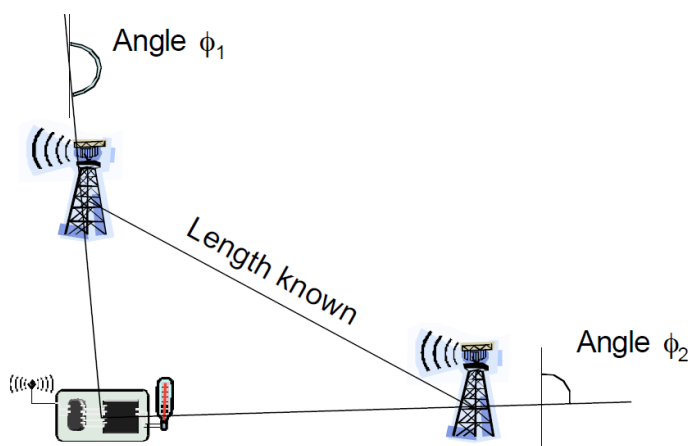
Jedná se o jednu z nejjednodušších metod určování polohy. Pro výpočet je třeba znát polohu tří vysílačů a přesnou vzdálenost od každého vysílače. Přesná poloha bodu je určena průsečíkem tří kružnic, jež mají každá střed v jednom z vysílačů a jejich poloměr je vzdáleností od daného vysílače. Grafické znázornění vidíme na obr. 6.1. [11]



Obr. 6.1 Proximity [11]

## 6.2 Trilaterace

Trilaterace nebo také Multilaterace určuje polohu bodu na základě dvou a více vysílačů o známé poloze, známé vzdálenosti mezi vysílači a úhlu, pod kterým se od jednotlivých vysílačů nachází hledaný bod. Grafické znázornění určení polohy bodu vidíme na obr. 6.2. [11]



Obr. 6.2 Trilaterace [11]

### 6.3 Analýza prostoru

Poloha bodu je určena porovnáním aktuálních hodnot s předem naměřenými hodnotami. Tato metoda je tedy založena na myšlence, že ve stejném bodě a rozdílném čase jsme schopni opakovaně naměřit stejné hodnoty síly signálu. Přesnost této metody závisí na rozdílu podmínek měření v čase určování polohy bodu oproti podmínkám měření v čase analýzy prostoru. [11]

### 6.4 Indikace síly signálu

Z vysílače je vyslán signál o známé síle a se známou charakteristikou úbytku signálu. V hledaném bodě je pak změřena síla tohoto signálu. Na základě úbytku na síle signálu je dle předem známé charakteristiky určena vzdálenost bodu od vysílače. Aby tato metoda byla přesná, musí se bod nacházet ve středu paprsku vyslaného signálu. [11]

### 6.5 Doba přenosu

Vzdálenost bodu od vysílače je určena pomocí doby putování signálu a známé rychlosti šíření signálu. Pro správné určení vzdálenosti je zapotřebí přesné synchronizace času na vysílači a přijímači, jehož vzdálenost je určována. [11]

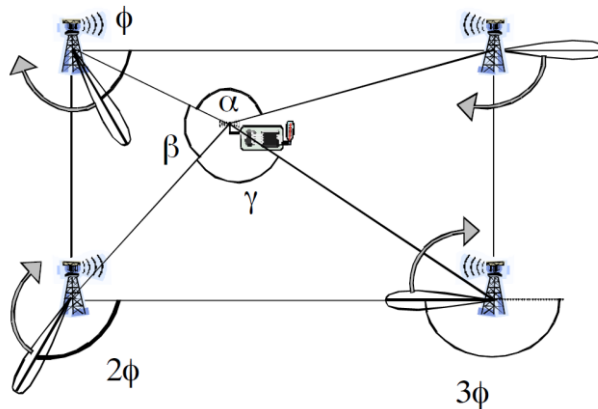
### 6.6 Časový rozdíl přenosu

U této metody jsou z vysílače vyslány současně dva signály, každý s jinou rychlostí šíření. Například kombinace rádiového signálu a ultrazvuku, jenž se šíří prostorem pomaleji. Po přijetí obou signálů je vypočítán časový rozdíl v příjmu signálu. Na základě tohoto rozdílu je poté dopočítána skutečná vzdálenost od vysílače. Problémem této metody jsou velké náklady na drahý a energeticky náročný hardware, jenž je potřeba přesně kalibrovat. [11]

### 6.7 Směrové antény

Poloha bodu je určena pomocí úhlů, jež jsou získány měřením pomocí směrových antén. Bod se musí nacházet mezi směrovými anténami. Tyto antény se otáčejí buď

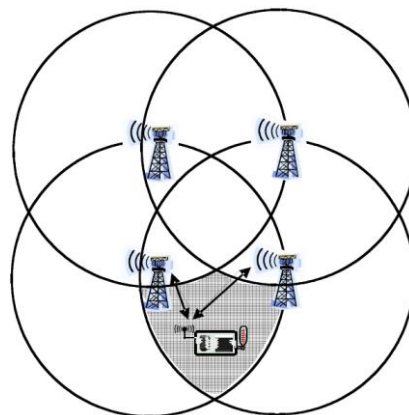
mechanicky konstantní rychlostí, nebo jsou řízeny elektronicky. Při otáčení se měří časová prodleva v zachycení signálu jiné antény a signálu hledaného bodu. Ze známé rychlosti otáčení a doby otáčení do zachycení signálu je dopočítán úhel, pod nímž se nachází hledaný bod. Po určení úhlů z jednotlivých směrových antén je dopočítána poloha bodu (obr. 6.3). [11]



Obr. 6.3 Určení polohy bodu pomocí směrových antén [11]

## 6.8 Překrytí signálů

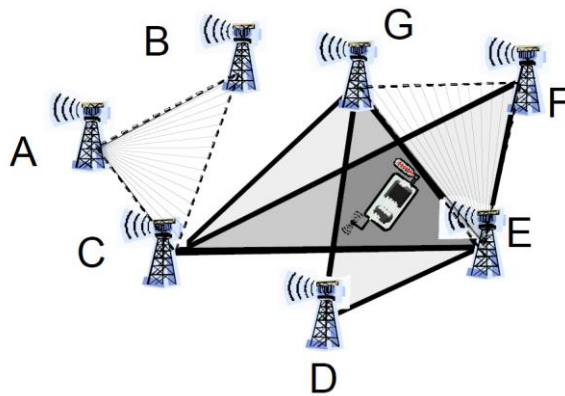
Při této metodě se zjišťují dostupné signály z okolních vysílačů, jejichž poloha je známa. Na základě prolnutí signálů je určena poloha bodu ve středu plochy překrytí těchto signálů. U této metody je určena pouze přibližná poloha. Grafické znázornění této metody vidíme na obr. 6.4. [11]



Obr. 6.4 Určení polohy bodu pomocí překrytí signálů [11]

## 6.9 Aproximace bodu v trojúhelníku

U této metody jsou propojeny vysílače, jejichž polohu známe, pomocí trojúhelníků. Zjišťuje se, ve kterých trojúhelnících se objekt, jehož poloha se určuje, nachází. Objekt se nachází ve společné ploše těchto trojúhelníků (viz obr. 6.5). Tato metoda pouze odhaduje polohu bodu, není tedy určena jeho přesná poloha. [11]



Obr. 6.5 Určení polohy bodu pomocí aproximace v trojúhelníku [11]

## 7 Stávající řešení používané ve světě

Vytvořením technologie, jež by umožňovala přesně určovat polohu v uzavřených prostorech, se zabývá spousta firem po celém světě. Potenciál využití takovéto technologie je obrovský. Hlavním využitím je navigace po rozlehlých a složitých budovách, např. letištních halách, obchodních centrech, nemocnicích apod. S touto navigací se již můžeme setkat v praxi na mezinárodním letišti Eldorado v Kolumbii, v tokijské pobočce Google či na univerzitě v Kodani. Tyto technologie jsou však zároveň velmi diskutabilní z důvodu omezování osobní svobody.

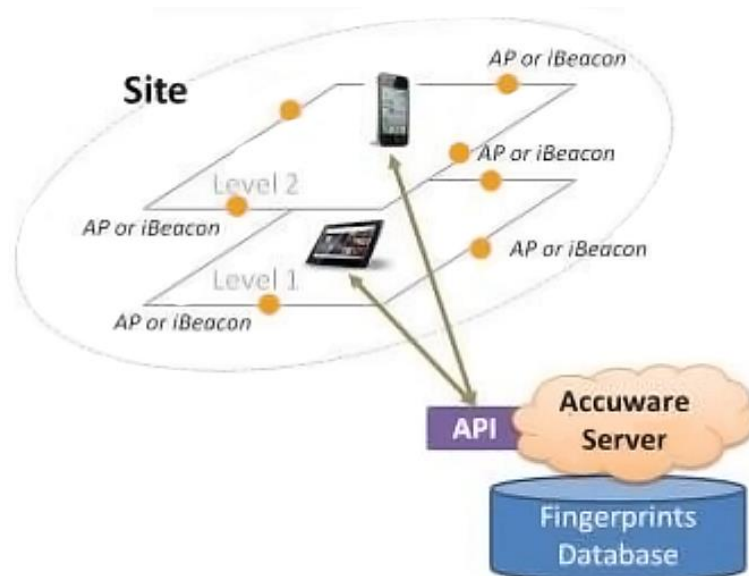
Při hledání existujících řešení, jež se již používají v praxi, byly posuzovány pouze technologie využívající signál Wi-Fi. Bohužel všechny firmy zabývající se touto technologií drží konkrétní informace o způsobu určení polohy jako obchodní tajemství. Práce se zmíní o několika nejznámějších firmách a nastíní, na jakém principu technologie dané firmy funguje.

### 7.1 Accuware

Firma Accuware se zabývá monitorováním pohybu osob a zařízení, lokalizováním zařízení Bluetooth a Wi-Fi. Produkt firmy Accuware indoor navigation slouží k navigaci osob v rozlehlých budovách. Technologie využívá kombinaci Wi-Fi a Bluetooth signálů. Klientské zařízení je smartphone, jež má nainstalovanou aplikaci této firmy (viz obr. 7.2). [12]

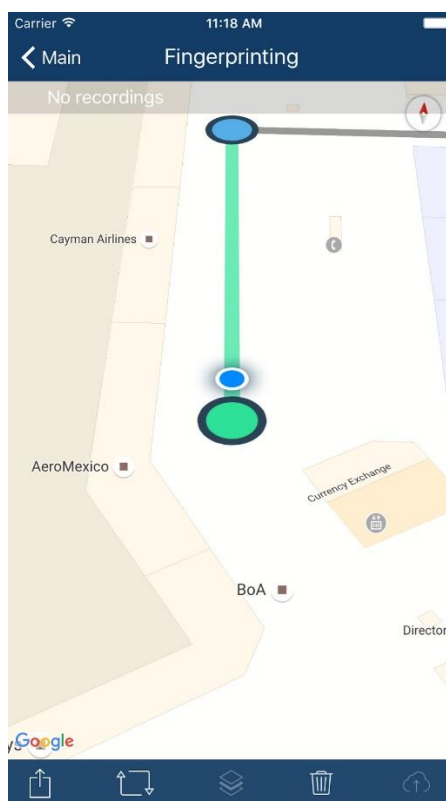
Aplikace odesílá pomocí internetového připojení informace o síle signálů dostupných AP a informace z kompasu zařízení na server firmy Accuware (viz Obr. 7.1 Accuware indoor navigation - schéma), jež na základě přijatých dat vypočte polohu zařízení a informace o této poloze odešle zpět do zařízení. [12]





Obr. 7.1 Accuware indoor navigation - schéma [12]

To následně uživateli zobrazí mapu s označením aktuální polohy, a cestu, kudy se má uživatel vydat, aby se dostal na požadované místo (viz obr. 7.2). [12]



Obr. 7.2 Accuware indoor navigation - aplikace [12]

## 7.2 Ekahau

Firma Ekahau se primárně zabývá analýzou spektra Wi-Fi signálu. Vyvíjí aplikaci, jež umožňuje vypracovat velmi podrobnou spektrální mapu signálu (viz obr. 7.3). Firma také dodává zařízení ve formě náramku, který měří aktuální sílu signálu jednotlivých AP. Na základě těchto naměřených hodnot, jež jsou odeslány server, je určena poloha zařízení. Firma Ryston electronics, jež nabízí produkty Ekahau v České republice, udává přesnost této technologie na 1 metr. [13] [14]



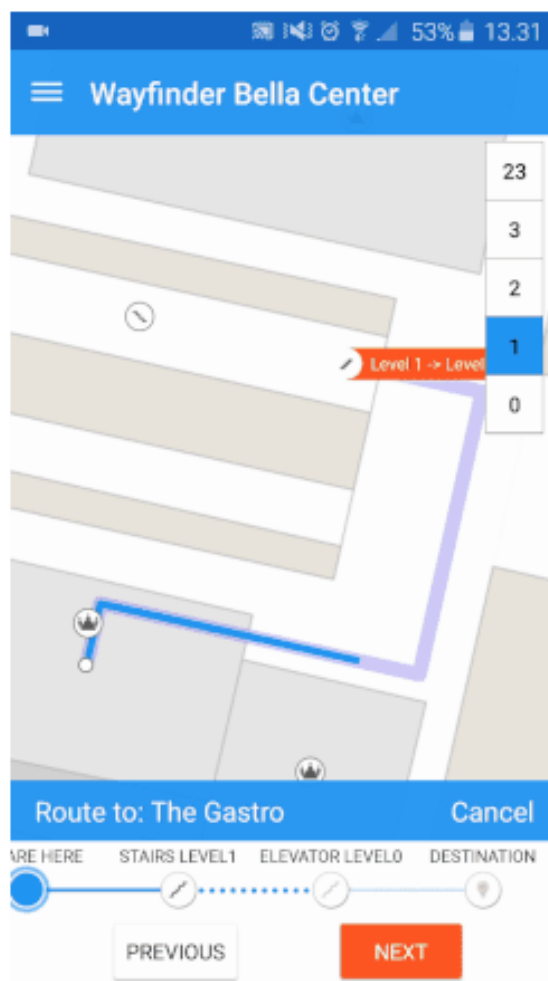
Obr. 7.3 Ekahau - spektrální mapa [14]

## 7.3 Infsoft

Tato firma vyvíjí aplikaci pro zařízení s operačním systémem Android. Tato aplikace na základě síly signálu, MAC adresy dostupných AP a předem známých naměřených hodnot určí přibližnou polohu zařízení. Firma Infsoft udává přesnost této technologie na 5 – 15 metrů. [15]

## 7.4 Mapspeople

Technologie firmy Mapspeople je nejvíce rozšířena v praxi. Firma úzce spolupracuje s firmou Google. Technologie je postupně implementována do aplikace Google maps. Jakmile uživatel, který je navigován pomocí aplikace Google maps, vstoupí do vnitřních prostor, jež mají instalovanu tuto technologii, dojde k přepnutí zobrazení mapy na zobrazení vnitřní mapy objektu (viz obr. 7.4). Uživatel je tak navigován až na konkrétní místo v objektu. Technologie využívá kombinaci Wi-Fi, magnetických polí a osvětlení. [16]



Obr. 7.4 MapsIndoors [16]

## 8 Koncepce řešení

Podstatou této diplomové práce je navrhnout a otestovat technologii monitorující pohyb osob v uzavřeném objektu pomocí signálu Wi-Fi. To znamená, že dozor musí mít k dispozici nástroj, jenž mu zobrazí polohu monitorovaných osob. Je tedy potřeba vytvořit server, který bude shromažďovat informace o poloze osoby a zařízení (klienta), jež bude předávat na server informace o dostupných Wi-Fi signálech. Na základě těchto informací bude následně určena přibližná poloha osoby.

Zařízení klienta bude zkonstruováno z běžně dostupných komponentů tak, aby bylo co nejjednodušší. Zařízení bude získávat údaje o dostupných signálech Wi-Fi v daném bodě, síle tohoto signálu a MAC adrese AP, z něhož je signál vysílán. Tyto informace budou zaslány prostřednictvím zvolené a dostupné Wi-Fi sítě na server. Kvůli přenositelnosti bude zařízení napájeno pomocí baterií a zkonstruováno v co nejmenším možném provedení.

Pro operační systém Windows bude vytvořen program, jehož součástí bude server pracující na síťovém protokolu TCP/IP (IPv4). Prostřednictvím tohoto protokolu budou předávány informace mezi klientem a serverem. Program získané informace porovná s předem vypočtenou mapou síly signálů a určí přibližnou polohu. Tu poté zobrazí v grafickém okně programu, jenž obsahuje vnitřní mapu objektu.

Data budou klientem odesílána na server v pravidelném intervalu dle možností zvoleného hardware.

Po sestavení zařízení klienta bude provedeno úvodní testování, na jehož základě bude navržen algoritmus pro určení polohy. Poté bude naprogramován samotný server a technologie bude podrobena úvodnímu testování. Na základě tohoto testování bude postupně upravován algoritmus tak, aby bylo dosaženo co největší přesnosti určení polohy.

Následně bude technologie aplikována v poloprovozních podmínkách (školních prostorech) a důkladně otestována. Na základě vyhodnocení těchto testů budou stanovena závěrečná doporučení a použitelnost této technologie v praxi.

## 9 Praktické řešení

Po teoretickém návrhu jsem se zaměřil na praktické vytvoření potřebných součástí zařízení, aby bylo možné danou technologii otestovat.

### 9.1 Návrh a sestavení hardware

Jako hardware bylo zapotřebí použít Wi-Fi modul, jenž bude snadno dostupný a plně programovatelný. Na základě dobrých zkušeností s vývojovou deskou Arduino od firmy Atmel se práce zaměřuje na Wi-Fi moduly určené pro tuto vývojovou desku.



Obr. 9.1 Arduino Uno Rev3 [17]

#### 9.1.1 Programovatelné Wi-Fi moduly

Pro tuto desku jsou aktuálně dostupné tři moduly: WiFi Shield V2.2 for Arduino, ESP 8266 a NRF24L01. Modul NRF24L01 komunikuje na frekvenci 2,4 GHz, ale nepodporuje ani jeden protokol IEEE 802.11. Pro účely určování polohy je nezbytné navázat komunikaci po Wi-Fi síti, proto byl tento modul z výběru vyřazen. [18] [19] [20]

##### 9.1.1.1 WiFi Shield V2.2

Modul WiFi Shield V2.2 (obr. 9.2) je rozšířením vývojové desky Arduino Uno (obr. 9.1). Je napájen napětím 3,3V a primárně je určen pro bezdrátové ovládání robotů.

Modul podporuje protokoly IEEE 802.11 b/g/n, bezpečnostní protokoly WEP, WPA/WPA2 a přenosové protokoly UDP, TCP/IP (IPv4), DHCP, ARP, DNS, HTTP/HTTPS Client, HTTP/HTTPS Server. Výrobce udává spotřebu při přenosu 135 mA. Součástí modulu je odnímatelná anténa. Přehled základních parametrů tohoto modulu WiFi Shield V2.2 vidíme v tab. 9.1. [21] [20]

Tab. 9.1 Základní parametry WiFi Shield V2.2 [20]

Parametr	Hodnota
WiFi protokoly	802.11 b/g/n
Frekvenční rozsah	2 400 MHz – 2 497 MHz
Anténa	Externí – IPEX konektor
Provozní napětí	3.3 V
Spotřeba při odesílání dat	135 mA
Provozní teplota	-40 – 125°C
Wi-Fi módy	client, softAP, softAP + client
Wi-Fi security	WEP, WPA/WPA2
Síťové protokoly	UDP, TCP (IPv4), DHCP, ARP, HTTP/HTTPS



Obr. 9.2 Modul WiFi Shield V2.2 [21]

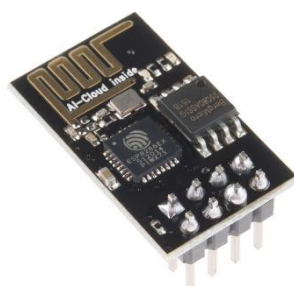
Cena modulu WiFi Shield V2.2 se pohybuje kolem 1 900 Kč za kus. Jeho rozměry jsou 32 x 23,5 x 3 mm. [21] [20]

### 9.1.1.2 ESP 8266

ESP 8266 (obr. 9.3) je velmi kompaktní Wi-Fi modul, jenž slouží k rozšíření vlastních vyvíjených periférií nebo jej lze díky vlastnímu mikro kontroléru použít jako samostatnou funkční součástku. Stejně jako WiFi Shield V2.2 je napájen napětím 3,3V. Podporuje Wi-Fi protokoly IEEE 802.11 b/g/n, bezpečnostní protokoly WEP, WPA/WPA2 a přenosové protokoly UDP, TCP (IPv4), HTTP a FTP. Spotřeba tohoto modulu se pohybuje v závislosti na síle signálu a aktuálním protokolu IEEE 802.11 od 120 do 170 mA. V tab. 9.2 vidíme přehled základních parametrů modulu ESP 8266. [19]

Tab. 9.2 Základní parametry ESP 8266 [19]

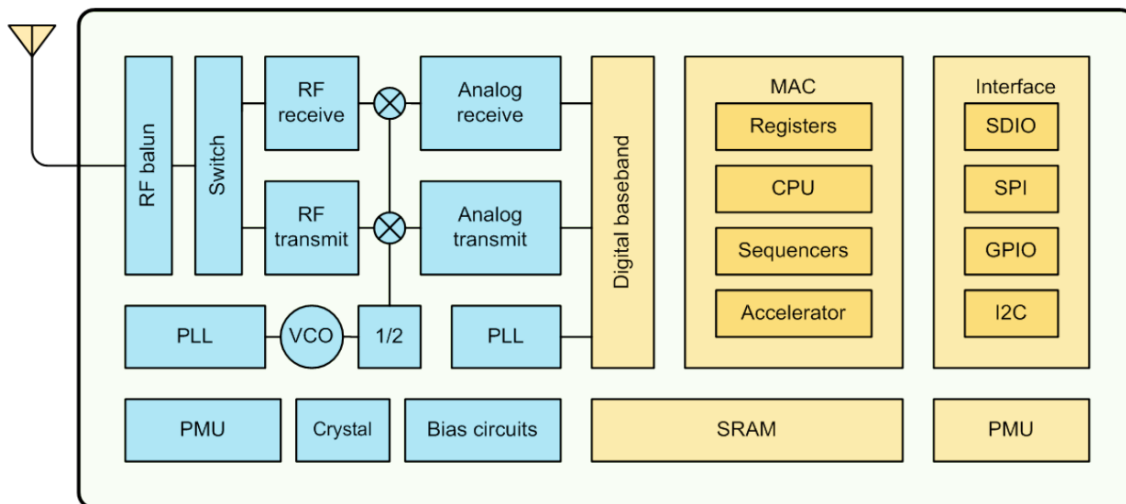
Parametr	Hodnota
WiFi protokoly	802.11 b/g/n
Frekvenční rozsah	2 400 MHz – 2 483,5 MHz
Anténa	interní
Provozní napětí	3.0 – 3.6 V
Spotřeba při odesílání dat	170 mA
Provozní teplota	-40 – 125°C
Wi-Fi mody	client, softAP, softAP + client
Wi-Fi security	WEP, WPA/WPA2
Síťové protokoly	UDP, TCP (IPv4), http, FTP



Obr. 9.3 Modul ESP 8266 [22]



Cena modulu ESP 8266 se pohybuje kolem 56 Kč za kus. Díky této velmi nízké ceně existuje obrovská komunita nadšenců tohoto modulu. Rozměry jsou velmi malé (20 x 10 x 1 mm). Na obr. 9.4 vidíme schéma rozložení komponent na modulu. [19]



Obr. 9.4 Schéma ESP 8266 [19]

### 9.1.1.3 Porovnání a výběr modulu

Byly porovnány klady a zápory modulů WiFi Shield V2.2 a ESP 8266. Výsledky tohoto porovnání jsou shrnuty v tab. 9.3.

Tab. 9.3 Porovnání parametrů modulů WiFi Shield V2.2 a ESP 8266 [21] [19]

Vlastnost	WiFi Shield V2.2	ESP 8266
Wi-Fi 2,4 GHz	Ano	Ano
Protokol 802.11b	Ano	Ano
Protokol 802.11g	Ano	Ano
Protokol 802.11n	Ano	Ano
Wi-Fi mód client	Ano	Ano
Wi-Fi WPA/WPA2	Ano	Ano
Síťový protokol TCP (IPv4)	Ano	Ano
Síťový protokol UDP	Ano	Ano
Anténa	Externí	Interní
Provozní napětí	3,3 V	3,3 V
Spotřeba při odesílání	135 mA	170 mA
Samostatně funkční součástka	Ne	Ano
Cena	1 900 Kč	56 Kč

Výsledky porovnání ukazují, že parametry obou zařízení jsou téměř shodné. Vzhledem k podstatnému rozdílu v ceně byl vybrán modul ESP 8266. Dalším důvodem tohoto rozhodnutí byla interní anténa, jež díky menšímu zisku zajistí větší rozdíly v síle signálu. Kolem modulu ESP 8266 existuje obrovská komunita nadšenců. Díky tomu byl při hledání informací o tomto modulu nalezen volně dostupný firmware s názvem NodeMCU, jenž umí zpracovávat LUA skripty a umožňuje plně naprogramovat požadované funkce tohoto modulu. Díky tomu byla tedy volba tohoto modulu jednoznačná. [18]

### 9.1.2 Potřebné komponenty pro zprovoznění modulu

Velmi častým problémem řešeným v souvislosti s modulem je napájení ESP 8266. Modul má při odesílání dat spotřeba 170 mA. Pokud napájecí zdroj nedokáže plně pokrýt spotřebu energie při odesílání dat, dojde k restartování modulu a k přerušení komunikace. Byl tedy použit převodník napětí doporučený výrobcem, jenž měl dobré ohlasy na komunitních fórech. Jedná se o převodník napětí I2C 5V – 3,3V (obr. 9.5), jenž převádí vstupních 5V na 3,3V a zároveň chrání komunikační linku proti přepětí. [23]



Obr. 9.5 Přebodník napětí I2C 5v – 3,3V [24]

Jako zdroj napětí byly použity 1,5V baterie AA. Pro dosažení potřebného minimálního napětí 5V je zapotřebí zapojit do série čtyři tyto baterie. Výsledné napětí zdroje pak bude 6V. Mezi napájecí zdroj a převodník napětí byl předřazen stabilizátor napětí AMS1117-5V (obr. 9.6). Ten je schopen stabilizovat napětí až z 12V na požadovaných 5V. Maximální nárazový proud, který je schopen stabilizovat je až 800 mA. To je pro Wi-Fi modul ESP 8266, jenž má maximální odběr 170 mA, více než dostačující. [23]

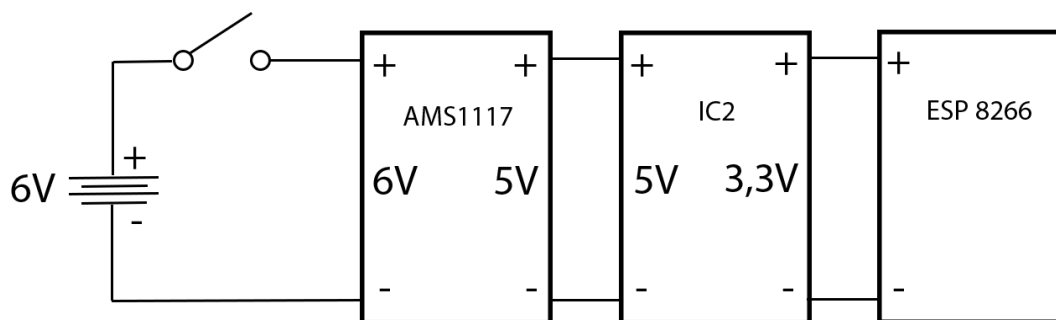


Obr. 9.6 Stabilizátor napětí AMS1117-5V [23]

Dále byly použity dva mikropřepínače. Jeden pro zapínání a vypínání zdrojového napětí a druhý pro přepínání modulu ESP 8266 do režimu přepisování firmware. Také byl použit pinový pás pro možnost připojení modulu k PC přes sériovou linku. Veškeré komponenty byly instalovány na epoxidovou desku, s vyleptanými plošnými spoji.

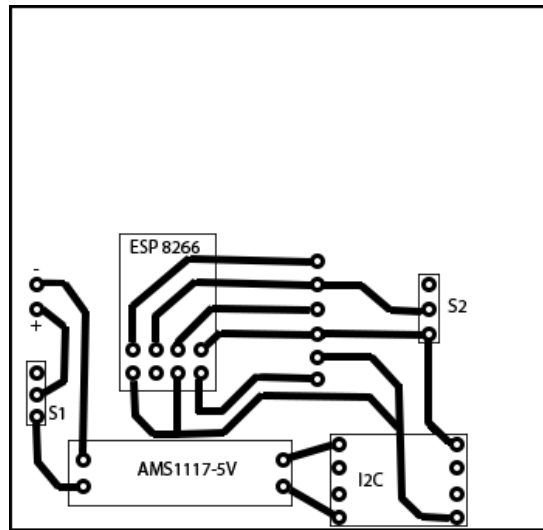
### 9.1.3 Sestavení komponent

Nejdříve bylo určeno rozmístění komponent na epoxidové desce tak, aby bylo možné propojit všechny komponenty dle schématu na obr. 9.7. Rozměry epoxidové desky jsou určeny velikostí bateriového boxu na čtyři 1,5V baterie AA, na který bude deska připevněna.



Obr. 9.7 Schéma zapojení komponent [vlastní]

Na obr. 9.8 je vidět schéma rozložení komponent a plošných spojů. Přepínač S1 slouží k vypnutí přívodního napětí. V případě potřeby přehrání firmware v modulu ESP 8266 je k dispozici přepínač S2, který propojí GPIO 0 (obr. 9.9) modulu se zemí, čímž se modul přepne do režimu přepisování firmware.



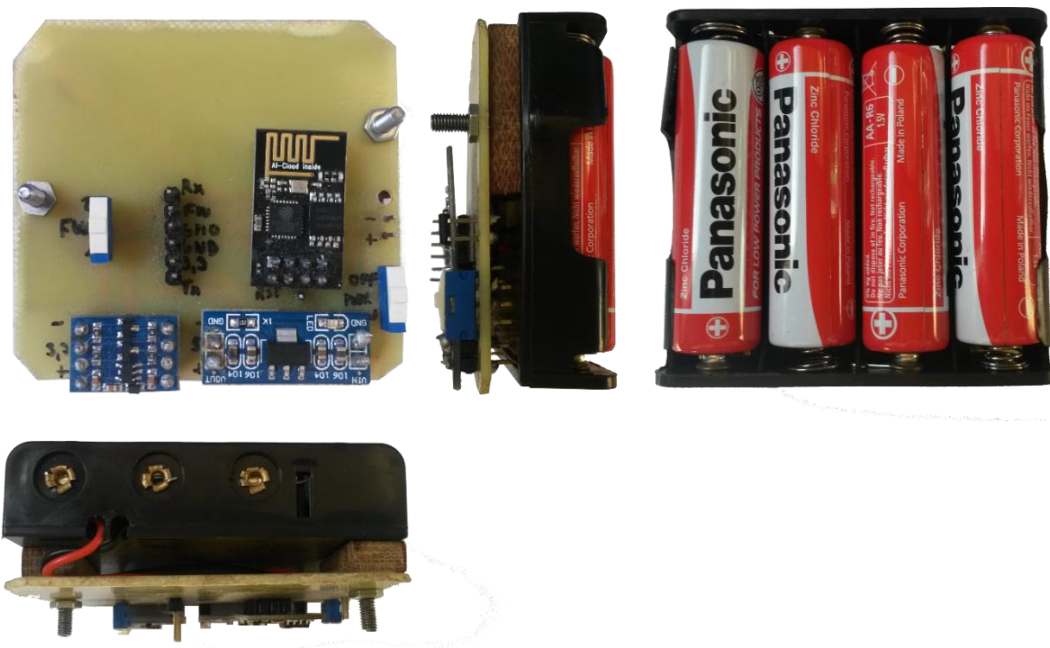
Obr. 9.8 Schéma plošných spojů [vlastní]

ESP 8266 je připojeno dle obr. 9.9, přičemž VCC = napětí, GND = zem, RX/TX = komunikační linky, GPIO0 = při uzemnění přepnuto do režimu přehrávání firmware, GPIO2 = vstup / výstup, RST = reset, CH\_PD = povoluje vypnutí napájení. [25]



Obr. 9.9 ESP 8266 - piny [25]

Po vyleptání plošných spojů a sestavení komponent vzniklo funkční zařízení, jež můžeme vidět na obr. 9.10.



Obr. 9.10 Zkonstruované zařízení klienta [vlastní]

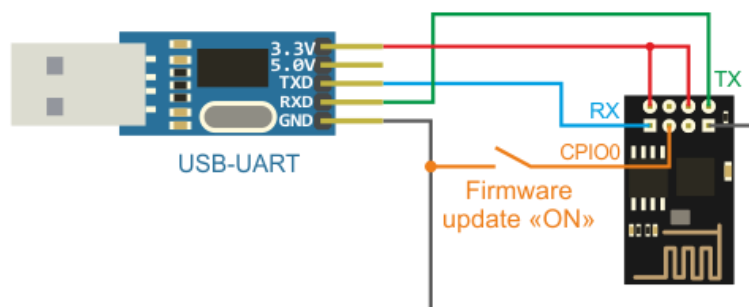
#### 9.1.4 Programování Wi-Fi modulu

Pro připojení ESP 8266 k PC byl použit USB – UART převodník (obr. 9.11).



Obr. 9.11 USB - UART převodník [vlastní]

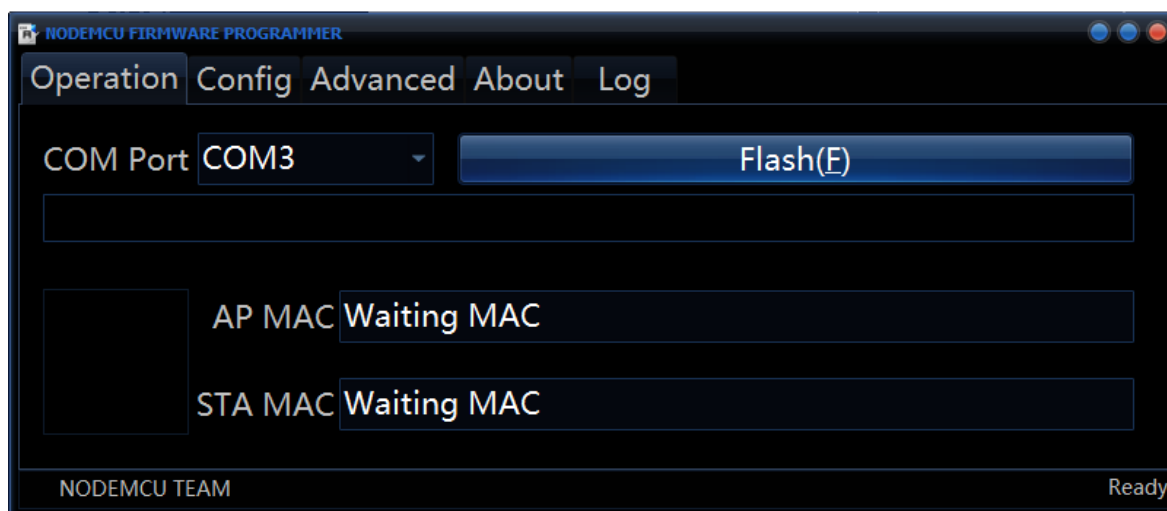
Připojení ESP 8266 a USB – UART převodníku je provedeno dle schéma na obr. 9.12.



Obr. 9.12 Schéma zapojení ESP 8266 a USB - UART převodníku [26]

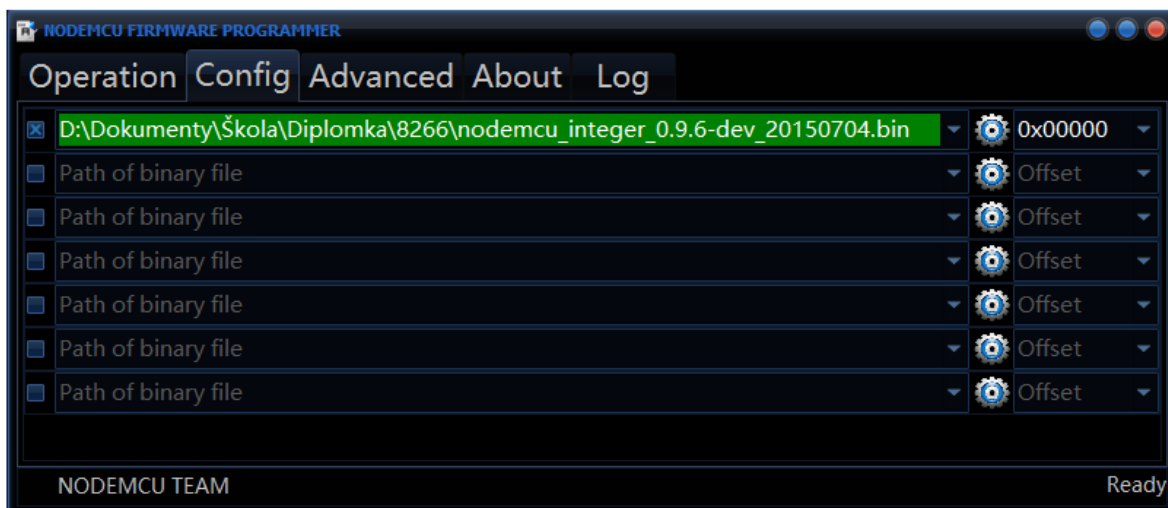
Modul ESP 8266 obsahuje předinstalovaný firmware od výrobce. Tato verze však obsahuje chybu, která neumožňuje korektní komunikaci. Z tohoto důvodu je v první řadě nezbytné nahrát novou verzi firmware. Při aktualizaci nebyla použita nová verze firmware od výrobce, ale volně dostupný firmware s názvem NodeMCU, jenž podporuje programování modulu pomocí LUA skriptů. [26] [27]

Nahrání firmware NodeMCU jsem provedl dle návodu na stránce <http://remotexy.com/en/help/esp8266-firmware-update/>. Nejdříve byl připojen pin GPIO0 modulu ESP 8266 k pinu GND na USB – UART převodníku. Tím došlo k přepnutí modulu do režimu přepisování firmware. Pro nahrání firmware nebyl použit program Flash Download Tools v2.4, doporučený v návodu, ale volně dostupný ESP8266Flasher (obr. 9.13), jenž je přizpůsobený přímo pro modul ESP 8266.



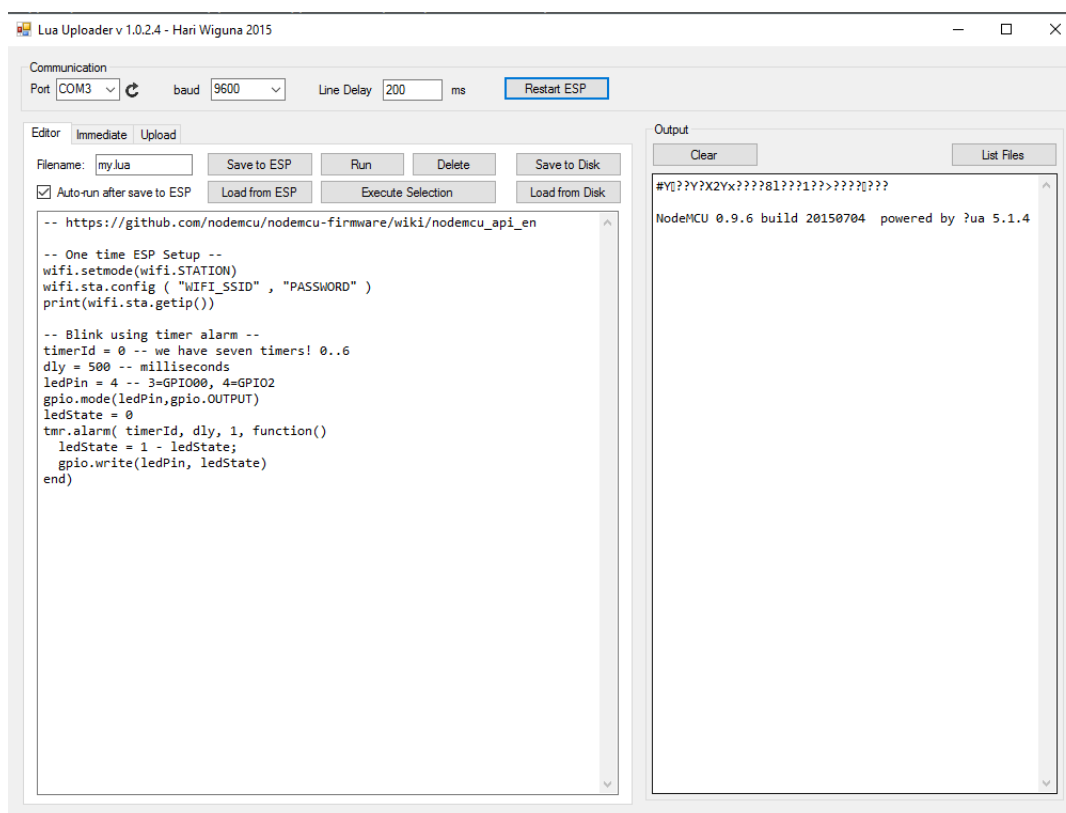
Obr. 9.13 ESP8266Flasher [vlastní]

Po spuštění programu byl nastaven v záložce Operation COM port na COM3, na němž je připojen USB – UART převodník. Následně byl v záložce Config vybrán obraz firmware NodeMCU (obr. 9.14), jenž je třeba nahrát do paměti modulu ESP 8266. Firmware se v paměti nachází na pozici 0x00000. Dále jsem spustil nahrávání nového firmware pomocí tlačítka Flash v záložce Operation. Nahrávání nového firmware trvalo přibližně minutu a půl. [26]



Obr. 9.14 ESP8266Flasher - konfigurace [vlastní]

Pro nahrávání LUA skriptu je k dispozici opět volně dostupný program od Hari Wiguna Lua Uploader v 1.0.2.4 (obr. 9.15). Po nastavení komunikačního portu na COM3 a zapnutí ESP 8266 se v okně Output zobrazí uvítací zpráva a informace o firmwaru, jak je vidět na obr. 9.15 je NodeMCU 0.9.6. [26]



Obr. 9.15 Lua Uploader v1.0.2.4 [vlastní]

Při spuštění ESP 8266 se volá program umístěný v souboru init.lua. V textovém editoru byl vytvořen soubor init.lua, do něhož je umístěna funkční část (program), jež načte síly signálu okolních Wi-Fi AP a pomocí Wi-Fi a TCP připojení tyto data odešle na server. Výsledný program se nachází v příloze 1. Na začátku souboru se nacházejí proměnné, jež definují název a heslo k Wi-Fi, k níž se má modul připojit. Po připojení do této sítě se modul připojí k TCP serveru na zadané IP adrese a portu. Program obsahuje 5 funkcí. První funkce s názvem „listap“ vytvoří řetězec skládající se z identifikátoru (ID) zařízení sloužícího pro rozlišení klientů serverem a informací o dostupných signálech. Výsledný řetězec, jež zároveň tvoří přenášenou zprávu na server, vypadá následovně (pozn. do vzoru zprávy bylo pro přehlednost vloženo řádkování): [27]

1 [

```
UPC662134(3,-89,e0:69:95:f7:bd:86,1);  
IrenaR(2,-87,5c:f4:ab:17:1f:bb,10);  
eMeMka(3,-55,00:11:32:4d:1b:c3,4);  
WLAN1-000327(4,-76,d0:65:ca:db:76:11,13);  
UPC672679(3,-84,e8:40:f2:9a:9a:39,11);  
MikroTik-B8B907(3,-85,4c:5e:0c:b8:b9:07,2);
```

]

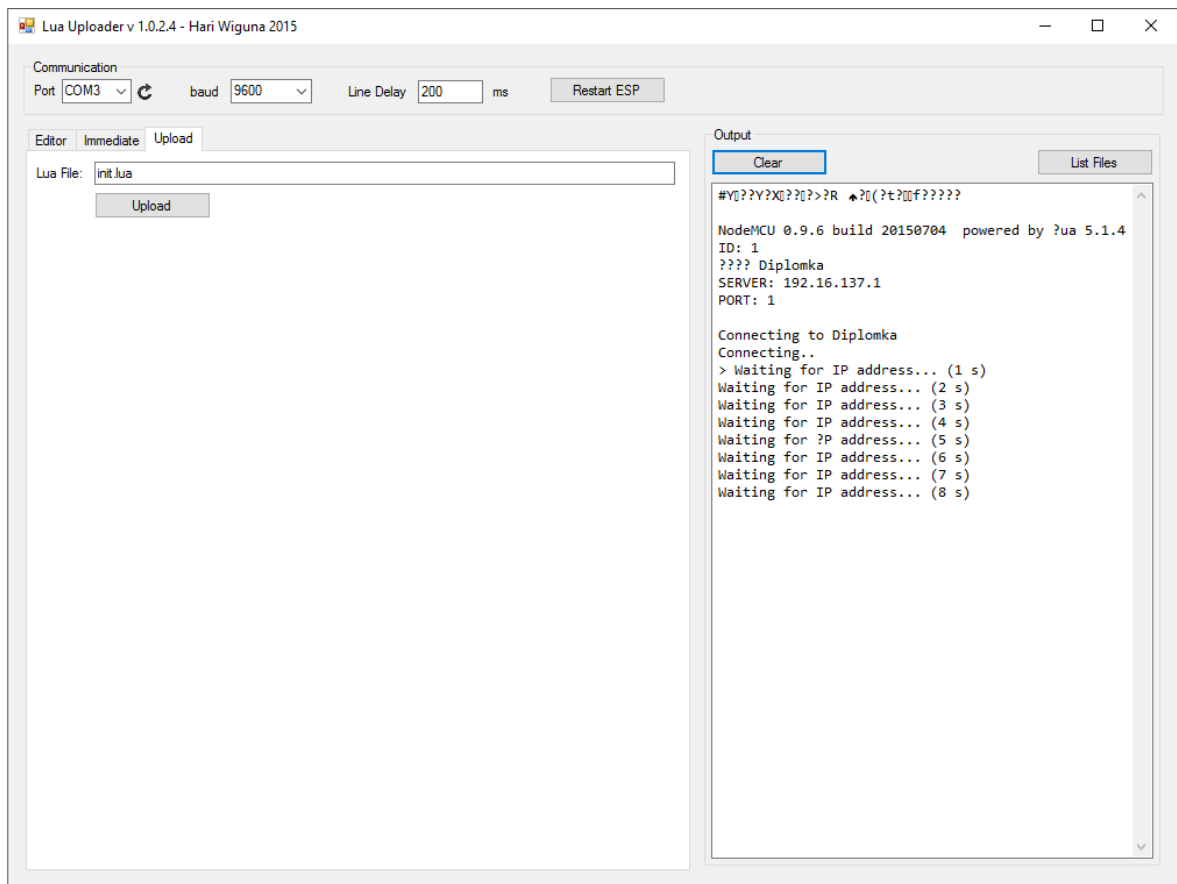
Na prvním místě se nachází číslo reprezentující ono ID zařízení. V hranatých závorkách je umístěn seznam dostupných AP, přičemž je vypsáno SSID a v kulatých závorkách číslo reprezentující typ zabezpečení Wi-Fi sítě, sílu signálu a MAC adresu AP. Jednotlivé AP jsou odděleny středníkem.

Dále se v programu nachází funkce „connect“ pro připojení k zadané Wi-Fi síti, „disconnect“ pro odpojení. Funkce „printAP“ načte okolní AP do pole, jež předá funkci listap pro sestavení zprávy. Ta pak pomocí funkce „send“ odešle data na TCP server pomocí socket (aplikační rozhraní poskytované operačním systémem), k němuž je zařízení připojeno. Po spuštění ESP 8266 a tohoto programu dojde k vypsání nastavených údajů, připojení k Wi-Fi, vyčkání na přidělení IP, připojení k TCP serveru a následně pomocí



časovače nastaveného na 10 sekund dochází k opakovanému načítání dostupných AP a odesílání sestavené zprávy na server.

Následně byl tento program umístěný v souboru init.lua nahrán do ESP 8266 pomocí funkce upload v programu Lua Uploader v 1.0.2.4 viz obr. 9.16.



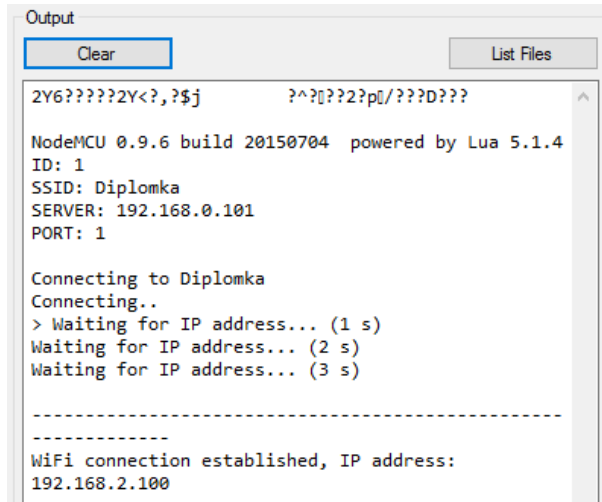
Obr. 9.16 Lua Uploader - nahrání init.lua [vlastní]

Na tomto obrázku můžeme vidět, že po nahrání souboru init.lua a spuštění ESP 8266 dojde ke spuštění tohoto programu.

### 9.1.5 Testování funkčnosti

Po nahrání programu do modulu a jeho spuštění bylo testováno připojení do Wi-Fi sítě s SSID „Diplomka“, zabezpečené pomocí WPA2 s heslem „diplomka12345“. Proces přihlašování do sítě byl monitorován pomocí výpisu do konzole (okna Output) v programu

Lua Uploader (viz obr. 9.17). Připojení do sítě bylo úspěšné, přičemž proces od začátku připojování do získání IP adresy trval přibližně 3 sekundy.



```
Output
Clear List Files

2Y6?????2Y<?,?j      ?^?[]?2?p[]/???D???

NodeMCU 0.9.6 build 20150704 powered by Lua 5.1.4
ID: 1
SSID: Diplomka
SERVER: 192.168.0.101
PORT: 1

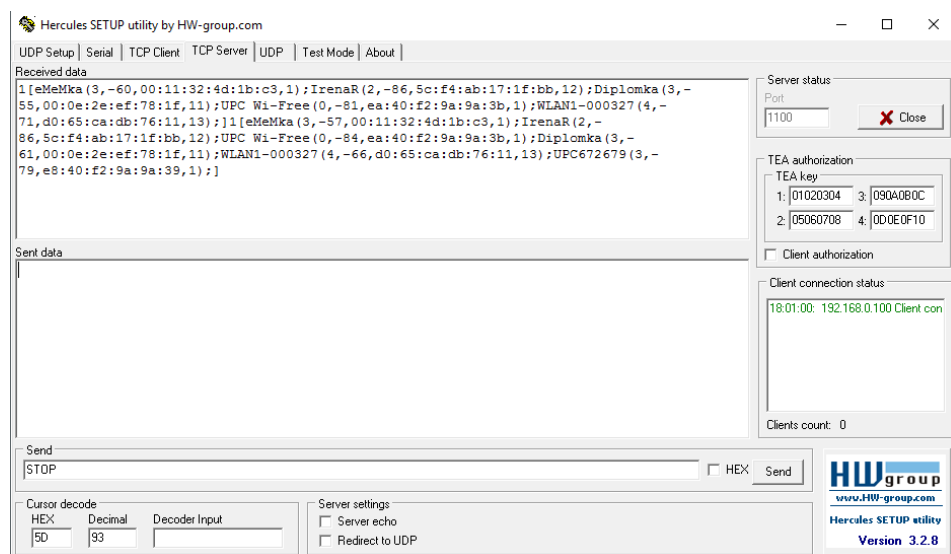
Connecting to Diplomka
Connecting..
> Waiting for IP address... (1 s)
Waiting for IP address... (2 s)
Waiting for IP address... (3 s)

-----
WiFi connection established, IP address:
192.168.2.100
```

Obr. 9.17 Lua Uploader - připojení do sítě Wi-Fi [vlastní]

### 9.1.5.1 Test připojení k TCP serveru

Pro otestování komunikace ESP 8266 s TCP serverem byl použit volně dostupný program Hercules (viz obr. 9.18), jenž umožňuje spustit TCP server na zvoleném portu. Při tomto testování byl vypnut firewall v počítači, na němž je spouštěn TCP server, aby se zamezilo zablokování komunikace.



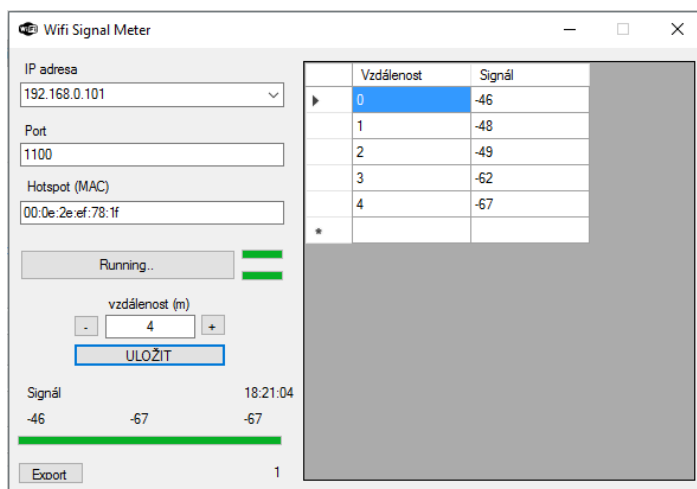
Obr. 9.18 Hercules - TCP server[vlastní]

Po spuštění TCP server v programu Hercules na zvoleném portu 1100 a restartování modulu došlo automaticky k opětovnému připojení do sítě a následně k připojení k TCP serveru. Připojení k serveru bylo navázáno téměř okamžitě po získání IP adresy. Navázání připojení k TCP serveru spustilo časovač, jenž v intervalu 10 sekund načítal dostupné signály Wi-Fi sítí a sestavený řetězec odesílat na server. Zprávy přijaté TCP serverem vidíme v okně „Received Data“ v programu Hercules (viz obr. 9.18). Komunikace mezi ESP 8266 a TCP serverem je tedy plně funkční.

#### 9.1.5.2 Měření úbytku síly signálu v závislosti na vzdálenosti od vysílače

Toto měření bylo provedeno za cílem určit, zda jsou rozdíly síly signálu v různé vzdálenosti od vysílače dostačující pro určování polohy.

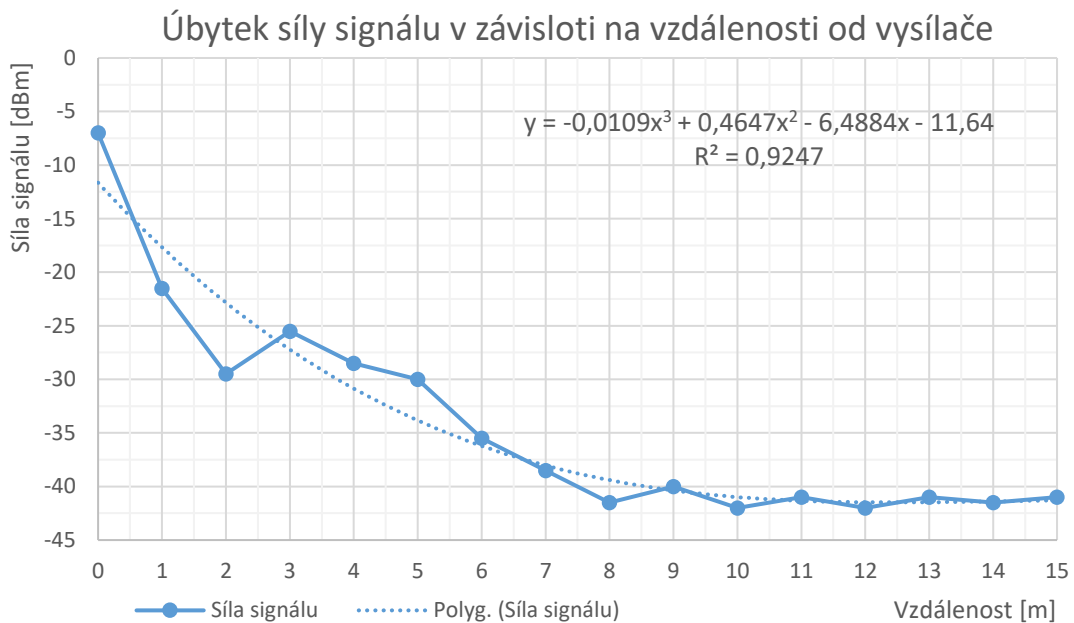
Pro měření úbytku síly signálu v závislosti na vzdálenosti od vysílače byl vytvořen jednoduchý program v jazyce C# (viz obr. 9.19), jehož zdrojové soubory jsou umístěny v příloze na CD. Součástí tohoto programu je TCP/IP (IPv4) server. Po spuštění tohoto programu se nastaví IP adresa a port, na kterém má naslouchat, dále pak MAC adresa monitorovaného AP. Po přijetí dat zaslaných od klienta programem, dojde k vyčtení síly signálu na daný Access Point. Uživatel nastaví aktuální vzdálenost od AP a hodnotu uloží pomocí tlačítka „Uložit“. Takto získaná data lze pomocí tlačítka „Export“ uložit do souboru CSV, jenž lze následně otevřít v programu Microsoft Excel.



Obr. 9.19 Wifi Signal Meter [vlastní]

Měření bylo provedeno ve volném prostranství za slunného dne s použitím AP CANYON Wireless Broadband Router IEEE 802.11g MIMO, k němuž nebyl připojen žádný klient. Signál byl měřen po jednom metru až na vzdálenost 15 metrů, jež byla určena jako maximální velikost místnosti. Měření bylo provedeno ve směru od vysílače a k vysílači. Tento proces měření jsem provedl celkem 3x. Naměřené hodnoty byly zprůměrovány a přeneseny do programu Microsoft Excel. Výsledek měření je zobrazen na graf 9.1.

Graf 9.1 Úbytek síly signálu v závislosti na vzdálenosti od vysílače



Sílu signálu jsem proložil polynomicou spojnicí trendu 3. řádu, viz rovnice 9.1. Koeficient determinace  $R^2 = 0,9247$ .

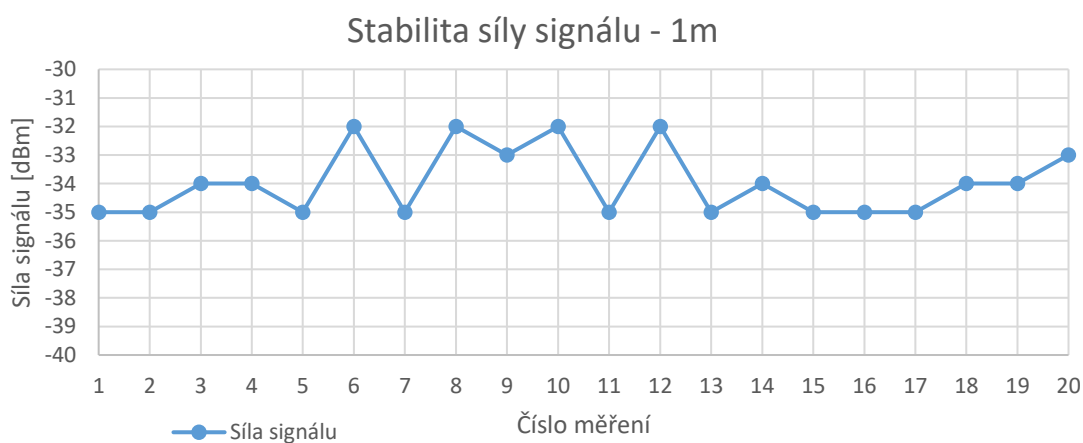
$$y = -0,0109x^3 + 0,4647x^2 - 6,4884x - 11,64 \quad (9.1)$$

Z výsledku měření plyne, že Wi-Fi signál lze použít pro určení polohy, přičemž nejpresnějšího určení polohy dosáhneme přibližně na prvních dvou metrech od vysílače. Ve vzdálenosti větší než osm metrů jsou rozdíly v signálu velmi malé a určení polohy tedy bude méně přesné.

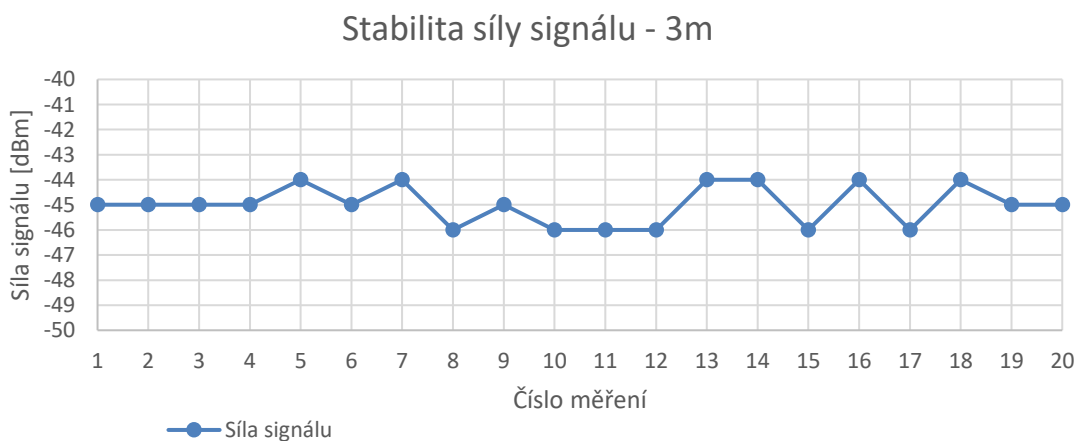
### 9.1.5.3 Měření stability signálu v bodě

Pro přesné učení polohy je zapotřebí, aby v daném bodě byla síla signálu stabilní. Proto bylo provedeno měření stability signálu v bodě. Měření se provedlo celkem 3x ve vzdálenosti 1m, 3m a 6m od AP. V každé vzdálenosti byla naměřena síla signálu 20x. K měření signálu byl opět použit AP CANYON Wireless Broadband Router IEEE 802.11g MIMO, k němuž nebyl připojen žádný klient. Výstupy měření jsou shrnuty v následujících grafech 9.2, 9.3 a 9.4:

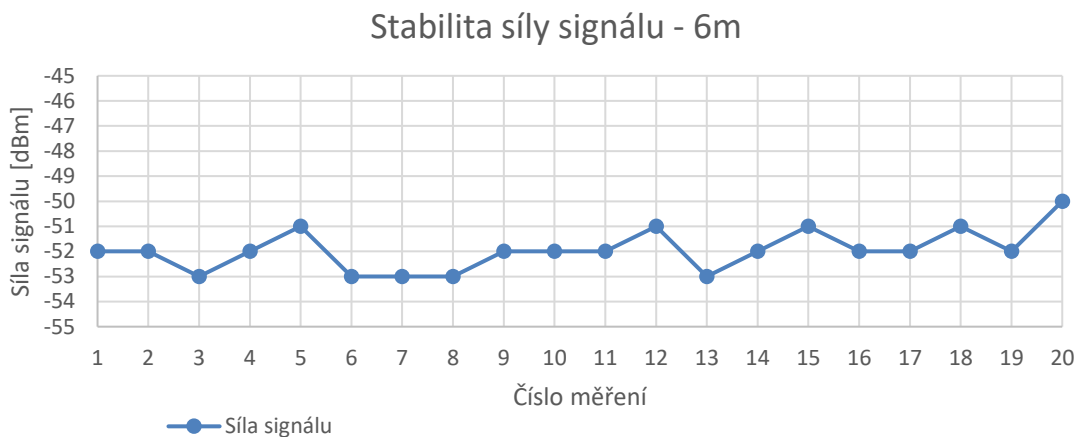
Graf 9.2 Stabilita síly signálu - 1m



Graf 9.3 Stabilita síly signálu - 3m



Graf 9.4 Stabilita síly signálu - 6m

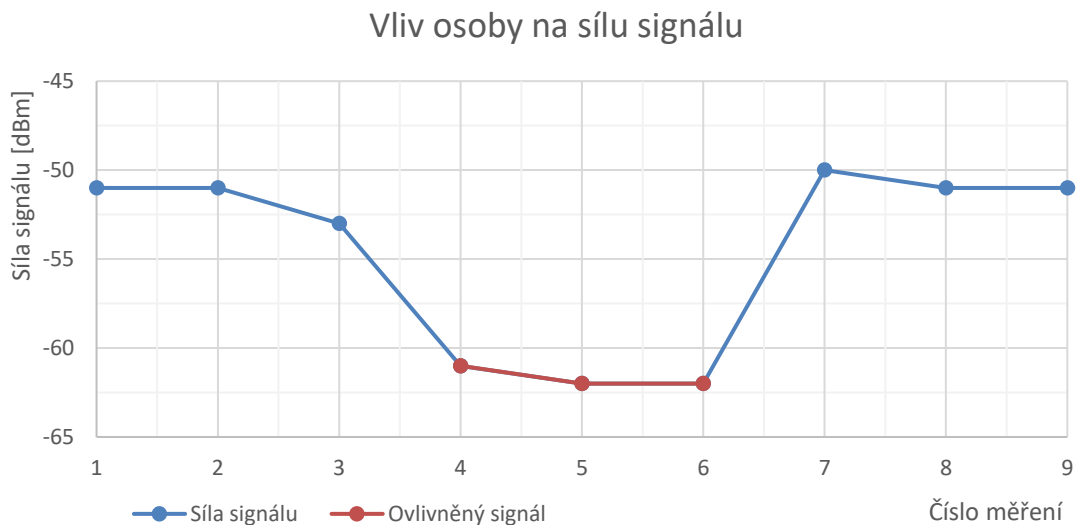


Výsledky měření ukazují, že signál se v daném bodě může lišit až o 3 dBm. Během měření však nebyl signál ovlivněn žádným dodatečným rušením. V běžném provozu proto budou tyto rozdíly mnohem vyšší.

#### 9.1.5.4 Vliv osoby na sílu signálu

Navrhovaná technologie má sloužit pro určování polohy osob. Při měření signálu může tedy dojít k zastínění signálu z jednoho či více AP osobou, jejíž poloha se bude určovat, nebo osobou pohybující v okolí. Z tohoto důvodu bylo otestováno, jaký vliv má na sílu signálu lidské tělo. Měření bylo provedeno opět s AP CANYON Wireless Broadband Router IEEE 802.11g MIMO, ve vzdálenosti 6 metrů. Tato vzdálenost byla zvolena na základě předchozího měření stability signálu, jenž se na vzdálenosti 6 metrů zdál nejstabilnější. Při měření bylo zaznamenáno devět po sobě jdoucích měření signálu klientem. Při 4., 5. a 6. měření síly signálu byl signál rušen postavením osoby mezi AP a klienta. Výsledek měření je vyobrazen na grafu graf 9.5.

Graf 9.5 Vliv osoby na sílu signálu



Měřením bylo zjištěno, že osoba ovlivní sílu signálu přibližně o 10,5 dBm. Z tohoto zjištění vyplývá, že určování polohy na základě síly signálu Wi-Fi se stává velmi nepřesné v případech, že se v prostoru mezi AP a klientem pohybují osoby.

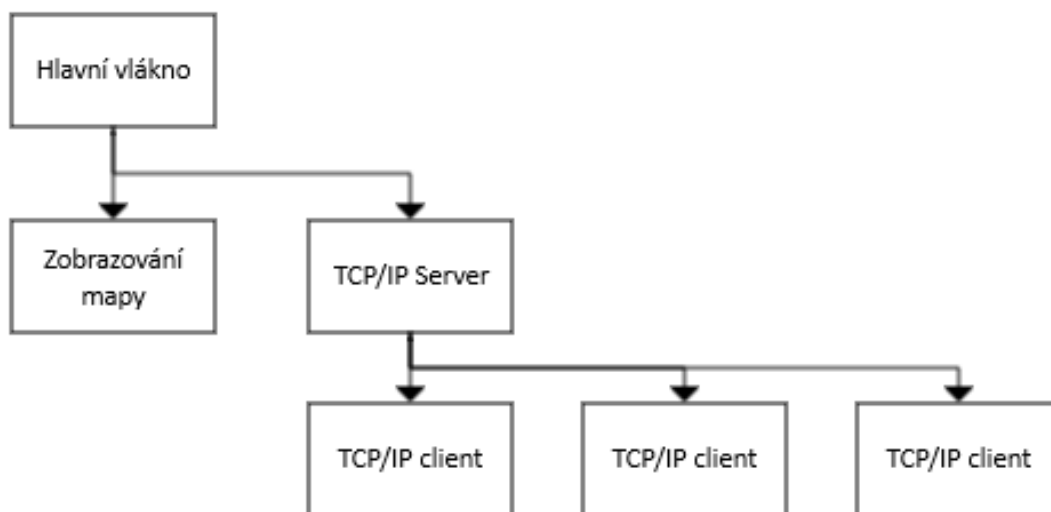
## 9.2 Vytvoření software

Poloha klienta bude zobrazována na monitorovací stanici (počítači) v lokální síti. Ta bude obsluhována dozorčí osobou. Za tímto účelem se práce věnuje vytvoření software, jenž obsahuje TCP/IP server pro komunikaci s klientem, uživatelské rozhraní zobrazující polohu klienta na mapě a algoritmus pro výpočet polohy klienta. Na základě předchozích testů byla zvolena triangulační metoda Analýza prostoru, jenž je popsána v kapitole 6.3. Tato metoda určuje polohu na základě předchozích naměřených hodnot v daných bodech. Jelikož signál Wi-Fi je velice náchylný na rušení, jeví se tato metoda v tomto případě jako nevhodnější. Při zavádění technologie v objektu je nejdříve provedena analýza signálu v klíčových bodech objektu. Následně je programem dopočítána mapa síly signálu pro každé monitorované AP.

### 9.2.1 Návrh software

Jelikož je k dispozici počítač s operačním systémem Windows a jedná se o jeden z nejrozšířenějších operačních systémů, bude software vytvořen pro tuto platformu. Z celé škály programovacích jazyků pro platformu Windows byl zvolen programovací jazyk C#, jenž umožňuje naprogramovat TCP/IP server a uživatelské rozhraní v rámci jednoho programu.

Program je vytvořen ve vývojovém prostředí Microsoft Visual Studio 2015, jako WPF (Windows Presentation Foundation) aplikace. V programu běží několik vláken najednou (viz obr. 9.20). Hlavní vlákno programu zobrazuje okno programu a reaguje na události uživatele, vedlejší časové vlákno pro pravidelnou aktualizaci zobrazení polohy klientů na mapě, vedlejší vlákno TCP/IP serveru, jež vytváří další vlákna programu v závislosti na počtu připojených klientů. Každý klient komunikuje s vlastním vláknem programu, aby byla zajištěna paralelní komunikace, při připojení více klientů.



Obr. 9.20 Schéma vláken programu [vlastní]



Program se skládá z následujících objektů:

Tab. 9.4 Seznam tříd

Název	Popis
<b>MainWindow</b>	Hlavní okno programu
<b>SettingWindow</b>	Okno s nastavením programu
<b>SignalWindow</b>	Okno pro měření signálu
<b>Server</b>	TCP/IP server
<b>Client</b>	TCP/IP client
<b>Map</b>	Mapa budovy
<b>SignalMap</b>	Mapa signálů
<b>Material</b>	Materiál zdi
<b>Wall</b>	Zed'
<b>Door</b>	Dveře
<b>Mlabel</b>	Text v mapě
<b>Signal</b>	Síla signálu v bodě
<b>PointGroup</b>	Skupina bodů
<b>Point</b>	Bod (x,y)

Návaznost jednotlivých objektů, jejich atributy a metody jsou vyobrazeny v diagramu tříd v příloze č.2. Tento diagram popisuje statickou strukturu systému, souvislost mezi objekty, jejich atributy a metody.

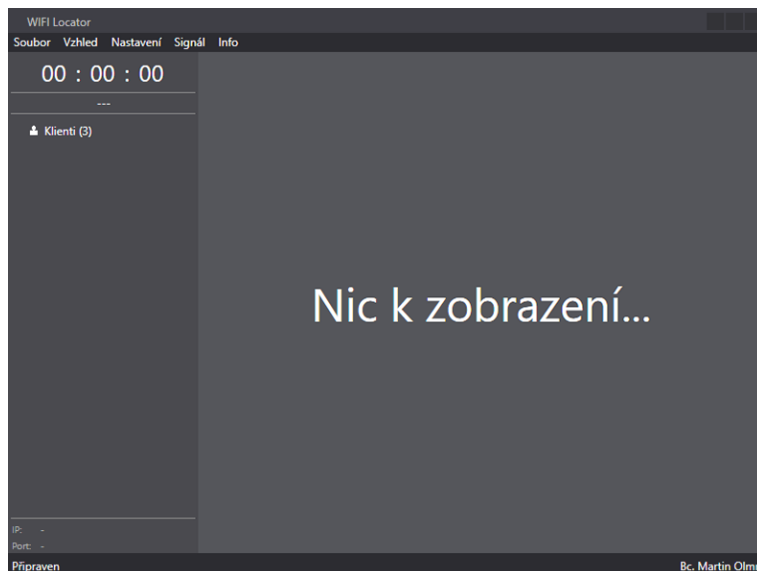
### 9.2.2 Programování software

Po založení nového projektu v Microsoft Visual Studio 2015, jenž byl nazván WifiLocator, se práce věnovala grafickému návrhu programu.

#### 9.2.2.1 Grafické rozhraní

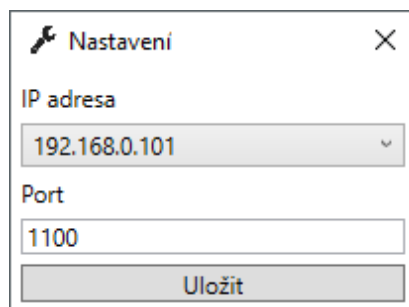
Nejdříve byla vytvořena grafická podoba hlavního okna programu, jež můžeme vidět na obr. 9.21. Okno obsahuje hlavní menu (horní lišta), hlavní plochu a patičku s informacemi o aktuálním dění a názvem autora. Hlavní plocha je rozdělena vertikálně na dvě části. V levé je aktuální čas, název mapy, seznam klientů a aktuální IP adresa a port, na němž je spuštěn TCP/IP server. V pravé části je umístěn Canvas, v němž se zobrazují

jednotlivé části mapy. Rozhraní programu je plně responsivní, tedy přizpůsobuje se jakémukoli rozlišení monitoru.



Obr. 9.21 Grafické rozhraní programu - hlavní okno [vlastní]

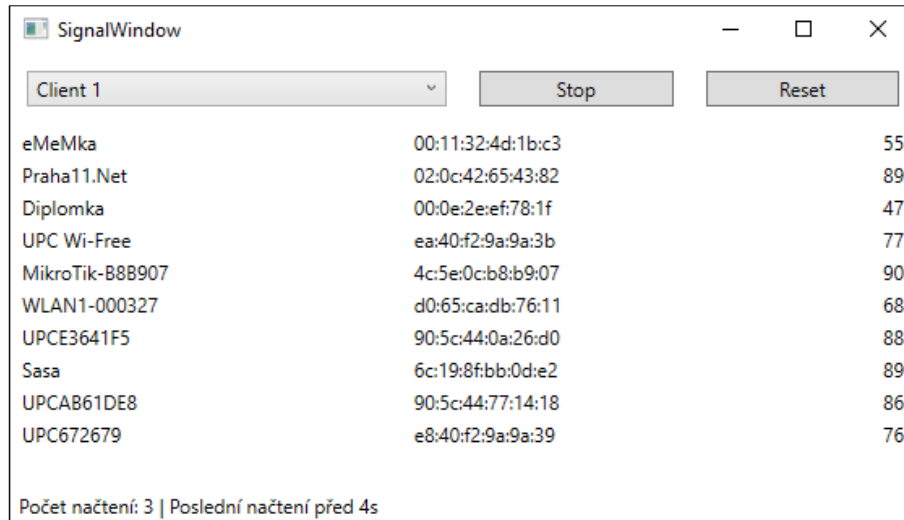
Okno nastavení programu (viz obr. 9.22) slouží k nastavení IP adresy a portu, na němž TCP/IP server běží.



Obr. 9.22 Grafické rozhraní programu - okno nastavení [vlastní]

Okno měření signálů (viz obr. 9.23) usnadňuje analýzu síly signálu a umožňuje zaznamenat klíčová data pro výpočet mapy síly signálů. Po připojení klienta k TCP/IP serveru a spuštění měření tlačítkem „Start“ dojde k zaznamenávání síly signálu

a MAC adresy dostupných AP. V okně se zobrazuje počet měření a počet sekund od posledního měření.



Client 1	MAC Adresa	Signál
eMeMka	00:11:32:4d:1b:c3	55
Praha11.Net	02:0c:42:65:43:82	89
Diplomka	00:0e:2e:ef:78:1f	47
UPC Wi-Free	ea:40:f2:9a:9a:3b	77
MikroTik-B8B907	4c:5e:0c:b8:b9:07	90
WLAN1-000327	d0:65:ca:db:76:11	68
UPCE3641F5	90:5c:44:0a:26:d0	88
Sasa	6c:19:8f:bb:0d:e2	89
UPCAB61DE8	90:5c:44:77:14:18	86
UPC672679	e8:40:f2:9a:9a:39	76

Počet načtení: 3 | Poslední načtení před 4s

Obr. 9.23 Grafické rozhraní programu - okno měření signálů [vlastní]

Zdrojové kódy jsou uloženy v příloze na CD.

### 9.2.2.2 TCP/IP server

Server je naprogramován tak, aby se spustil automaticky při spuštění programu. Program implicitně použije první IPv4 adresu v seznamu IP adres, jenž předá operační systém. Port je přednastaven na hodnotu 1100. Pokud dojde v okně nastavení ke změně IP adresy či portu, dojde k automatickému restartu serveru.

Třída *Server* obsahuje veřejnou metodu *Run*, jež je volána vedlejším vláknem programu. Před vytvořením vedlejšího vlákna serveru je vytvořena instance objektu *Server* a nastaveny atributy *ip* (IP adresa) a *port*. Kód vytvoření vlákna:

```
server = new Server();
server.ip = this.ip;
server.port = this.port;
serverThread = new Thread(server.Run);
serverThread.IsBackground = true;
serverThread.Start();
```

Při zavolání metody *Run* je do veřejné proměnné *Clients* uložen prázdný *List*, jenž slouží k uchování objektů typu *Client*. Hlavní vlákno programu přistupuje k této proměnné a v uživatelském okně zobrazuje seznam aktuálně připojených klientů. Následně je vytvořen serverový *Socket*. Počet slotů pro připojení klientů je nastaven na 16. Kód vytvoření serverového Socketu:

```
serverSocket = new Socket(  
    AddressFamily.InterNetwork,  
    SocketType.Stream,  
    ProtocolType.Tcp  
);  
serverSocket.Bind(new IPEndPoint(this.ip, this.port));  
serverSocket.Listen(16);
```

Po spuštění serverového Socketu je spuštěna smyčka, jež běží po celou dobu běhu serveru. Smyčka čeká na připojení nového klienta prostřednictvím TCP protokolu. Jakmile se klient připojí, dojde k vytvoření nového vlákna pro komunikaci serveru s klientem. Po vytvoření je vlákno spuštěno, smyčka se vrací na začátek a čeká na nové připojení. Kód smyčky:

```
while (running)  
{  
    Console.WriteLine("Waiting on connection");  
    Socket clientSocket = serverSocket.Accept();  
    Console.WriteLine("New connection");  
    Thread t = new Thread(() => clientListener(clientSocket));  
    t.IsBackground = true;  
    int index = clientThreads.Count;  
    clientThreads.Insert(index, t);  
    clientThreads[index].Start();  
}
```

Vlákno klienta přijímá pomocí nekonečné smyčky jednotlivé přenášené zprávy. Obsah těchto zpráv je přenášen jednotlivými byty. Ty jsou pomocí následujícího kódu převedeny na řetězec (*String*):

```
byte[] idata = new byte[clientSocket.SendBufferSize];  
int j = clientSocket.Receive(idata);  
Console.WriteLine("New data");  
byte[] buf = new byte[j];  
for (int i = 0; i < j; i++)  
    buf[i] = idata[i];  
string data = Encoding.Default.GetString(buf);
```

Přijatá zpráva je následně otestována pomocí regulárního výrazu, zda odpovídá vzoru. Vzor zprávy, jež odesílá zkonstruovaný klient, byl popsán v kapitole 9.1.4. Pokud zpráva odpovídá vzoru, tak je ze zprávy vyseparováno ID zařízení a seznam signálů.

```
string pattern = @"^(?<id>[0-9]+\)\[(?<msg>[^\]]+\)\]$";
Regex r = new Regex(pattern, RegexOptions.IgnoreCase);
Match m = r.Match(data);
if (m.Success) {
    //parsování ID zařízení
    string c = m.Groups["id"].Value;
    int id = int.Parse(c);

    //parsování seznamu signálu
    string msg = m.Groups["msg"].Value;
}
```

Po získání ID zařízení je zkontrolován seznam klientů, zda klient není připojen pod jiným vláknem. V případě, že klient navázal nové připojení pod novým vláknem, je původní vlákno ukončeno. Pokud se jedná o připojení nového klienta, je vytvořen nový objekt *Client*, jenž je následně přidán do seznamu připojených klientů.

```
int listindex = 0;
foreach (Client client in Clients) {
    if (client.Id == id) {
        index = listindex;
        break;
    }
    listindex++;
}
if(index < 0) {
    int i = id - 1;
    Client client = new WifiLocator.Client(
        id,
        clientNames[i],
        clientColors[i],
        0,0
    );
    index = Clients.Count;
    Clients.Insert(index, client);
}
```

Po získání příslušného objektu klienta je zavolána veřejná metoda *parseMessage* tohoto objektu. Tato metoda uloží aktuální čas, jenž reprezentuje čas příjmu nových dat, a nastaví hodnotu atributu *newData* na *true*, což znamená, že z těchto dat zatím nebyla určena pozice klienta. Dále jsou pak pomocí regulárních výrazů vyčteny jednotlivé síly

signálů a MAC adresy ze zprávy. Pro každý aktuálně dostupný AP vyčtený ze zprávy je vytvořen objekt *Signal*, jenž uchovává MAC adresu AP, aktuální sílu signálu a SSID.

```
public void parseMessage(string msg) {
    this.time = DateTime.Now;
    this.newData = true;
    this.signals = new List<Signal>();
    string[] hotspots = Regex.Split(msg, ";");
    foreach (string hotspot in hotspots) {
        string pattern = @"^(?<ssid>[^\(]+)\((?<msg>[^\)]+\)$";
        Regex r = new Regex(pattern, RegexOptions.IgnoreCase);
        Match m = r.Match(hotspot);
        if (m.Success)
        {
            string[] data = Regex.Split(m.Groups["msg"].Value, ",");
            List<string> dataList = new List<string>();
            foreach (string x in data) {
                dataList.Add(x);
            }
            if(dataList.Count == 4)
            {
                string ssid = m.Groups["ssid"].Value;
                int strenght = Math.Abs(int.Parse(dataList[1]));
                string mac = dataList[2];
                Signal signal = new Signal(mac, strenght, ssid);
                signals.Add(signal);
            }
        }
    }
}
```

### 9.2.2.3 Mapa a zobrazení

Při spuštění programu je vytvořeno vedlejší časové vlákno, jež každých 100ms volá veřejnou metodu hlavního okna *Display*. Tato metoda aktualizuje seznam připojených klientů dle seznamu klientů v objektu *Server*:

```
treeClients.Items.Clear();
treeClientsLabel.Content = "Klienti (" + server.Clients.Count.ToString() + ")";
List<Client> clients = server.Clients;
foreach (Client client in clients) {
    ... skrytý kód ...
}
```

Dále se zkontroluje, zda již byl načten zdrojový soubor mapy. Pokud ano, je zavolána veřejná metoda *Display* objektu mapy a dle polohy kurzoru jsou dopočítány souřadnice na mapě, na něž kurzor ukazuje. Pokud ne, je zobrazen nápis „Nic k zobrazení“.

```
if (this.map != null)
{
    if (this.map.isDisplay()){
        overlay.Visibility = Visibility.Collapsed;
        mapWindow.Children.Clear();
        Canvas canvas = new Canvas();
        if (showMousePosition) {
            double x = Math.Round(
                (MousePosition.X - this.map.posunX) / this.map.Meritko
            );
            double y = Math.Round(
                (MousePosition.Y - this.map.posunY) / this.map.Meritko
            );
            labelStatus.Content = "X: " + x.ToString() + " | Y: " + y.ToString();
        }
        this.map.display(this.mapWindow, canvas, server.Clients);
        mapWindow.Children.Add(canvas);
    }else{
        labelOverlay.Content = "Nic k zobrazení...";
        overlay.Visibility = Visibility.Visible;
    }
}
```

Po spuštění programu není načtena žádná implicitní mapa. Tu je potřeba načíst kliknutím na tlačítko „Načíst mapu“ v horním menu programu. Po kliknutí na toto tlačítko je zobrazeno dialogové okno pro výběr souboru. Dále je uživateli zobrazen text informující o načítání mapy. Je vytvořen nový objekt *Map* s parametrem obsahující cestu a název souboru mapy, jenž se má načíst.

```
Microsoft.Win32.OpenFileDialog dlg = new Microsoft.Win32.OpenFileDialog();
dlg.DefaultExt = ".map";
dlg.Filter = "Map Files (*.map)|*.map";

Nullable<bool> result = dlg.ShowDialog();
if (result == true){
    labelOverlay.Content = "Načítání mapy...";
    overlay.Visibility = Visibility.Visible;
    string filename = dlg.FileName;
    if (this.map == null)
        this.map = new Map(filename);
    else{
        this.map.loadMap(filename);
    }
    mapName.Content = this.map.Name;
}
```

Pro uchování informací o mapě jsem zvolil textový soubor s koncovkou „map“. Obsah toho formátu má strukturu JSON, jenž umožňuje snadné načítání informací ze souboru. Soubor uchovává rozměry mapy, seznam a polohu zdí, dveří a nápisů zobrazených na mapě. Dále pak obsahuje seznam AP a informace o síle signálu v klíčových bodech mapy, z nichž je následně vypočítána mapa signálů. Obsah souboru obsahující testovací mapu:

```
{
  "name": "TEST",
  "width": 2000,
  "height": 1000,
  "materials": [
    {"id": "1", "name": "Beton", "color": "#000000"},
    {"id": "2", "name": "Sádrokarton", "color": "#0000FF"},
    {"id": "3", "name": "Dřevo", "color": "#00FF00"},
    {"id": "4", "name": "Cihla", "color": "#FF0000"}
  ],
  "walls": [
    {"material": 1, "depth": 10, "x1": 0, "y1": 0, "x2": 2000, "y2": 0},
    {"material": 2, "depth": 10, "x1": 2000, "y1": 0, "x2": 2000, "y2": 1000},
    {"material": 3, "depth": 10, "x1": 0, "y1": 1000, "x2": 2000, "y2": 1000},
    {"material": 4, "depth": 10, "x1": 0, "y1": 0, "x2": 0, "y2": 1000}
  ],
  "labels": [
    {"text": "Testovací zobrazení mapy", "size": 96, "color": "#CCCCCC", "x": 500, "y": 500}
  ],
  "doors": [
    {"x2": 100, "y2": 100, "xc": 200, "yc": 100, "x1": 200, "y1": 200}
  ],
  "signals": [
    {
      "mac": "00:11:32:4d:1b:c3",
      "ssid": "Diplomka",
      "points": [
        {"x": 0, "y": 0, "signal": 70},
        {"x": 250, "y": 0, "signal": 60},
        {"x": 580, "y": 0, "signal": 54},
        {"x": 100, "y": 450, "signal": 54}
      ]
    }
  ]
}
```

Objekt *Map* při vytváření instance a předání názvu souboru načte obsah daného souboru. Tento obsah je následně převeden na dynamická data pomocí funkce `JsonConvert.DeserializeObject(content)`. Tato funkce umožní pracovat s obsahem textového souboru ve formátu JSON jako s objektem. Při zpracovávání dat jsou vytvářeny jednotlivé objekty mapy: `Material`, `Wall`, `Door`, `Mlabel`. Poloha těchto objektů na mapě je v textovém souboru uváděna v centimetrech. Kód načítání mapy je umístěn v příloze na CD.



Na základě načtených informací o mapě je vypočítáno měřítko zobrazení mapy. Toto měřítko je závislé na aktuální velikosti okna pro zobrazení mapy a při každém volání metody *Display* je přepočítáno tak, aby se mapa vždy zobrazila celá. Kód výpočtu měřítka:

```
this.Meritko = 1;

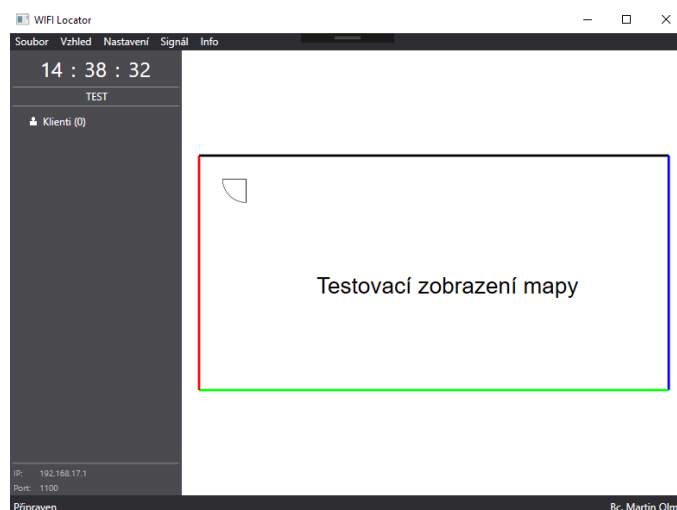
//velikost okna
double windowHeight = window.ColumnDefinitions[0].ActualWidth;
double windowHeight = window.RowDefinitions[0].ActualHeight;

posunX = 20; //posun mapy od okraje okna X
posunY = 20; //posun mapy od okraje okna Y

//výpočet měřítka pro souřadnici X a Y
double m1 = Math.Floor(((windowWidth - (posunX * 2)) / this.Width) * 1000) / 1000;
double m2 = Math.Floor(((windowHeight - (posunY * 2)) / this.Height) * 1000) / 1000;

//určení finálního měřítka
if (m1 < m2) {
    this.Meritko = Math.Abs(m1);
    posunY += (((m2 * this.Height) - (m1 * this.Height)) / 2);
}else if (m1 > m2){
    this.Meritko = Math.Abs(m2);
    posunX += (((m1 * this.Width) - (m2 * this.Width)) / 2);
}else{
    this.Meritko = Math.Abs(m1);
}
}
```

Po výpočtu aktuálního měřítka je zavolána metoda *Display* každého objektu, jenž mapa obsahuje. Zároveň je této metodě předáno aktuální měřítko mapy, posun v ose X a Y. Zdrojový kód těchto objektů včetně metody *Display* je umístěn v příloze na CD. Zobrazení testovací mapy vidíme na následujícím obrázku:



Obr. 9.24 Zobrazení testovací mapy [vlastní]

Pro snadnější analýzu síly signálu v monitorovaném prostoru bylo vytvořeno okno pro měření aktuální síly signálu přijaté klientem. Po kliknutí na tlačítko „Start“ je zahájen záznam dat. Dostupné AP a síly signálu jsou zobrazovány v tabulce. Při opakovaném příjmu síly signálu na dané AP jsou všechny předchozí hodnoty zprůměrovány a v tabulce je zobrazena průměrná hodnota síly signálu na dané AP. Tyto hodnoty jsou následně přeneseny do souboru mapy, aby bylo možné vypočítat mapu pokrytí signálem. Pro jednodušší získání aktuálních souřadnic klienta, které je potřeba zapsat do souboru k síle signálu, slouží zobrazení souřadnic, na něž ukazuje kurzor na mapě. Zdrojový kód okna pro měření síly signálu je umístěn v příloze na CD.

### 9.2.3 Mapa síly signálu a algoritmus určování polohy klienta

Při vývoji byl algoritmus pro určování polohy několikrát upravován a laděn tak, aby bylo určování polohy co nejpřesnější. Nyní bude uvedena konečná podoba tohoto algoritmu.

Při aktualizaci zobrazení mapy metodou *Display* jsou převzaty objekty typu *Client* z objektu *Server*. Program projde všechny tyto objekty a zkontroluje atribut *newData*. Pokud je hodnota tohoto atributu nastavena na *true*, znamená to, že je potřeba určit novou polohu klienta. Dojde tedy k zavolání veřejné metody *calculatePosition* objektu *Client*. Tato metoda obsahuje algoritmus pro určení polohy a při volání této metody je předáván list objektů *SignalMap*.

Počet objektů *SignalMap* je stejný jako počet sledovaných AP. Pro každé AP je tedy vytvořena mapa reprezentující pokrytí prostoru signálem tohoto AP. Instance těchto map jsou vytvářeny při načítání mapy ze souboru. Objekt obsahuje matici  $m \times n$  s názvem *Signals*, jež reprezentuje síť bodů s hustotou 1x1 metr a velikostí dle rozměrů načtené mapy. Např. pokud načítáme mapu 7x5 metrů je velikost matice 7x5. Hustota 1x1 metr byla stanovena na základě předběžných testů, jež jsou uvedeny v kapitole 9.1.5. Z těchto testů vyplývá, že rozdíly v síle signálu na jednom metru jsou minimální. Především jsou tyto

rozdíly menší než případný rozdíl při rušení signálu osobou či jiném proměnlivém rušení, jak ukázaly testy stability signálu a test vlivu osoby na sílu signálu.

Při načítání mapy jsou do matice ukládány známé síly signálů ve známých bodech. Vedle této matice je vytvořena druhá o stejné velikosti. Tato matice se nazývá *lockSignals* a obsahuje pouze nuly a jedničky. Na stejné pozice, na něž je při načítání uložena známá síla signálu do matice *Signals*, je uložena do matice *lockSignals* hodnota 1. Tím dojde k uzamčení hodnoty v tomto bodě a hodnota nebude změněna při následujícím výpočtu síly signálu.

Po naplnění matice *Signals* známými hodnotami je zavolána veřejná metoda *calculateSignals*. Úkolem této metody je dopočítat sílu signálu v neznámých bodech. Metoda obsahuje algoritmus, navržený v rámci této práce. Tento algoritmus pracuje s naměřenými hodnotami v matici, poloha AP není známa. Algoritmus prochází matici *Signals* po řádcích. V každé buňce matice se pokusí vyhledat známou sílu signálu horizontálně, vertikálně i diagonálně. Pokud sílu signálu nenalezne, buňku přeskočí a pokračuje další. K této buňce se vrátí při dalším průchodu maticí. Pokud např. horizontálně nalezne známou hodnotu nalevo i napravo od aktuální buňky, spočítá počet buněk mezi známými hodnotami a rozdíl těchto hodnot rozdělí do buněk mezi těmito hodnotami. Stejný systém platí o pro vertikální a diagonální vyhledávání. Pokud aktuální buňka obsahuje již známou hodnotu, tato hodnota není uzamčena v matici *lockSignals* a jsou známy všechny okolní hodnoty, je hodnota této buňky přepsána průměrnou hodnotou vypočtenou z okolních buněk.

Procházení maticí se opakuje tak dlouho, dokud dochází ke změně nějaké hodnoty v matici. Aby se zamezilo nekonečnému výpočtu, je cyklus přerušen v případě, že ani po stém průchodu maticí nebylo dosaženo konstantních hodnot. Při testovacím výpočtu mapy bylo u mapy o rozměrech 10 x 10 metrů a známém signálu ve čtyřech bodech dosaženo konstantních hodnot při prvním průchodu. U mapy o rozměrech 1000 x 1000 metrů a známém signálu ve čtyřech bodech bylo dosaženo konstantních

hodnot při třetím průchodu. Přerušeni výpočtu po 100 průchodech je tedy dostatečné. Zdrojový kód výpočtu mapy síly signálu je umístěn v příloze na CD.

Takto vypočtené mapy pokrytí jsou předávány metodě *calculatePosition* objektu *Client*. Algoritmus prochází objekty *SignalMap* a na každém objektu volá veřejnou metodu *getPoints*. Zároveň této metodě předává aktuální sílu signálu na AP, jemuž náleží daná mapa signálu a hodnotu tolerance signálu. Tato tolerance je nastavena na hodnotu nula. Pokud se při prvním získávání možných pozic klienta nezíská dostatečný počet možných bodů, je tato tolerance navýšena o 1 a celý proces určování možných bodů klienta se opakuje.

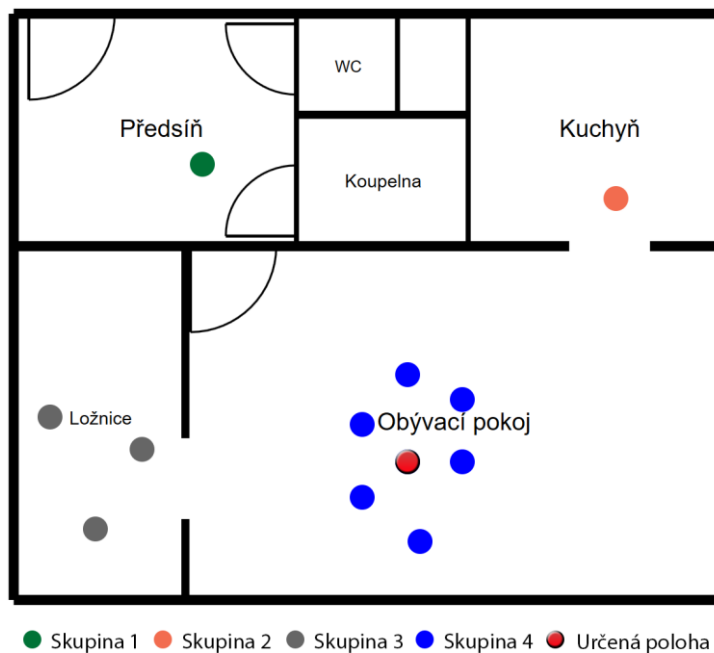
Metoda *getPoints* vrátí seznam bodů (objektů *Point*), jež odpovídají naměřené síle signálu. Takto jsou získány všechny body napříč mapami signálů, v nichž se může klient nacházet.

```
//signal pro danou mapu...
List<Point> sp = sm.getPoints(s.Strenght, tolerance_signal);
```

Algoritmus následně rozdělí získané body do skupin (*pointGroup*). Skupiny seskupují body v okruhu tří metrů od středního bodu skupiny. Nad každou skupinou je při vkládání bodu volána metoda *canBeAdd*, jež vrátí *true* v případě, že bod do dané skupiny patří. V případě, že bod nepatří do žádné skupiny, je vytvořena nová skupina obsahující tento bod. Grafické znázornění vidíme na obr. 9.25.

Kód funkce *canBeAdd*:

```
private bool canBeAdd(Point p) {
    Point ap = getAverangePoint(); //vrací střední bod skupiny
    if (
        p.X > ap.X - tolerance
        && p.X < ap.X + tolerance
        && p.Y > ap.Y - tolerance
        && p.Y < ap.Y + tolerance
    )
        return true;
    return false;
}
```



Obr. 9.25 Grafické znázornění rozdělení bodů do skupin a určení polohy klienta [vlastní]

Každý bod ve skupině navyšuje váhu skupiny o 1. Předpokládá se, že klient se nachází poblíž většiny bodů, tedy poblíž skupiny s největší vahou. Algoritmus vypočte střední bod skupiny bodů a prohlásí jej za aktuální přibližnou polohu klienta. Kód funkce *getAveragePoint*, jenž vrátí střední bod skupiny:

```
public Point getAveragePoint() {
    if (points.Count == 0) //pokud je počet bodů ve skupině roven 0 vrátí null
        return null;
    int x = 0;
    int y = 0;
    //procházení bodů
    foreach (Point p in points) {
        x += p.X;
        y += p.Y;
    }
    //zaokrouhlení na celé centimetry
    x = (int)Math.Round((decimal)x / points.Count);
    y = (int)Math.Round((decimal)y / points.Count);
    return new Point(x, y); //vrácení nového bodu
}
```

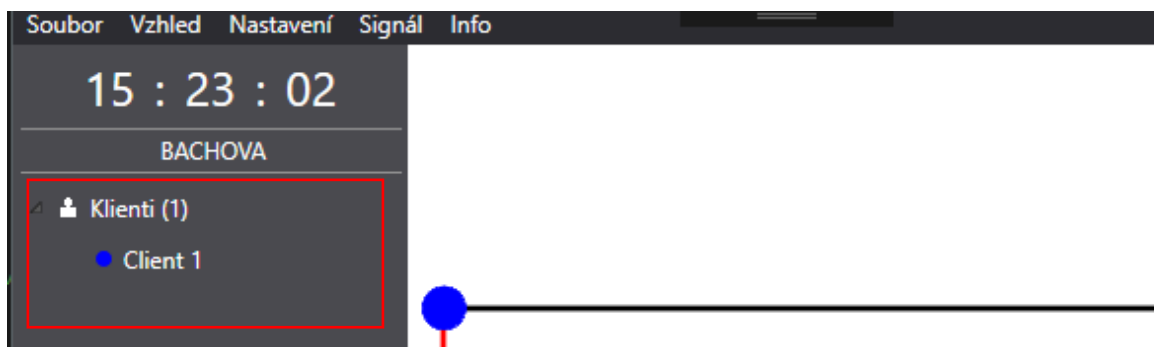
Tento bod je objektem *Client* uložen do proměnné *Position*. Při volání metody *Display* objektu *Client* dojde k zobrazení klienta na mapě v tomto bodě. Kompletní kód algoritmu pro určování polohy je umístěn v příloze na CD.

### 9.3 Základní testy

Po naprogramování softwaru bylo provedeno testování v testovacím bytě. Otestovala se komunikace mezi naprogramovaným software a zkonstruovaným hardware, výpočet map signálů a určování polohy klienta.

#### 9.3.1 Test komunikace Server – Klient

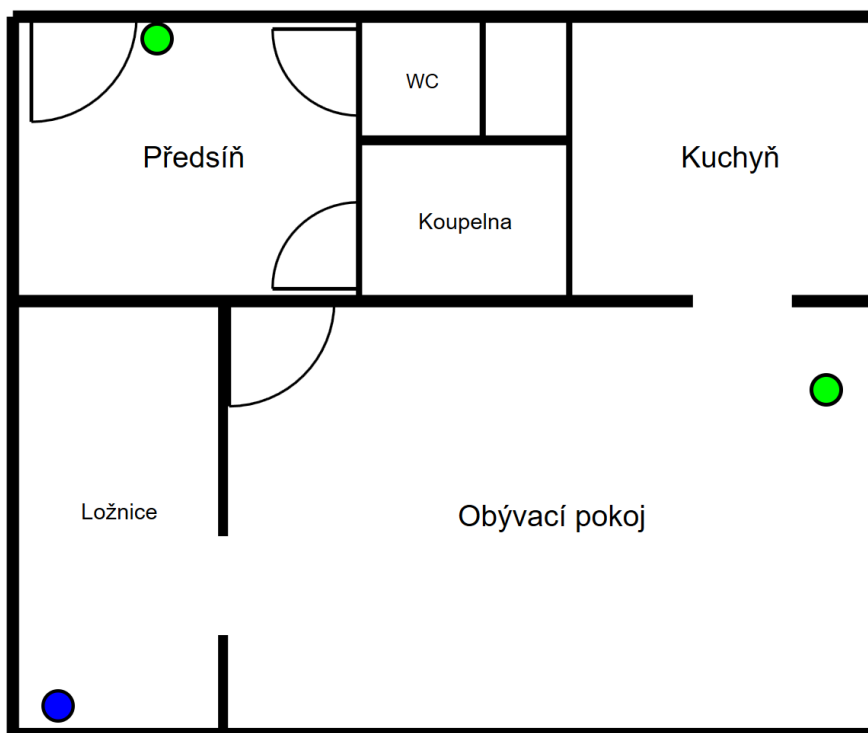
Klient je naprogramován tak, aby se po spuštění automaticky připojil na Wi-Fi síť s SSID Diplomka. Za tímto účelem byl spuštěn AP, jenž vysílá tuto síť. Součástí AP je router, na němž je spuštěn DHCP server. Do této sítě byl také připojen počítač, na němž je bude spuštěn vytvořený program WiFiLocator. V počítači byl vypnut firewall, aby nedocházelo k blokování příchozí komunikace. Po připojení počítače do sítě a přidělení IP adresy byl spuštěn program WiFiLocator. V nastavení programu byla vybrána aktuální IP adresa a nastaveno číslo portu na 1100. Poté byla v programu načtena testovací mapa a spuštěno zařízení klienta. Klient se úspěšně připojil do Wi-Fi sítě a získal IP adresu od DHCP serveru. Tato operace trvala přibližně 3 sekundy. Po přidělení IP adresy se téměř okamžitě připojil k TCP serveru, jenž běžel v programu WiFiLocator. Po deseti sekundách klient načel síly signálů dostupných AP a zprávu odeslal. Program zprávu úspěšně obdržel. Zpráva byla testováním pomocí regulárního výrazu prohlášena za validní a ze zprávy bylo zjištěno číslo klienta. Klient měl ID 1 a byla mu přiřazena modrá barva a název „Client 1“. Klient se úspěšně zobrazil v seznamu připojených klientů a na mapě (viz obr. 9.26).



Obr. 9.26 WiFiLocator - Test připojení klienta [vlastní]

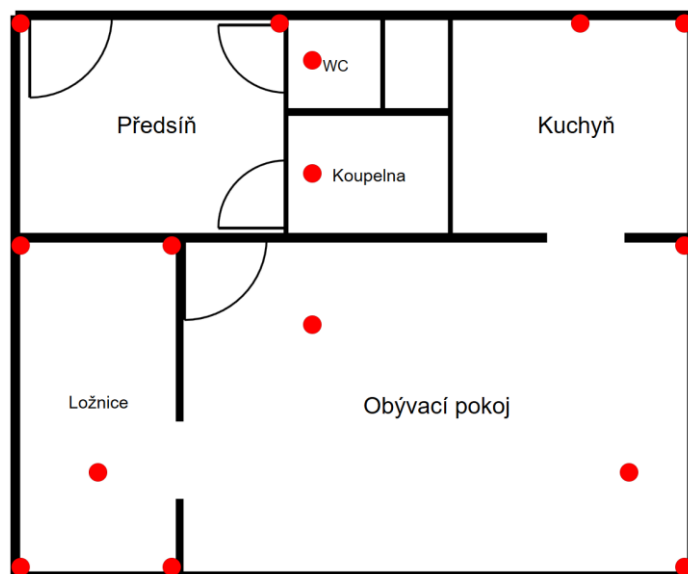
### 9.3.2 Test výpočtu map signálu

Při tomto testu byla vytvořena mapa testovacího bytu. Rozměr celkové plochy bytu je 7 x 5,8 metru. V bytě byly rozmístěny 3 Access Pointy. První byl umístěn do předsíně. Jedná se o zařízení CANYON Wireless Broadband Router IEEE 802.11g MIMO. Tento AP vysílá Wi-Fi Diplomka (2,4 GHz, protokol IEEE 802.11g), jež slouží pro komunikaci mezi klientem a serverem. Druhý AP byl umístěn v obývacím pokoji. Jednalo se o zařízení Synology RT1900ac. Tento AP vysílal síť eMeMka (2,4 GHz, protokol IEEE 802.11g). Jako třetí byl použit mobilní telefon Samsung Galaxy S4 mini, na němž byl spuštěn mobilní hotspot vysílající Wi-Fi síť ememka (2,3 GHz, protokol IEEE 802.11g). Grafické znázornění umístění AP je na následujícím obrázku:



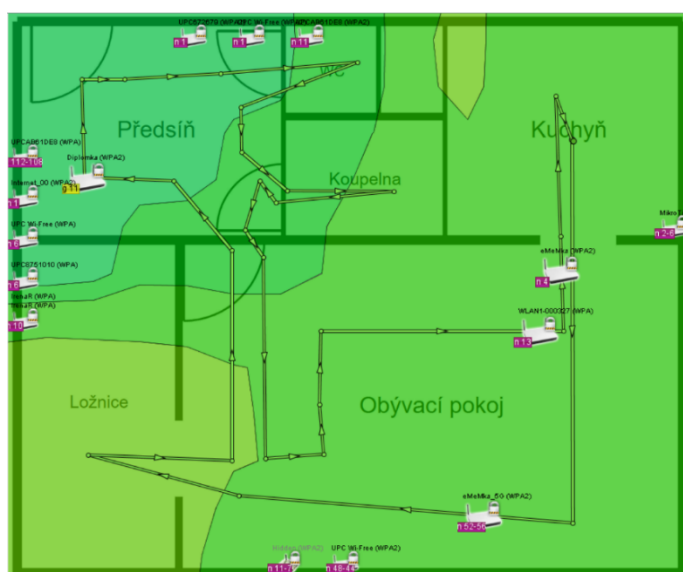
Obr. 9.27 Mapa rozmístění AP – Testovací byt [vlastní]

Následně byla měřena síla signálu v patnácti místech testovacího bytu. Tyto body jsou znázorněny červeně na obr. 9.28.



Obr. 9.28 Mapa bodů měření síly signálu – Testovací byt [vlastní]

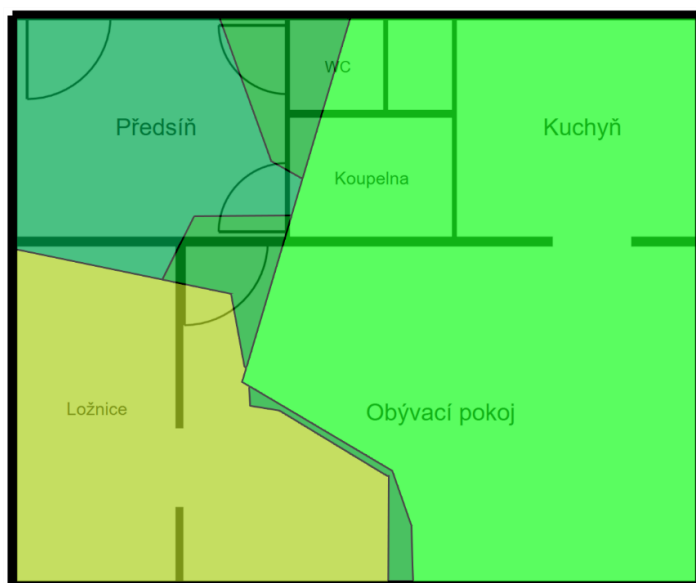
Naměřené údaje byly vloženy do souboru s mapou. Tato mapa byla načtena do programu WifiLocator. Program vypočítal mapy pokrytí signálem za 0,13s. Pro ověření správnosti výpočtu byl použit program od firmy Ekahaou. Do programu se nahraje obrázek reprezentující mapu objektu. Následně se s přijímačem projde objektem a cesta se zaznamenává do mapy. Program sám dopočítá pokrytí signálem. Výsledek, jenž je na obr. 9.29, je ovlivněn okolními Wi-Fi signály ze sousedství.



Obr. 9.29 Mapa pokrytí – Ekahaou [vlastní]



Pro porovnání byl vypsán obsah matic reprezentující mapu pokrytí do konzole programu WiFiLocator. Číselné hodnoty byly převedeny do grafické podoby. Obrázky reprezentující pokrytí signálem, jenž vypočítal navržený algoritmus, jsou umístěny v příloze na CD. Následně byl vytvořen průnik sil signálů od jednotlivých AP, aby se napodobila grafická podoba výstupu z programu od firmy Ekahaou. Výsledek reprezentující mapu pokrytí vypočítanou vytvořeným programem je zobrazen na následujícím obrázku:



Obr. 9.30 Mapa pokrytí – WiFiLocator [vlastní]

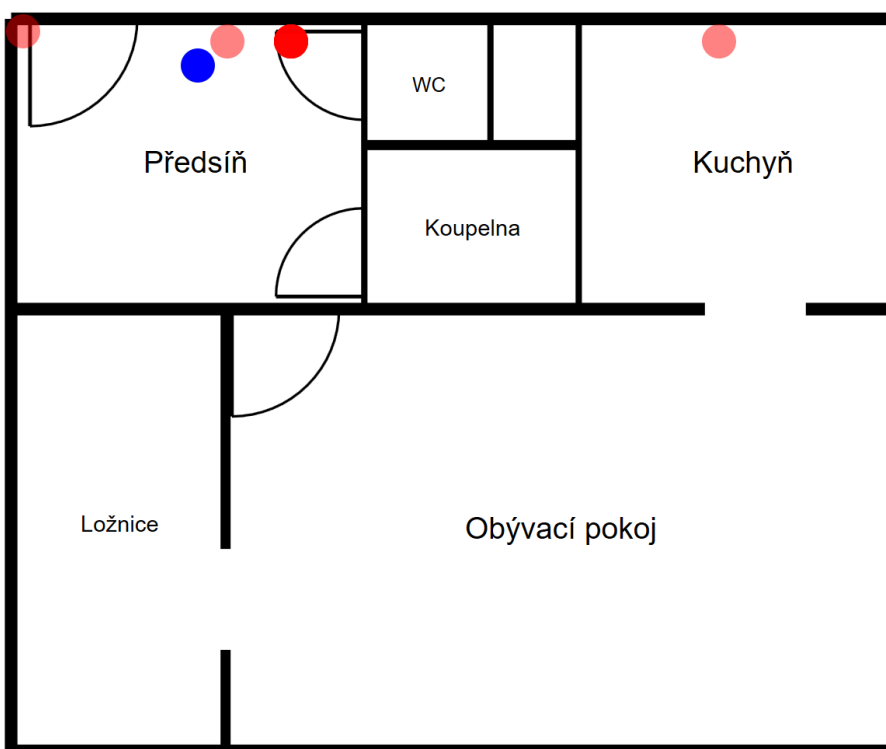
Porovnáním těchto dvou grafických znázornění pokrytí prostoru signálem vyplynulo, že navržený algoritmus pro výpočet mapy pokrytí pracuje správně a výsledek odpovídá skutečnosti.

### 9.3.3 Test určování polohy klienta

Po ověření správnosti výpočtu map síly signálu byla otestována technologie v testovacím bytě. Rozložení AP a měřené body zůstaly stejné jako v předešlém testu.

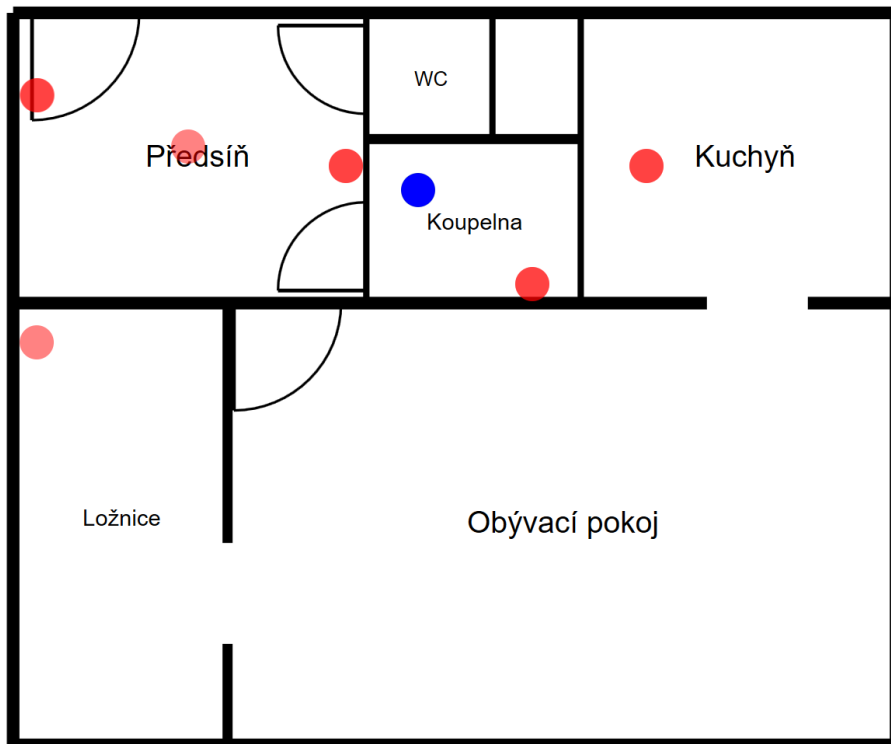
Testování bylo provedeno v každé místnosti bytu. Celkem jsem tedy provedl šest testů určování polohy. Každý test se skládal z deseti po sobě jdoucích určení polohy.

Testováním bylo zjištěno, že určování polohy je nejpřesnější v místech, kdy se klient nachází v blízkosti jednoho z monitorovaných AP, např. předsíni. Výsledek měření v této místnosti je zobrazen na následujícím obrázku, přičemž modře je označena skutečná poloha klienta, červeně určené polohy klienta. Sytost červeného puntíku odpovídá počtu určení polohy v daném bodě. Tzn., že v bodě, kde byla určena poloha 3x, je tmavší červený puntík než v bodě, kde byla poloha určena pouze jednou. Stejný princip zobrazení je aplikován na všechny výsledky měření, jenž jsou umístěny v příloze na CD.



Obr. 9.31 Výsledek měření – Testovací byt (předsíň) [vlastní]

Naopak nejhorších výsledků je dosaženo v místech, kde dochází k velkému rušení a signál je minimální. V tomto případě se jednalo o koupelnu, jejíž tři stěny jsou tvořeny sádkartonem a čtvrtá 10 cm tlustou betonovou zdí. Tyto dva materiály tvoří pro signál Wi-Fi velkou překážku. Výsledek určování polohy vidíme na obr. 9.32.



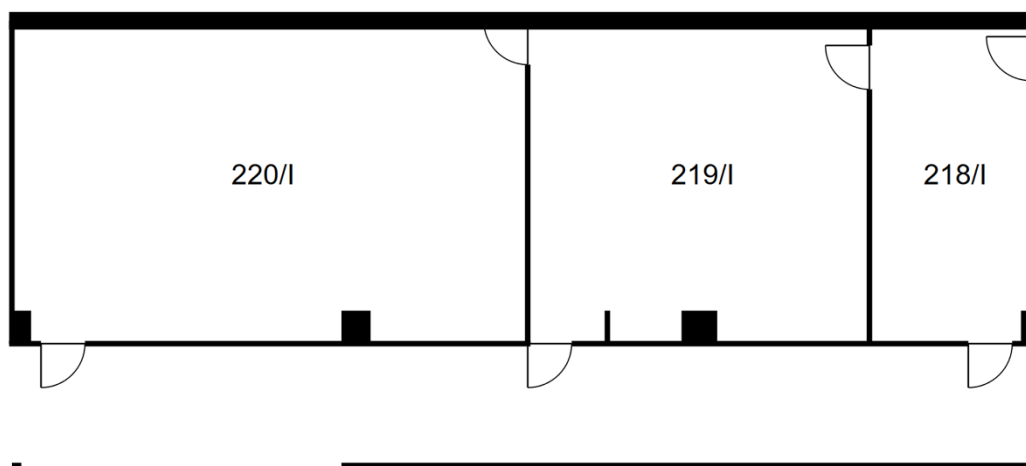
Obr. 9.32 Výsledek měření – Testovací byt (koupelna) [vlastní]

Z testování vyplývá, že pokud je klientem přijímán nerušený signál, je algoritmus schopen určit jeho polohu a je připraven na ověření v poloprovozních podmínkách.

## 10 Ověření v poloprovozních podmínkách

Ověření funkčnosti vytvořené technologie se provedlo ve školních prostorech. K dispozici jsem měl učebny 219/I, 220/I a kancelář 218/I v druhém patře prvního bloku Technické fakulty České zemědělské univerzity v Praze.

Školou byl poskytnut PDF dokument obsahující technický výkres budovy školy. Na základě získaných rozměrů z tohoto dokumentu byla zpracována mapa pro vytvořený program WiFiLocator znázorňující oblast testování, tedy výše uvedené učebny, kancelář a chodbu před těmito místnostmi. Celkové rozměry mapy jsou 18,6 x 8,1 m. Kód souboru mapy je uveden v příloze na CD. Grafické zobrazení mapy programem WiFiLocator je na následujícím obrázku:



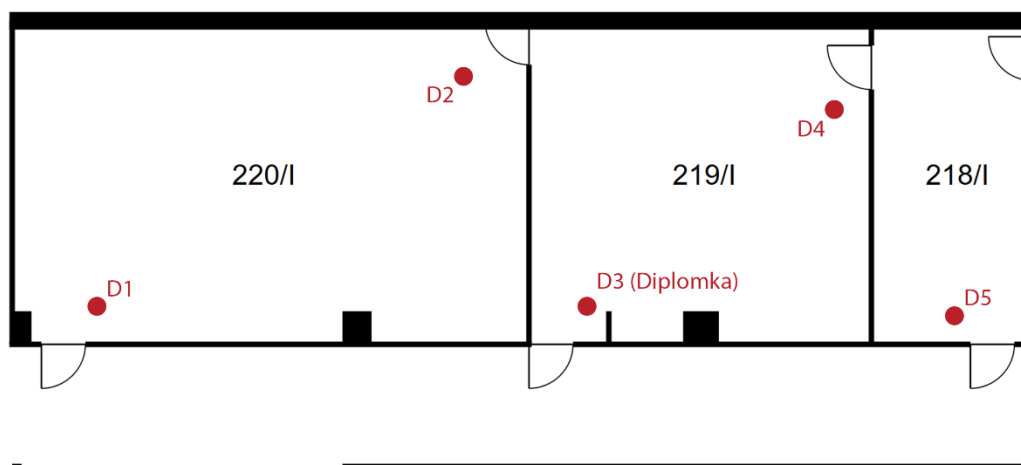
Obr. 10.1 Mapa testovací oblasti - TF ČZU [vlastní]

Katedra technologických zařízení staveb zapůjčila pro testování pět Access Pointů TP-link TL-WA 701ND. Jednotlivé AP byly nastaveny tak, aby vysílali Wi-Fi na protokolu IEEE 802.11g s konkrétními SSID pro každé AP. Seznam MAC adres a název vysílaného SSID je uveden v tab. 10.1.

Tab. 10.1 Seznam použitých AP

MAC adresa	SSID	Místnost
C0:4A:00:F1:A2:FA	D1	220/I
C0:4A:00:F1:AD:1F	D2	220/I
C0:4A:00:F1:AD:26	Diplomka (D3)	219/I
C0:4A:00:F1:A2:CC	D4	219/I
C0:4A:00:F1:AD:2D	D5	218/I

Access Pointy byly strategicky rozmístěny po monitorovaném prostoru tak, aby bylo zajištěno co nejlepší pokrytí a klient se nacházel pokud možno vždy poblíž jednoho z AP. Pozice jednotlivých AP jsou vyobrazeny na následujícím obrázku.

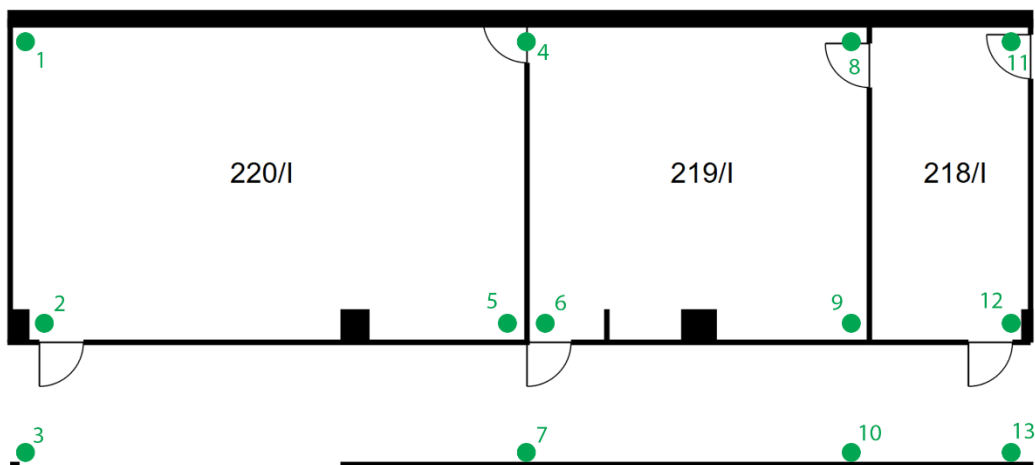


Obr. 10.2 Mapa rozmístění AP - TF ČZU [vlastní]

Po rozmístění a spuštění jednotlivých AP byl k síti Diplomka (D3) připojen notebook s vytvořeným programem WifiLocator. Po přidělení IP adresy byla tato adresa vložena do programu klienta a takto upravený program klienta nahrán stejným způsobem, jenž je uveden v kapitole 9.1.4. Na notebooku byla vypnuta brána firewall, aby nedocházelo k nechtěnému blokování komunikace. Brána firewall byla vypnuta po celou dobu testování.

Následně bylo spuštěno zařízení klienta. Ten se automaticky připojil do sítě Diplomka, získal IP adresu a připojil se pomocí protokolu TCP/IP (IPv4) k serveru, jenž běží v rámci

programu WifiLocator. Ten správně zaznamenal nové připojení a klient se zobrazil v seznamu klientů. Pomocí připraveného nástroje měření signálů v programu WifiLocator (*SignalWindow*) byla zahájena analýza pokrytí prostoru signály rozmístěných AP. Měření síly signálů se provedlo celkem ve třinácti bodech (viz obr. 10.3).



Obr. 10.3 Mapa bodů měření signálu - TF ČZU [vlastní]

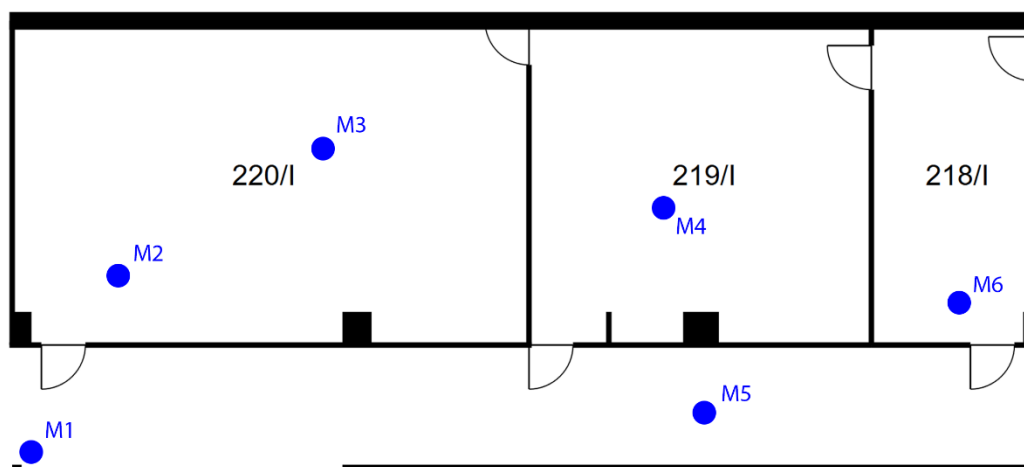
V každém měřeném bodě bylo provedeno deset naměření síly signálu. Těchto deset hodnot pro každé AP bylo programem automaticky zprůměrováno. Výsledné hodnoty jsou uvedeny v následující tabulce.

Tab. 10.2 Naměřené síly signálů na jednotlivé AP

Bod č.	Síla signálu [dBm]				
	D1	D2	D3	D4	D5
1	-44	-47	-62	-76	-71
2	-43	-53	-64	-59	-73
3	-41	-64	-70	-71	-68
4	-48	-30	-50	-62	-67
5	-55	-55	-49	-54	-63
6	-60	-52	-34	-53	-66
7	-64	-62	-54	-61	-58
8	-56	-49	-55	-44	-62
9	-59	-61	-57	-54	-47
10	-66	-62	-56	-57	-65
11	-57	-51	-65	-42	-50
12	-65	-60	-65	-51	-22
13	-74	-65	-67	-64	-53

Výsledné hodnoty byly zaneseny do kódu mapy a nová verze souboru byla načtena programem WifiLocator. Ten vypočítal pět map pokrytí signálem za 2 sekundy. Tím bylo dokončeno aplikování navržené technologie do monitorovaného prostoru a bylo možné zahájit testování určování polohy.

Test určení polohy byl proveden v šesti místech. Tato místa jsou vyobrazena na následujícím obrázku:



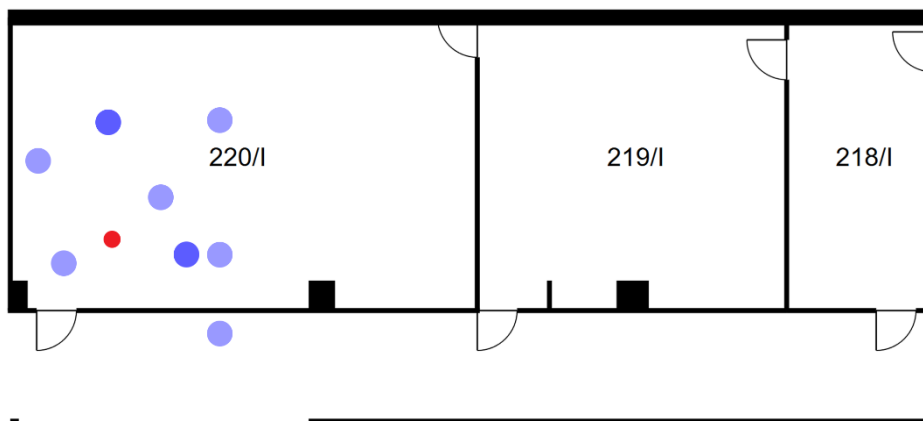
Obr. 10.4 Místa testování určení polohy - TF ČZU [vlastní]

V každém bodě se zaznamenalo deset po sobě jdoucích určení polohy. Pomocí souřadnic, jež určil program, a reálných souřadnic klienta byla pomocí Pythagorovy věty dopočítána vzdálenost určené polohy od skutečné. Přesnost lokalizace byla určena jako medián z vypočtených vzdáleností. Výsledky v jednotlivých bodech měření jsou uvedeny v následující tabulce.

Tab. 10.3 Přesnost určování polohy

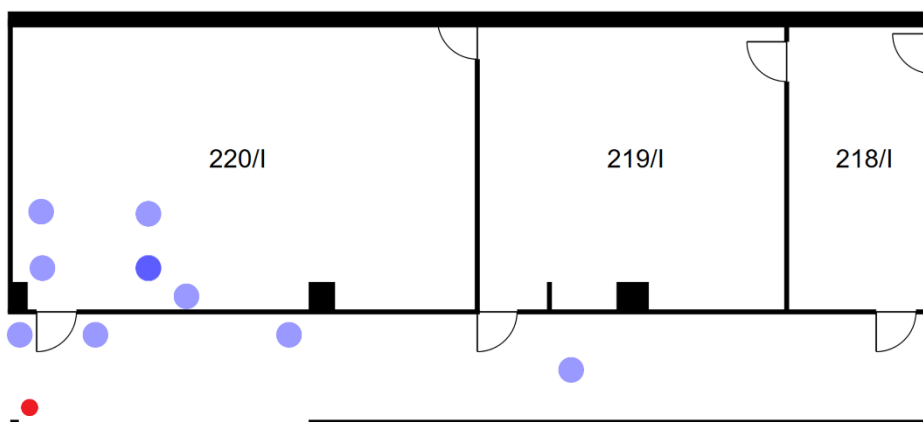
Bod	Minimální odchylka [m]	Maximální odchylka [m]	Medián [m]
M1	1,38	4,20	3,37
M2	0,99	3,81	1,53
M3	1,42	2,84	2,06
M4	1,35	8,45	2,60
M5	1,18	6,61	3,10
M6	1,36	6,92	2,46

Nejlepšího výsledku bylo dosaženo v bodě M2. Zde byla stanovena střední odchylka 1,53 metru od skutečné polohy klienta. Grafické znázornění je na následujícím obrázku, přičemž červeně je označena skutečná poloha klienta, modře určené polohy klienta. Sytost modrého puntíku odpovídá počtu určení polohy v daném bodě. Tzn. že v bodě, kde byla určena poloha 3x, je tmavší modrý puntík než v bodě, kde byla poloha určena pouze jednou.



Obr. 10.5 Výsledek měření - TF ČZU (M2) [vlastní]

Naopak nejhorších výsledků bylo dosaženo na chodbě, především v bodě M1, v němž byla určena střední odchylka 3,37 metru od skutečné polohy klienta. Tato odchylka byla s velkou pravděpodobností ovlivněna skutečností, že se na chodbě nenacházelo žádné monitorované AP. Grafické znázornění výsledku testování v bodě M1 je na následujícím obrázku.



Obr. 10.6 Výsledek měření - TF ČZU (M1) [vlastní]



Kompletní grafické vyobrazení výsledků testování v jednotlivých bodech se nachází v příloze č.3.

Z výsledků vyplývá, že průměrná střední odchylka od skutečné polohy je 2,518 metru. Pro vyhledání osoby v objektu je zapotřebí určit místnost, ve které se daná osoba nachází. Dle normy ČSN 73 4301 je stanovena minimální šířka obývacího pokoje 3300 mm. V porovnání s průměrnou odchylkou lze konstatovat, že přesnost technologie je dostačující. [28]

Považujeme-li určené polohy blíže než 3,3 metru od skutečné polohy za správné a určené polohy dále než 3,3 metru za nesprávné, lze určit spolehlivost určení polohy v jednotlivých bodech následovně:

Tab. 10.4 Spolehlivost určování polohy

Bod	Počet správných určení	Počet nesprávných určení	Spolehlivost [%]
M1	5	5	50
M2	9	1	90
M3	10	0	100
M4	8	2	80
M5	5	5	50
M6	8	2	80

Z výpočtů spolehlivosti určení polohy vyplývá, že absolutní přesnosti určení polohy bylo dosaženo v bodě M3, jenž se nachází v blízkosti AP D2 a mezi AP D1 a AP D3. Tato oblast je tedy pokryta poměrně stabilním signálem. Naopak nejhorší spolehlivosti bylo dosaženo na chodbě, což bylo způsobeno absencí AP s přímou viditelností a tedy nestabilním signálem.

Při zprůměrování vypočtených spolehlivostí dostáváme průměrnou spolehlivost určování polohy v monitorovaném prostoru 75%.

**Z testování vyplývá, že navržená technologie je funkční a že tedy lze určovat polohu v uzavřeném objektu pomocí signálu Wi-Fi.**

## 10.1 Porovnání výsledků s již dostupnými technologiemi

Výsledky získané testováním navržené technologie v poloprovozních podmínkách byly porovnány s parametry již existujících technologií. Srovnání vidíme v následující tabulce:

Tab. 10.5 Porovnání dostupných technologií na trhu s navrženou technologií [16] [14] [12] [13]

	Přesnost [m]	Technologie
<b>Navržená technologie</b>	2,5	- Wi-Fi
<b>Accuware</b>	2 – 3	- Wi-Fi - Bluetooth
<b>Ekahau</b>	1	- Wi-Fi
<b>Infsoft</b>	5 – 15	- Wi-Fi
<b>Mapspeople</b>	1	- Wi-Fi - Bluetooth - Magnetická pole - intenzita osvětlení

Z porovnání vyplývá, že navržená technologie je schopna konkurovat ostatním technologiím, jež jsou zavedeny na trhu. Technologie firem Accuware a Mapspeople, jež dosahují lepších výsledků, jsou založeny na kombinaci využití Wi-Fi a dalších technologií. Pokud tedy navrženou technologii porovnáme pouze s technologiemi používající k určování polohy pouze Wi-Fi signál, umístí se navržená technologie na druhém místě za technologií firmy Ekahau. Náklady na zprovoznění jednotlivých technologií nejsou známy. Jelikož navržená technologie je sestavena z běžně dostupných komponent, lze konstatovat, že je tato technologie konkurence schopná i z finančního hlediska.

## 10.2 Ekonomické vyhodnocení

Pro integraci navržené technologie je zapotřebí minimálních nákladů. Pokud dochází k aplikaci technologie do prostor dostatečně pokrytých signálem Wi-Fi, je potřeba investovat pouze do vytvořeného software, zařízení klienta, vytvoření mapy pro navržený program a prvotní analýzy pokrytí prostoru signálem.

Náklady na sestavení vytvořeného klienta v rámci této diplomové práce činily 248 Kč. Licence navrženého software by se mohla prodávat přibližně za 3 500 Kč. Složitost vytvoření mapy pro software závisí na monitorovaném prostoru, v případě testu v poloprovozních podmínkách zabralo vytváření mapy přibližně 30 minut. Analýza jedné místnosti zabere přibližně 10 minut.

Z těchto údajů vyplývá, že náklady na integraci navržené technologie do prostor již pokrytých Wi-Fi signálem by měly být menší než 10 000 Kč. V případě integrace do prostor nepokrytých Wi-Fi signálem by tyto náklady byly navýšeny o pořizování Access Pointů, přičemž jejich počet by byl závislý na velikosti a počtu místností monitorovaného prostoru.

Do každé místnosti doporučuji umístit jeden až dva Access Pointy v závislosti na velikosti místnosti. Závěrem lze konstatovat, že z finančního hlediska se u této technologie jedná o výhodnou volbu v porovnání s alternativními technologiemi.

## 11 Závěr

Cílem práce bylo navrhnout technologii, jež bude postavena na Wi-Fi triangulaci a vyhodnocována vlastním navrženým prostředkem pro monitoring osob v uzavřených prostorech, např. nemocnicích, LDN apod., ověřit přesnost a spolehlivost v poloprovozních podmínkách a provést srovnání s alternativními technologiemi.

Byla provedena analýza využití signálu Wi-Fi nejen k přenosu dat, ale i k dalším alternativním účelům. Práce popisuje bezdrátové přenosy z fyzikálního hlediska se zaměřením na elektromagnetické pole, elektromagnetické vlnění, vysílání a příjem signálu, antény, rozdělení frekvencí a rušení signálu. Je zmíněna role Českého telekomunikačního úřadu v bezdrátových přenosech a omezení vyplývající z nařízení tohoto úřadu. Zaměřuje se na jednotlivé protokoly IEEE 802.11, jejich frekvence, šířky pásma, přenosové rychlosti, na způsoby zabezpečení Wi-Fi a na rušení signálu této technologie.

Důležitou součástí teoretické části je vysvětlení pojmu triangulace a popis jednotlivých triangulačních metod. Závěrem jsou přiblížena stávající řešení používaná ve světě, jejich výhody a nevýhody.

Byl navržen způsob určování polohy pomocí Wi-Fi technologie. Bylo zkonstruováno a naprogramováno zařízení klienta, jehož poloha je určována. Toto zařízení je sestaveno z Wi-Fi modulu ESP 8266 a naprogramováno pomocí LUA skriptu tak, aby každých 10 sekund načetl dostupné Wi-Fi sítě a informace o síle signálu odeslal prostřednictvím TCP/IP protokolu na server umístěný v síti. Byla otestována funkčnost a komunikace se serverem prostřednictvím protokolu TCP/IP. V jazyce C# byl vytvořen program obsahující TCP/IP server nazvaný Wifi Signal Meter. Program posloužil při základním testování zařízení klienta a chování Wi-Fi signálu v prostoru. Na základě těchto testů byla zvolena triangulační metoda Analýza prostoru.

Dále byl vytvořen v programovacím jazyce C# pro operační systém Windows software s uživatelským rozhraním zobrazujícím určenou polohu klienta a TCP/IP server pro komunikaci s klientem.

Pro co nejpřesnější určování polohy je součástí programu speciálně vytvořený algoritmus, jenž je dle testování schopen určit polohu klienta s přesností na 2,5 m, čímž se vyrovná konkurenčním technologiím na trhu.

Navržená technologie byla otestována v poloprovozních podmínkách. Testování ověřilo funkčnost, přesnost a spolehlivost navržené technologie. Technologie je schopna určovat pozici klienta v ideálních podmínkách s přesností na 2,5 metru a spolehlivostí 75%. Zároveň však testování poukázalo i velký vliv rušení na přesnost určování polohy. Významné rušení představuje především pohyb osob ve sledovaném prostoru.

Technologie byla navržena z běžně dostupných komponent a z finančního hlediska lze konstatovat, že se jedná o velmi výhodnou volbu v porovnání s alternativními technologiemi.

Práce jednoznačně ukazuje na možnost použití signálu Wi-Fi k určování polohy v uzavřených prostorech. Zároveň z výsledků vyplývají i některé nevýhody tohoto způsobu určování polohy, což ovlivňuje použitelnost této technologie v prostorách s velkým pohybem osob. Pro praktické využití bude pravděpodobně nutné zkombinovat tuto technologii i s dalšími technologiemi, např. Bluetooth, magnetická pole, intenzita osvětlení apod.

## 12 Závěrečná doporučení

V budoucnu bych doporučil navrženou technologii otestovat i v pásmu 5 GHz, na které má rušení rozdílný vliv v porovnání s pásmem 2,4 GHz.

Také bych doporučil tuto technologii zkombinovat s další technologií, jež by minimalizovala vliv rušení na přesnost určování polohy. Většina komerčních technologií určujících polohu pomocí signálu Wi-Fi, jež je dostupná na světovém trhu, využívá právě kombinaci více technologií, např. Bluetooth, magnetická pole, intenzitu osvětlení apod.

Při aplikaci navržené technologie do provozu doporučuji respektovat poznatky o vlivu intenzivního vyzařování signálu na 2,4 GHz na zdraví osob, jež se pohybují v takto pokrytém prostoru.

Při monitorování pohybu osob v prostoru je zapotřebí brát v potaz i případný zásah do soukromí těchto osob. Získané informace o pohybu osob spadají pod ochranu osobních údajů a je zapotřebí s nimi nakládat dle příslušného zákona. **Osoba by neměla být monitorována bez jejího souhlasu.**

Před použitím této technologie v praxi je zapotřebí upravit zkonstruovaný hardware tak, aby byl odolný, vodotěsný a co nejmenší. Doporučoval bych vyhotovit finální verzi v podobě náramku, jenž by umožnil snadné nošení.

## Seznam zdrojů

1. **Olmr, Martin.** *Analýza bezdrátových přenosů pro datovou komunikaci z pohledu fyzikálních vlastností.* Praha : Česká zemědělská univerzita v Praze, Technická fakulta, 2015.
2. **Sopko, Bruno, Samek, Ladislav a Černý, František.** *Fyzika II.* Praha : České vysoké učení technické v Praze, 2005. 80-01-03194-2.
3. **Černý, František, Samek, Ladislav a Sopko, Bruno.** *Fyzika I.* Praha : České vysoké učení technické v Praze, 2009. 978-80-01-03650-1.
4. **ČTÚ.** Využívání vymezených rádiových kmitočtů. *Český telekomunikační úřad.* [Online] [Citace: 18. 2 2015.] <https://www.ctu.cz/ctu-informuje/jak-postupovat/radiove-kmitocty/vyuzivani-vymezenych-radiovyh-kmitoctu.html>.
5. **ČTÚ.** Základní informace. *Český telekomunikační úřad.* [Online] [Citace: 18. 2 2015.] <https://www.ctu.cz/o-ctu/zakladni-informace.html?action=detail&ArticleId=123>.
6. **Mezánek, Miloš, Vrba, Jan a Český, Tomáš.** *Radiokomunikace současnosti a budoucnosti.* Praha : Nakladatelství dopravy a spojů, 1981. OS-31-029-81-05-38.
7. **Vysoká škola báňská.** *Vysoká škola báňská - Technická univerzita Ostrava.* [Online] [Citace: 2. 3 2015.] [http://fei1.vsb.cz/kat420/vyuka/FEI/sireni\\_vln/teze/otazka\\_18.pdf](http://fei1.vsb.cz/kat420/vyuka/FEI/sireni_vln/teze/otazka_18.pdf).
8. **Kaisler, Petr,** *Parametry a typy antén. Učíme v prostoru.* [Online] [Citace: 02. 03 2015.] [http://uvp3d.cz/dum/?page\\_id=2652](http://uvp3d.cz/dum/?page_id=2652).
9. **Spurná, Ivona.** *Počítačové sítě praktická příručka správce sítě.* : Computer Media, 2010. 978-80-7402-036-0.
10. **inc., Apple.** *Možné zdroje rušení Wi-Fi.* [Online] 18. 04 2016. [Citace: 2017. 03 02.] <https://support.apple.com/cs-cz/HT201542>.
11. **Schindelbauer, Christian.** *Wireless Sensor Networks.* [Wireless Sensor Networks.pdf] Freiburg : University of Freiburg, 2006.
12. **Inc., Accuware.** *Accuware Indoor Navigation fact sheet.* [[http://public.accuware.com/files/Accuware\\_Indoor\\_Navigation\\_Fact\\_Sheet.pdf](http://public.accuware.com/files/Accuware_Indoor_Navigation_Fact_Sheet.pdf)] místo neznámé : Accuware inc.
13. **s.r.o., Ryston Electronics.** Lokalizace pomoci Wi-Fi sítě | Macroweil. *macroweil.cz.* [Online] Ryston Electronics s.r.o. [Citace: 05. 03 2017.] <http://www.macroweil.cz/cs/wifi-lokalizace-rtls/lokalizace-pomoci-wifi-site.html>.
14. **Ekahau.** Products | Ekahau. *ekahau.com.* [Online] 2017. [Citace: 04. 03 2017.] <https://www.ekahau.com>.

- 15. GmbH, infsoft. infsoft.com. infsoft.com.** [Online] infsoft GmbH, 2017. [Citace: 05. 03 2017.] <https://www.infsoft.com/technology/sensors/wifi>.
- 16. MapsPeople. MapsIndoors | MapsPeople. MapsPeople.** [Online] MapsPeople. [Citace: 05. 03 2017.] <https://www.mapspeople.com/mapsindoors>.
- 17. Alza.cz. Arduino UNO Rev3 - Stavebnice | Alza.cz. Alza.cz.** [Online] [Citace: 20. 02 2017.] <https://i.alza.cz/lmgW.ashx?fd=f3&cd=ARD204a>.
- 18. terrye. NodeMCU. esp8266.com.** [Online] 13. 02 2016. [Citace: 10. 08 2016.] <http://www.esp8266.com/wiki/doku.php?id=nodemcu>.
- 19. ESP8266.com. ESP8266.com - datasheet. ESP8266.com.** [Online] [Citace: 20. 02 2017.] [http://www.esp8266.com/wiki/lib/exe/fetch.php?media=0a-esp8266\\_datasheet\\_en\\_v4.3.pdf](http://www.esp8266.com/wiki/lib/exe/fetch.php?media=0a-esp8266_datasheet_en_v4.3.pdf).
- 20. WIZnet Co., Ltd. http://www.wiznet.co.kr. WIZnet Co., Ltd. - WiFi Shield V2.2 - Datasheet.** [Online] [Citace: 20. 02 2017.] [http://www.wiznet.co.kr/wiki/lib/exe/fetch.php?media=0a-esp8266\\_datasheet\\_en\\_v4.3.pdf](http://www.wiznet.co.kr/wiki/lib/exe/fetch.php?media=0a-esp8266_datasheet_en_v4.3.pdf).
- 21. RobotShop. RobotShop - Wifi Shield V2.2 for Arduino - datasheet. RobotShop.** [Online] [Citace: 20. 02 2017.] <http://www.robotshop.com/en/dfrobot-wifi-shield-v22-arduino.html>.
- 22. cdn.sparkfun.com. cdn.sparkfun.com - ESP 8266 image. cdn.sparkfun.com.** [Online] [Citace: 20. 02 2017.] <https://cdn.sparkfun.com/assets/parts/1/1/1/2/9/13678-01.jpg>.
- 23. alldatasheet.com. alldatasheet.com - AMS1117-3.3 Datasheet. alldatasheet.com.** [Online] [Citace: 23. 08 2016.] <http://www.alldatasheet.com/view.jsp?Searchword=Ams1117-3.3&gclid=CNHn2dmbs9ICfde6GwoduO8OPA>.
- 24. dxcdn.com - Obrázek I2C 5V3.3V. dxcdn.com.** [Online] [Citace: 21. 02 2017.] [http://img.dxcdn.com/productimages/sku\\_197198\\_3.jpg](http://img.dxcdn.com/productimages/sku_197198_3.jpg).
- 25. osoyoo.com. osoyoo.com - ESP 8266 PIN. osoyoo.com.** [Online] 25. 5 2016. [Citace: 26. 08 2016.] <http://osoyoo.com/wp-content/uploads/2016/08/esp8266.jpg>.
- 26. remotexy.com. remotexy.com - ESP8266 firmware update. remotexy.com.** [Online] [Citace: 28. 08 2016.] <http://remotexy.com/en/help/esp8266-firmware-update/>.
- 27. terrye. esp8266.com - NodeMCU. esp8266.com.** [Online] 13. 03 2016. [Citace: 29. 08 2016.] <http://www.esp8266.com/wiki/doku.php?id=nodemcu>.
- 28. institut, Český normalizační. Norma ČSN 73 4301.** [Obytné budovy ČSN 73 4301.pdf] Praha : Český normalizační institut, 2004.



**29. Pužmanová, Rita.** *Bezpečnost bezdrátové komunikace.* Brno : Vydavatelství a nakladatelství CP Books, 2005. 80-251-0791-4.

**30. g01.a.alicdn.com.** *alicdn.com.* [Online] [Citace: 20. 02 2017.]  
<http://g01.a.alicdn.com/kf/HTB1zl1LIVXXXXaqXFXXq6xXFXXZ/AMS1117-3-3-DC-DC-Step-Down-Voltage-Regulator-Adapter-Convertor-3-3V-Output.jpg>.

## Seznam obrázků

Obr. 4.1 Vlnová délka.....	8
Obr. 4.2 Amplituda.....	9
Obr. 4.3 Frekvence.....	10
Obr. 4.4 Spektrum elektromagnetického vlnění .....	11
Obr. 4.5 Přenos signálu .....	12
Obr. 4.6 Schéma vytvoření přenosového signálu .....	13
Obr. 4.7 Schéma zpracování signálu .....	14
Obr. 4.8 Drátové antény - a) přímý vodič, b) smyčka, c) šroubovice.....	16
Obr. 4.9 Plošná anténa .....	16
Obr. 4.10 Parabolická anténa .....	17
Obr. 4.11 Yagiho anténní řada .....	17
Obr. 4.12 Anténní čočky – a) konvexní, b) konkávní .....	18
Obr. 6.1 Proximity .....	26
Obr. 6.2 Trilaterace .....	26
Obr. 6.3 Určení polohy bodu pomocí směrových antén .....	28
Obr. 6.4 Určení polohy bodu pomocí překrytí signálů .....	28
Obr. 6.5 Určení polohy bodu pomocí aproximace v trojúhelníku .....	29
Obr. 7.1 Accuware indoor navigation - schéma .....	31
Obr. 7.2 Accuware indoor navigation - aplikace.....	31
Obr. 7.3 Ekahau - spektrální mapa .....	32
Obr. 7.4 MapsIndoors .....	33
Obr. 9.1 Arduino Uno Rev3.....	36
Obr. 9.2 Modul WiFi Shield V2.2.....	37
Obr. 9.3 Modul ESP 8266 .....	38
Obr. 9.4 Schéma ESP 8266.....	39
Obr. 9.5 Převodník napětí I2C 5v – 3,3V .....	40
Obr. 9.6 Stabilizátor napětí AMS1117-5V.....	41
Obr. 9.7 Schéma zapojení komponent .....	41
Obr. 9.8 Schéma plošných spojů.....	42
Obr. 9.9 ESP 8266 - piny.....	42
Obr. 9.10 Zkonstruované zařízení klienta .....	43
Obr. 9.11 USB - UART převodník.....	43

Obr. 9.12 Schéma zapojení ESP 8266 a USB - UART převodníku.....	43
Obr. 9.13 ESP8266Flasher.....	44
Obr. 9.14 ESP8266Flasher - konfigurace.....	45
Obr. 9.15 Lua Uploader v1.0.2.4.....	45
Obr. 9.16 Lua Uploader - nahrání init.lua.....	47
Obr. 9.17 Lua Uploader - připojení do sítě Wi-Fi.....	48
Obr. 9.18 Hercules - TCP server.....	48
Obr. 9.19 Wifi Signal Meter.....	49
Obr. 9.20 Schéma vláken programu.....	54
Obr. 9.21 Grafické rozhraní programu - hlavní okno.....	56
Obr. 9.22 Grafické rozhraní programu - okno nastavení.....	56
Obr. 9.23 Grafické rozhraní programu - okno měření signálů.....	57
Obr. 9.24 Zobrazení testovací mapy.....	63
Obr. 9.25 Grafické znázornění rozdělení bodů do skupin a určení polohy klienta.....	67
Obr. 9.26 WiFiLocator - Test připojení klienta.....	68
Obr. 9.27 Mapa rozmístění AP – Testovací byt.....	69
Obr. 9.28 Mapa bodů měření síly signálu – Testovací byt.....	70
Obr. 9.29 Mapa pokrytí – Ekahaou.....	70
Obr. 9.30 Mapa pokrytí – WiFiLocator.....	71
Obr. 9.31 Výsledek měření – Testovací byt (předsíň).....	72
Obr. 9.32 Výsledek měření – Testovací byt (koupelna).....	73
Obr. 10.1 Mapa testovací oblasti - TF ČZU.....	74
Obr. 10.2 Mapa rozmístění AP - TF ČZU.....	75
Obr. 10.3 Mapa bodů měření signálu - TF ČZU.....	76
Obr. 10.4 Místa testování určení polohy - TF ČZU.....	77
Obr. 10.5 Výsledek měření - TF ČZU (M2).....	78
Obr. 10.6 Výsledek měření - TF ČZU (M1).....	78

## Seznam tabulek

Tab. 4.1 Rozdělení frekvencí podle způsobu využití.....	12
Tab. 5.1 Protokoly standardu IEEE 802.11.....	20
Tab. 9.1 Základní parametry WiFi Shield V2.2.....	37
Tab. 9.2 Základní parametry ESP 8266.....	38
Tab. 9.3 Porovnání parametrů modulů WiFi Shield V2.2 a ESP 8266.....	39
Tab. 9.4 Seznam tříd.....	55
Tab. 10.1 Seznam použitých AP.....	75
Tab. 10.2 Naměřené síly signálů na jednotlivé AP.....	76
Tab. 10.3 Přesnost určování polohy.....	77
Tab. 10.4 Spolehlivost určování polohy.....	79
Tab. 10.5 Porovnání dostupných technologií na trhu s navrženou technologií.....	80

## Seznam rovnic

4.1	I. Maxwellova rovnice (integrální tvar) .....	6
4.2	I. Maxwellova rovnice (diferenciální tvar).....	6
4.3	II. Maxwellova rovnice (integrální tvar) .....	6
4.4	II. Maxwellova rovnice (diferenciální tvar).....	7
4.5	III. Maxwellova rovnice (integrální tvar) .....	7
4.6	III. Maxwellova rovnice (diferenciální tvar).....	7
4.7	IV. Maxwellova rovnice (integrální tvar) .....	7
4.8	IV. Maxwellova rovnice (diferenciální tvar) .....	7
4.9	Vztah frekvence a periody .....	9
4.10	Vztah frekvence a vlnové délky .....	10
4.11	Vztah závislosti frekvence a vlnové délky .....	10
9.1	Rovnice trendu úbytku síly signálu v závislosti na vzdálenosti od vysílače.....	50

## Seznam grafů

Graf 9.1	Úbytek síly signálu v závislosti na vzdálenosti od vysílače .....	50
Graf 9.2	Stabilita síly signálu - 1m.....	51
Graf 9.3	Stabilita síly signálu - 3m.....	51
Graf 9.4	Stabilita síly signálu - 6m.....	52
Graf 9.5	Vliv osoby na sílu signálu .....	53

## Seznam příloh

Příloha 1 .....	Program ESP 8266
Příloha 2 .....	Diagram tříd
Příloha 3 .....	Výsledky testování v poloprovozních podmínkách
Příloha CD.....	Program modulu ESP 8266
Příloha CD.....	Firmware modulu ESP 8266
Příloha CD.....	Zdrojové soubory map pro program WifiLocator
Příloha CD.....	Mapy pokrytí signálem
Příloha CD.....	Půdorysy TF ČZU
Příloha CD.....	Naměřené hodnoty testování stability signálu Wi-Fi
Příloha CD.....	Naměřené hodnoty testování závislosti síly signálu na vzdálenosti

Příloha CD.....	Výsledky testování technologie Bachova
Příloha CD.....	Výsledky testování technologie TF ČZU
Příloha CD.....	Zdrojové kódy programu WifiLocator
Příloha CD.....	Zdrojové kódy programu Wifi Signal Meter

## Příloha 1: Program ESP 8266 (init.lua)

```
-----  
SSID      = "Diplomka"  
PASSWORD  = "diplomka12345"  
SERVER    = "192.168.1.10"  
PORT      = 1100  
ID        = 1  
-----
```

```
function listap(t)  
  if t == nil then  
    print("NO DATA!")  
  else  
    data = ID.."["  
    for k,v in pairs(t) do  
      data = data .. k.."("..v..");"  
    end  
    data = data .. "]"  
    send(data)  
  end  
end  
function connect(ssid, pwd)  
  print("")  
  print("Connecting to "..ssid)  
  wifi.setmode(wifi.STATION)  
  wifi.sta.config(ssid, pwd)  
end  
function disconnect()  
  wifi.sta.disconnect()  
  socket:close()  
  print("disconnected")  
end  
index = 0  
function printAP()  
  index = index + 1  
  wifi.sta.getap(listap)  
end  
function send(data)  
  print(data)  
  socket:send(data)  
end  
  
print("ID: "..ID)  
print("SSID: "..SSID)
```

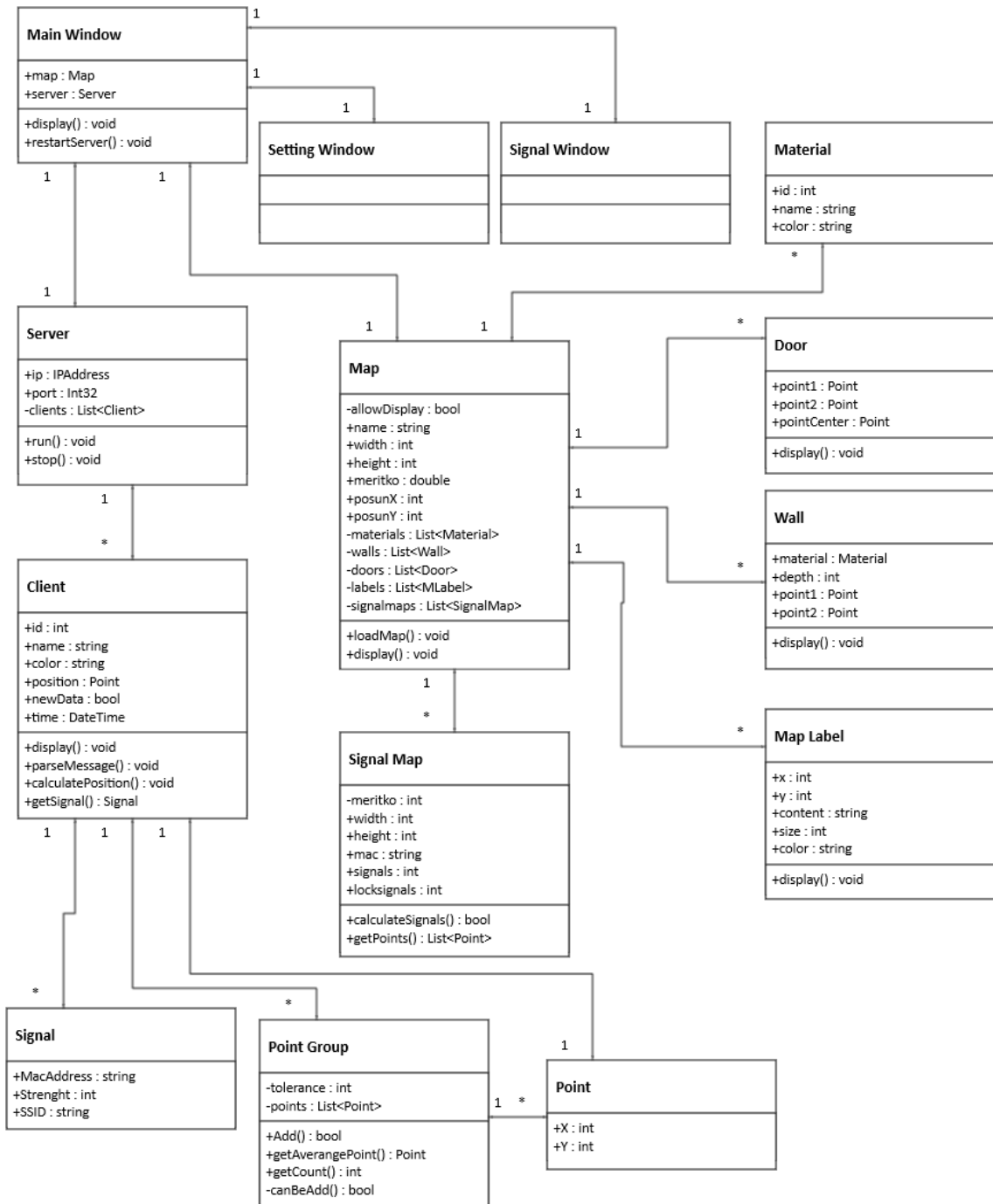
```

print("SERVER: "..SERVER)
print("PORT: "..ID)
connect(SSID,PASSWORD)
print("Connecting..")

sec = 0
-- socket
socket = net.createConnection(net.TCP, 0)
socket:on("receive",function(sck,c)
  if c=="STOP" then
    print("STOPPED")
    tmr.stop(2)
  elseif c=="RESET" then
    node.restart()
  else
    print(c)
  end
end)
socket:on("connection", function(sck, c)
  print("Connected!")
  print("You have 10 seconds to abort")
  print("Waiting...")
  tmr.alarm(2, 10000, 1, printAP)
end)
-- pripojeni k AP
tmr.alarm(1, 1000, 1, function()
  if wifi.sta.getip() == nil then
    sec = sec + 1
    print("Waiting for IP address... "..("..sec.." s"))
    if sec == 30 then
      tmr.stop(1)
      print("WAITING STOPPED")
    end
  else
    tmr.stop(1)
    print("")
    print("-----")
    print("WiFi connection established, IP address: " .. wifi.sta.getip())
    print("Connecting to server:" .. SERVER ..":"..PORT)
    socket:connect(PORT,SERVER)
  end
end)

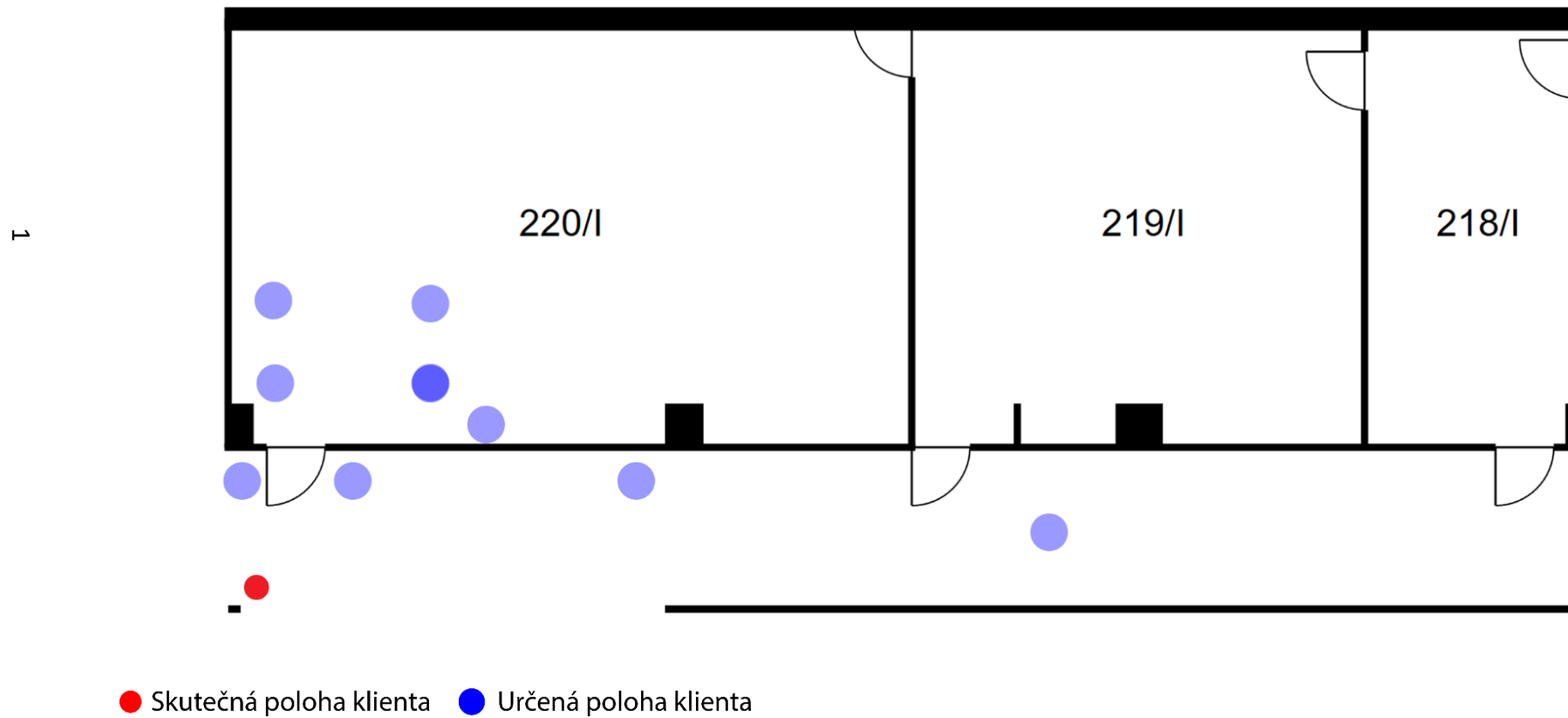
```

## Příloha 2: Diagram tříd



### Příloha 3: Výsledky testování v poloprovozních podmínkách

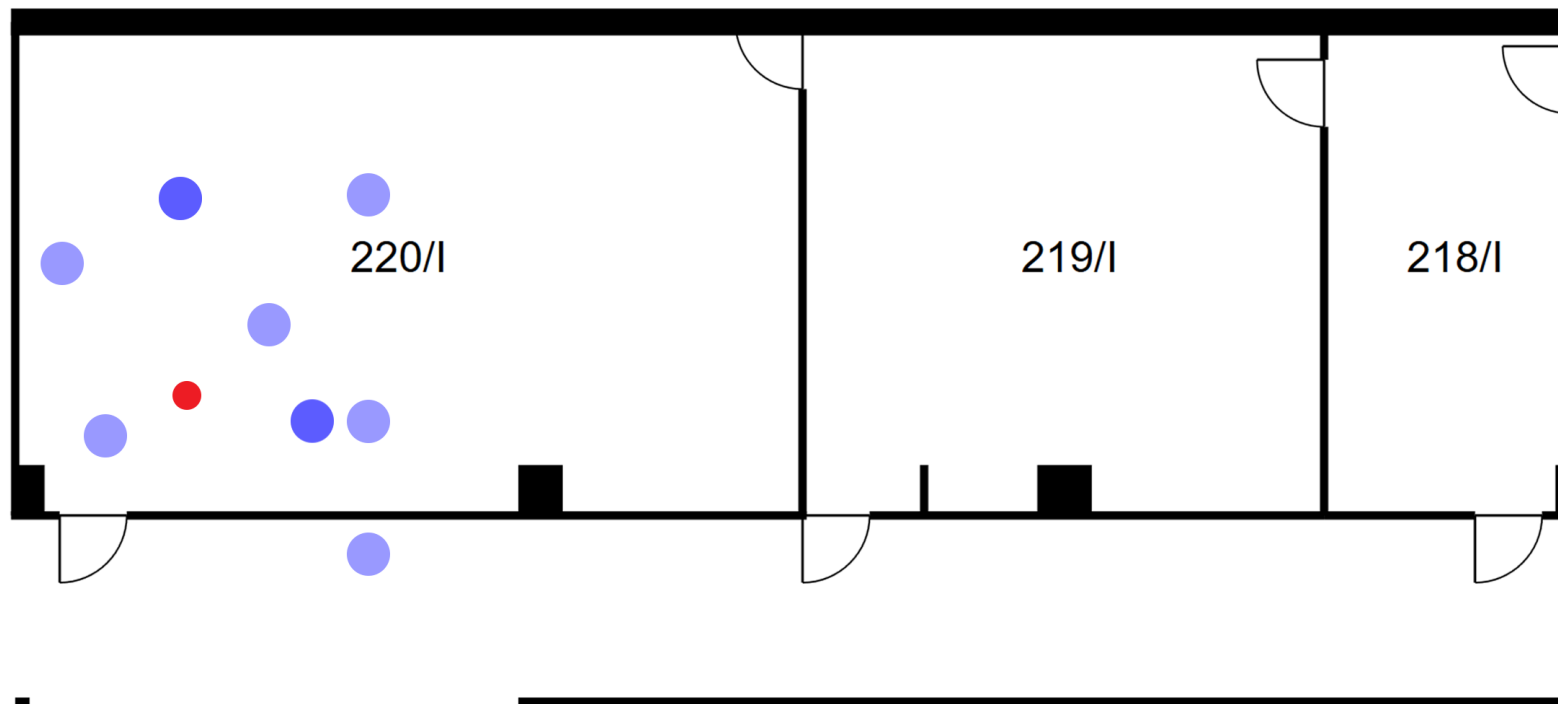
Výsledek měření v bodě M1





Výsledek měření v bodě M2

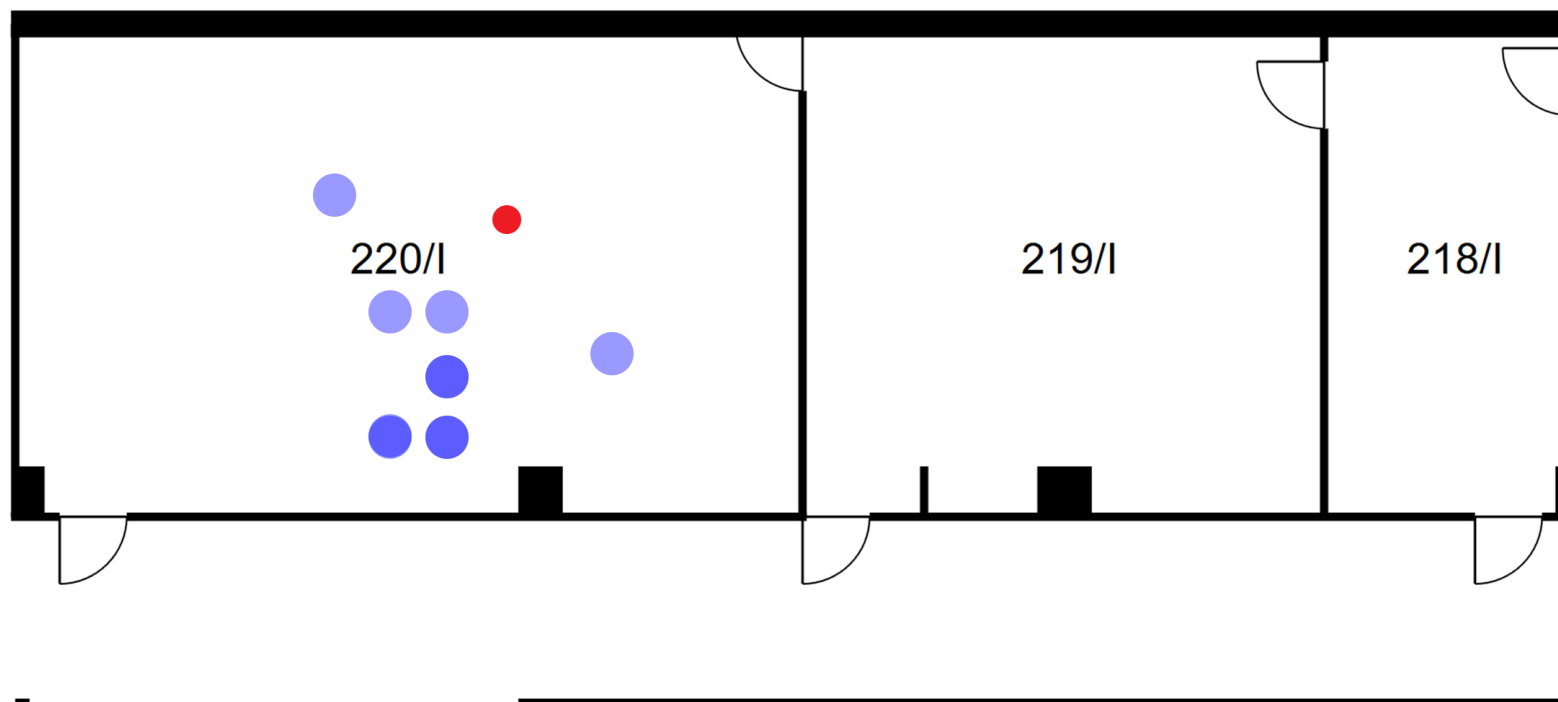
2



● Skutečná poloha klienta ● Určená poloha klienta

### Výsledek měření v bodě M3

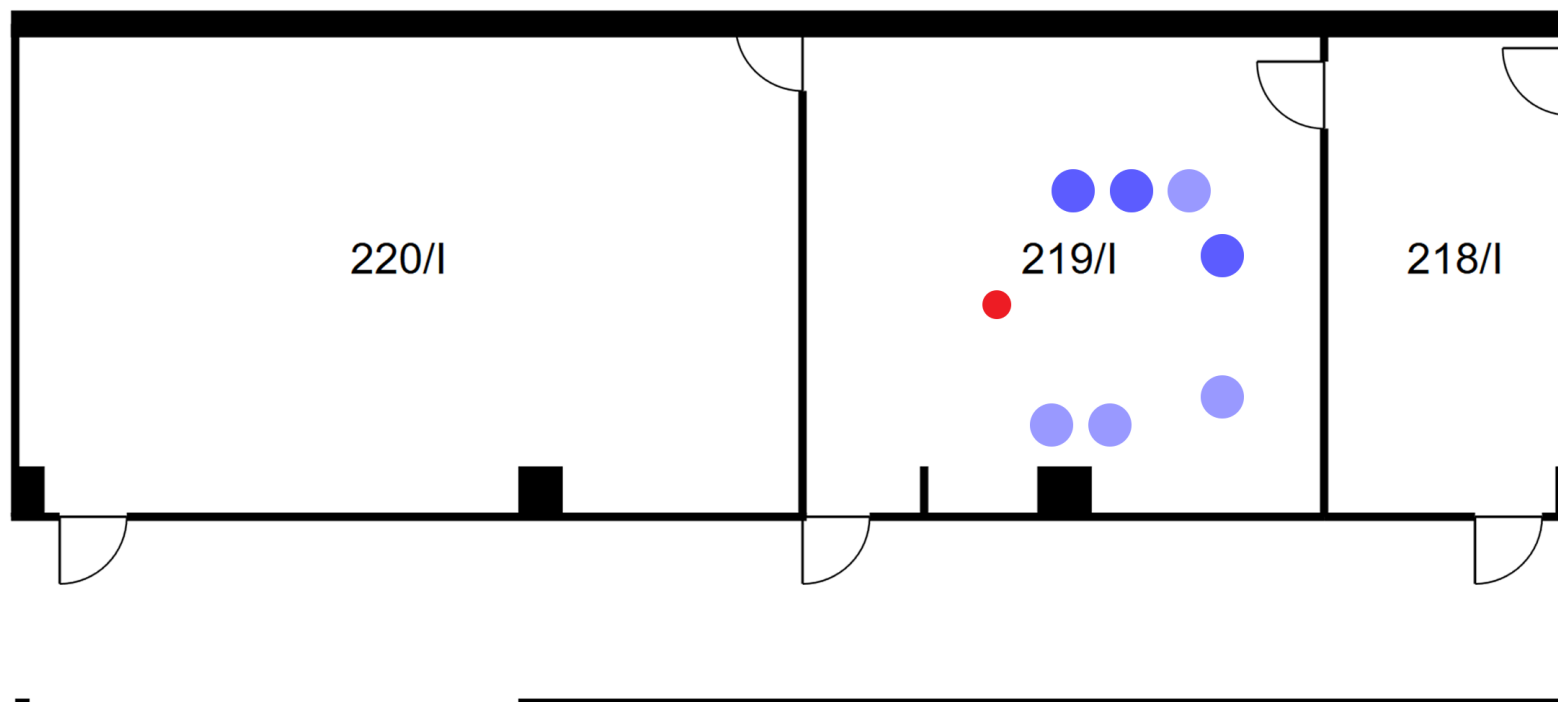
3



● Skutečná poloha klienta ● Určená poloha klienta

### Výsledek měření v bodě M4

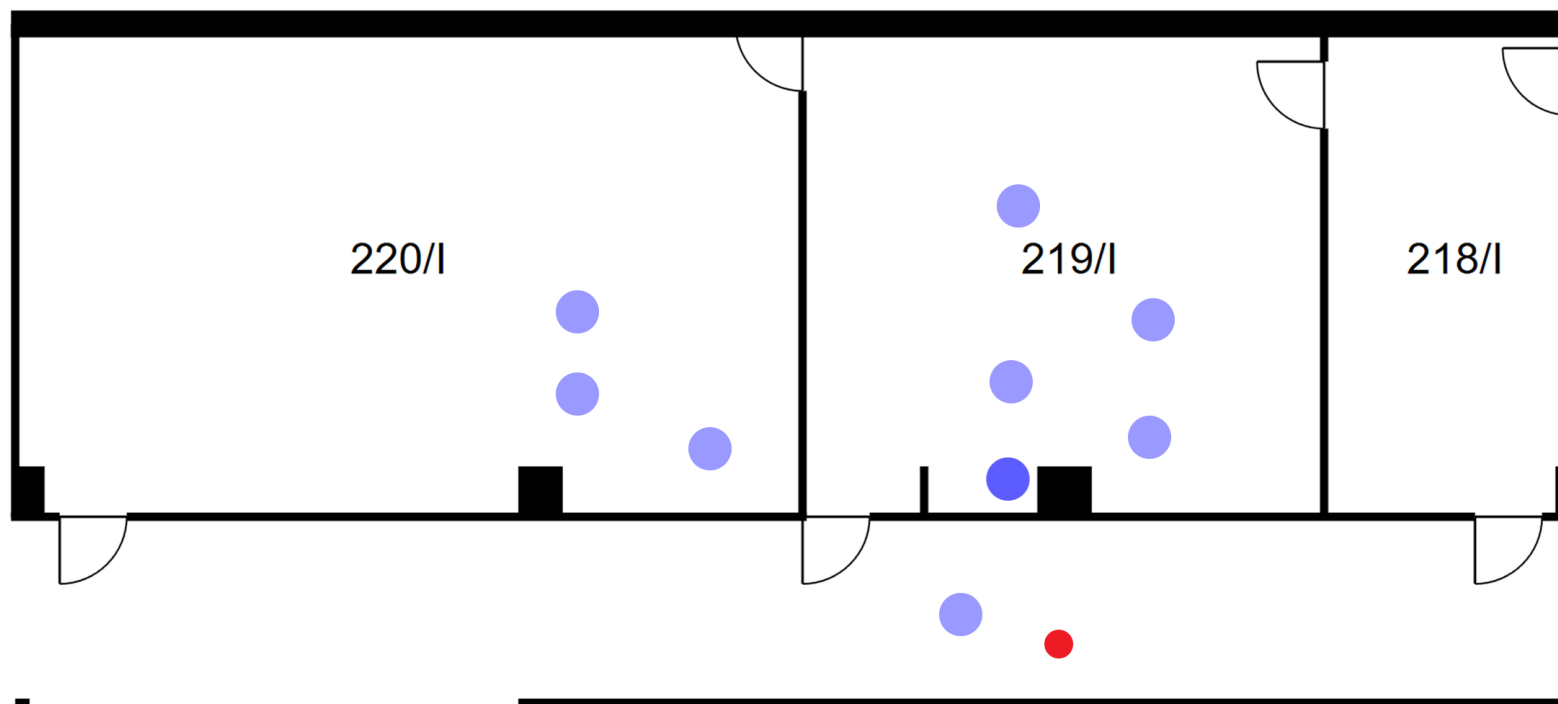
4



● Skutečná poloha klienta    ● Určená poloha klienta

### Výsledek měření v bodě M5

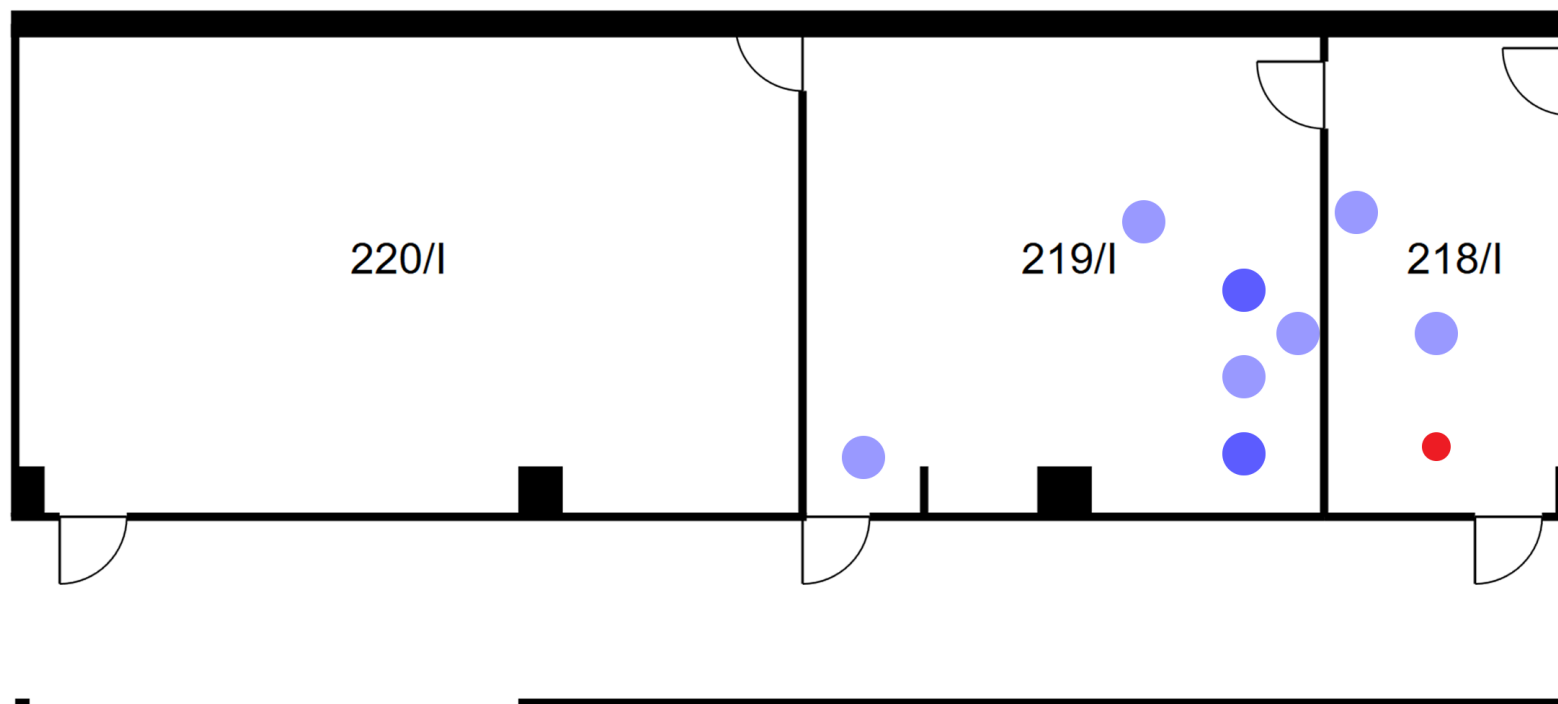
5



● Skutečná poloha klienta ● Určená poloha klienta

### Výsledek měření v bodě M6

9



● Skutečná poloha klienta ● Určená poloha klienta