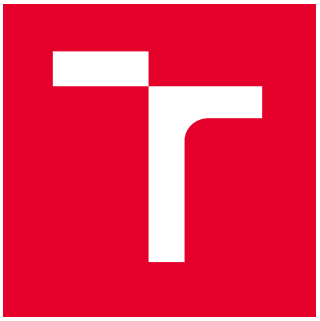


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV AUTOMATIZACE A MĚŘICÍ TECHNIKY

DEPARTMENT OF CONTROL AND INSTRUMENTATION

NÁSTROJE PRO MONITOROVÁNÍ RÁDIOVÝCH SÍTÍ

RF MONITOR TOOL

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — **Filip Hűbl**

AUTHOR

VEDOUCÍ PRÁCE — **Ing. Soběslav Valach**

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Automatizační a měřicí technika**

Ústav automatizace a měřicí techniky

Student: Filip Hůbl ***ID:*** 230078

Ročník: 3 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Nástroje pro monitorování rádiových sítí

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je návrh analyzátoru monitoringu zařízení pracujících v RF pásmech. Především by se mělo jednat o zařízení WiFi, Bluethooth, IoT. Ze získaných dat bude třeba vytěžit informace o pohybu / poloze zařízení, počtu průchodu monitorovanými stanovišti a odhadem počtu osob, které prošly daným stanovištěm za jednotku času. Cílová platforma by měla využívat procesor s jádrem ARM (např. modul Raspberry Pi).

1) Prostudujte principy a techniky monitorování a sledování RF sítí.
2) Vytvořte aplikaci pro monitorování provozu, ověřte její funkci.
3) Navrhněte vhodné uspořádání monitorovacích stanovišť v 2D prostoru.
4) Navrhněte vhodný komunikační protokol pro předávání dat nadřazenému systému.
5) Zpracujete data získaná data a vizualizujte vhodným způsobem.
6) Analyzujte spolehlivost a funkčnost navrženého řešení.

DOPORUČENÁ LITERATURA:

https://www.raspberrypi.org/

Stone R.; 30-Aug-2019: RASPBERRY PI 4 COMPLETE MANUAL: A Step-by-Step Guide to the New Raspberry Pi 4 and Set Up Innovative Projects

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 22.5.2024

Vedoucí práce: Ing. Soběslav Valach

Ing. Miroslav Jirgl, Ph.D.
předseda rady studijního programu

ABSTRAKT

Bakalářská práce zkoumá detekci aktivních WiFi a Bluetooth zařízení prostřednictvím mini počítače Raspberry Pi s využitím softwaru Kismet. Monitorování probíhá v pásmech 2,4 GHz a 5 GHz. V práci jsou detailně rozebrány principy fungování těchto technologií a metody jejich možné detekce. Získané výsledky poskytují informace o celkovém počtu identifikovaných aktivních zařízení během měření, pohybu těchto zařízení a tato zařízení jsou dále kategorizována podle svého typu.

KLÍČOVÁ SLOVA

WiFi, Bluetooth, 2,4 GHz, 5 GHz, Detekce, Raspberry Pi, Kismet, monitorovací mód, IEEE, ISM, Modulační technologie

ABSTRACT

This bachelor thesis investigates the detection of active WiFi and Bluetooth devices via a Raspberry Pi mini computer using Kismet software. Monitoring is performed in the 2.4 GHz and 5 GHz bands. The thesis discusses in detail the principles of operation of these technologies and methods of their possible detection. The results obtained provide information on the total number of active devices identified during the measurements, the movement of these devices and these devices are further categorized according to their type.

KEYWORDS

WiFi, Bluetooth, 2,4 GHz, 5 GHz, Detection, Raspberry Pi, Kismet, Monitoring Mode, IEEE, ISM, Modulation Technology

HŰBL, Filip. *Nástroje pro monitorování rádiových sítí*. Bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav automatizace a měřicí techniky, 2024. Vedoucí práce: Ing. Soběslav Valach

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Filip Hűbl
VUT ID autora:	230078
Typ práce:	Bakalářská práce
Akademický rok:	2023/24
Téma závěrečné práce:	Nástroje pro monitorování rádiových sítí

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Soběslavu Valachovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

V současné době se bezdrátové technologie staly nezbytnou součástí našeho každodenního života. WiFi sítě, Bluetooth zařízení a Internet of Things (IoT) senzory se využívají ve velkém množství aplikací, od domácích spotřebičů po průmyslové a komerční nasazení. S tímto rozšířením bezdrátových technologií vzniká také potřeba jejich monitorování a analýzy, zejména s ohledem na zajištění bezpečnosti, spolehlivosti a efektivity jejich provozu.

Cílem této práce je navrhnout a implementovat analyzátor monitoringu zařízení pracujících v rádiových frekvenčních pásmech. Tento analyzátor bude schopen shromažďovat data o síťovém provozu, identifikovat zařízení vybavená technologiemi bezdrátových sítí (WiFi, Bluetooth, IoT) a provádět analýzu těchto dat. Klíčovým aspektem bude extrahování informací o pohybu a poloze zařízení, sledování počtu průchodů monitorovanými stanovišti a odhad počtu osob, které prošly daným stanovištěm za jednotku času.

Pro implementaci tohoto analyzátoru bude využita platforma s procesorem architektury ARM, konkrétně Raspberry Pi. Tato volba platformy umožní praktickou realizaci nástroje v reálném prostředí a jeho potenciální nasazení v různých kontextech, včetně průmyslového monitorování.

V dalších částech této práce budeme podrobněji zkoumat problematiku monitorování rádiových sítí, analyzovat potřebné technické a softwarové prostředky, představíme konkrétní postupy a algoritmy pro získávání a analýzu dat. Nakonec budeme diskutovat o možných aplikacích, výhodách a nevýhodách navrženého monitorovacího nástroje.

1 WiFi

WiFi je technologie, která používá radiové vlny v nelicencovaných pásmech 2,4 GHz a 5 GHz pro přenos bezdrátového internetového připojení, a je založena na sadě standardů pro bezdrátovou komunikaci IEEE 802.11. To umožňuje zařízením, jako například mobilní zařízení (mobilní telefon, chytré hodinky, tablet, notebook), příslušenství (tiskárna, chytrá žárovka), komunikovat mezi sebou a připojit se k internetové síti. [1, 2]

Tato technologie se používá pro vytváření lokálních bezdrátových sítí pomocí WiFi routerů, které poté i zprostředkovává komunikaci s internetovým poskytovatelem. [1, 2]

Zařízení, které jsou vybaveny technologií WiFi budu dále označovat jako „WiFi zařízení“.

1.1 Standardy IEEE 802.11

Rodina standardů IEEE 802.11 se od jeho počátku velmi rozšířila a my si zde popíšeme ty nejdůležitější. [3, 4, 5]

1.1.1 IEEE 802.11

První standard IEEE 802.11, nebo také WiFi 0, byl uveden na trh v roce 1997. Dosahoval maximální přenosové rychlosti 2 Mbit/s. Nabízí tři různé způsoby implementace fyzické vrstvy: frequency hopping spread spectrum (FHSS) a direct sequence spread spectrum (DSSS) obě pracující v ISM pásmu 2,4 GHz nebo infrared (IR) v pásmu 316 THz - 353 THz, které nenašlo komerční využití. Později se však ukázalo, že tato přenosová rychlost a výše zabezpečení jsou nedostačující, a proto byly postupně přidávány dodatky k tomuto standardu, které postupně zlepšovaly rychlost přenosu, zabezpečení, spolehlivost a dosah bezdrátové sítě. [3, 4, 5, 6]

Tab. 1.1: Shrnutí standardu 802.11 [5]

Frekvence	Maximální rychlost přenosu	Šířka pásma	Modulace
2,4 GHz	2 Mbit/s	22 MHz	DSSS, FHSS

1.1.2 IEEE 802.11b

Standard IEEE 802.11b (WiFi 1), uvedený společností Apple v roce 1999, pracoval také v pásmu 2,4 GHz a dosahoval přenosových rychlostí až 11 Mbit/s. Pro snížení

rušení a zvýšení rychlosti bylo implementováno modulační schéma Direct-Sequence Spread Spectrum/complementary code keying (DSSS/CCK). Dosah signálu byl cca 38 m ve vnitřních prostorách a cca 140 m v otevřeném venkovním prostoru. [3, 4, 5]

Tab. 1.2: Shrnutí standardu 802.11b [5]

Frekvence	Maximální rychlost přenosu	Šířka pásma	Modulace
2,4 GHz	11 Mbit/s	22 MHz	CCK, DSSS

1.1.3 IEEE 802.11a

Standard IEEE 802.11a (WiFi 2), uveden ve stejném roce jako IEEE 802.11b, oproti jeho předchůdci však pracoval v pásmu 5 GHz a používal modulační metodu Orthogonal Frequency Division Multiplexing (OFDM), který rozděluje dostupnou šířku pásma na několik subkanálů, a tím docílí vyšší maximální přenosové rychlosti až 54 Mbit/s. Avšak vyšší frekvence s sebou nesla i nevýhody jako je větší absorpce signálu zdmi a pevnými objekty. V té době také byly zařízení, které podporovali 5 GHz, mnohem dražší. [3, 4, 5]

Tab. 1.3: Shrnutí standardu 802.11a [5]

Frekvence	Maximální rychlost přenosu	Šířka pásma	Modulace
5 GHz	54 Mbit/s	5/10/20 MHz	OFDM

1.1.4 IEEE 802.11g

Standard IEEE 802.11g (WiFi 3), který byl představen v roce 2003, dosahoval rychlosti až 54 Mbit/s, stejně jako IEEE 802.11a, avšak v pásmu 2,4 GHz. Těchto rychlostí dosahoval díky modulační metodě OFDM, stejně jako u IEEE 802.11a, a dalším zlepšení. [3, 4, 5]

Tab. 1.4: Shrnutí standardu 802.11g [5]

Frekvence	Maximální rychlost přenosu	Šířka pásma	Modulace
2,4 GHz	54 Mbit/s	5/10/20 MHz	OFDM

1.1.5 IEEE 802.11n

Standard IEEE 802.11n (WiFi 4), představen v roce 2009, používal pásma 2,4 GHz a 5 GHz (ne obě pásma zároveň, pouze jedno), díky tomu byl tento standard kompatibilní se zařízeními, které byly postaveny na standardu IEEE 802.11a/b/g. Šířka pásma byla 40 MHz a dosahoval přenosové rychlosti až 600 Mbit/s. Této rychlosti bylo dosaženo, mimo jiné, použitím modulace 64 - QAM (Quadrature amplitude modulation - Kvadraturní amplitudová modulace) a Multiple-Input Multiple-Output (MIMO) technologie. Zařízení s touto technologií využívají vícero antén pro vytvoření vícero datových toků současně, aby mohli přenášet více dat mezi dvěma zařízeními najednou, avšak bylo nutné aby přijímací i odesílací strana byla vybavena MIMO technologií a vícero anténami. Teoretický dosah ve vnitřních prostorách byl cca 70 m, což bylo velké zlepšení oproti předchozím standardům. [3, 4, 5, 7]

Tab. 1.5: Shrnutí standardu 802.11n [5]

Frekvence	Maximální rychlost přenosu	Šířka pásma	Modulace
2,4/5 GHz	600 Mbit/s	20/40 MHz	MIMO-OFDM, až 64-QAM

1.1.6 IEEE 802.11ac

Standard IEEE 802.11ac (WiFi 5), byl představen v roce 2013 a pracoval v pásmu 5 GHz. Používal technologii Downlink Multi-user MIMO (DL MU-MIMO), tedy na rozdíl od předchozího standardu dokáže zařízení pomocí vícero antén odesílat data vícero zařízením najednou. Šířka pásma se zvětšila na 80 až 160 MHz a použitím vyššího řádu modulace až 256 - QAM, tyto změny přispěly k zredukování odezvy a zlepšení přenosové rychlosti na teoretickou maximální rychlost 6,933 Gbit/s. Také již nebylo nutné, aby přijímací zařízení bylo vybaveno technologií MU-MIMO. [3, 4, 5, 7]

Tab. 1.6: Shrnutí standardu 802.11ac [5]

Frekvence	Maximální rychlost přenosu	Šířka pásma	Modulace
5 GHz	693 Mbit/s	20 MHz	DL MU-MIMO OFDM, až 256-QAM
	1600 Mbit/s	40 MHz	
	3467 Mbit/s	80 MHz	
	6933 Mbit/s	160 MHz	

Někteří prodejci však kombinovali technologii Wifi 4 a Wifi 5 tak, aby jejich produkt pracoval jak na 5 GHz tak na 2,4 GHz pásmu a tím docílili kompatibility jejich zařízení se standardy IEEE 802.11a/b/g/n. [4]

1.1.7 IEEE 802.11ax

Standard IEEE 802.11ax (WiFi 6/WiFi 6E) se v roce 2020 stal nejnovějším WiFi standardem. Implementací technologií, jako jsou OFDMA, uplink/downlink (UL/DL) MU-MIMO a 1024 - QAM, dosahuje rychlostí přenosu dat až 9,6 Gbit/s. WiFi 6 pracuje v pásmu 2,4 GHz a 5 GHz, což umožňuje kompatibilitu se standardy IEEE 802.11a/b/g/n/ac, a WiFi 6E pracuje v pásmu 6 GHz.[3, 4, 5, 7]

Tab. 1.7: Shrnutí standardu 802.11ax [5]

Frekvence	Maximální rychlost přenosu	Šířka pásma	Modulace
2,4/5/6 GHz	1147 Mbit/s	20 MHz	UL/DL MU-MIMO OFDMA, až 1024-QAM
	2294 Mbit/s	40 MHz	
	4804 Mbit/s	80 MHz	
	9608 Mbit/s	80+80 MHz	

1.2 Media Acces Control (MAC) Adresa

MAC adresa je jedinečný identifikátor přidělený každému síťovému zařízení při jeho výrobě. Skládá se z 12 hexadecimálních znaků (48 bitů) rozdělených do šesti skupin, kdy první polovina je přidělena na základě výrobce síťové karty a je pro všechny karty od stejného výrobce totožná a druhá polovina je unikátní pro každý výrobek. Každé síťové rozhraní má svoji MAC adresu, tedy pokud má zařízení vstup pro kabelové síťové připojení a současně je vybaveno technologií bezdrátového síťového připojení, ať už WiFi nebo Bluetooth, v systému budou zobrazeny dvě MAC adresy. Pomocí MAC adresy se identifikují zařízení v lokálních sítí a používá se v druhé vrstvě (Linkové vrstvě) Open Systems Interconnection (OSI) modelu, který vkládá MAC adresu zdroje a cíle do záhlaví každého datového rámce aby byla zajištěna komunikace mezi uzly. [8]

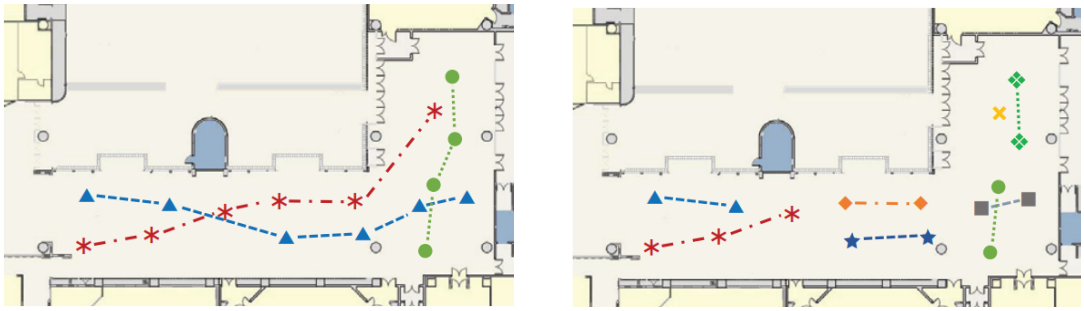
1.2.1 Randomizace MAC adresy

V dnešní době většina výrobců nositelné elektroniky implementuje do svých zařízení i takzvanou randomizaci MAC adresy, čímž se snaží omezit možnosti sledování pohybu zařízení (viz Obr. 1.1), tedy i osoby, která jej nosí. Zařízení s touto technologií

při aktivním skenovaní, tedy odesílání probe requestů, používá náhodně vytvořenou MAC adresu, kterou mění po různých intervalech, místo své originální. [9]

MAC adresy se dále mohou měnit při přechodu mezi sítěmi, ale v jedné síti zůstává stejná MAC adresa i po odpojení a připojení ke stejné síti. Tomuto se říká stálá randomizace (persistent randomization). [10]

Nebo se MAC adresa může měnit při navázání nového připojení ke stejné síti, nebo po 24 hodinách kdy nedošlo k odpojení a připojení zařízení k dané síti a v některých dalších případech. Tomuto se říká nestálá randomizace (non-persistent randomization). Tuto randomizaci však uživatel musí obvykle manuálně zapnout, v základu je u většiny zařízení použita stálá randomizace. [10]



(a) Trajektorie bez MAC randomizace (b) Trajektorie s MAC randomizací

Obr. 1.1: Porovnání výsledných trajektorií sledování při pohybu zařízení s a bez MAC randomizace [9]

1.3 Adress Resolution Protocol (ARP) [11]

Je to protokol, který umožňuje uzlům v sítí zjišťovat MAC adresy odpovídající konkrétní síťovým adresám. Slouží jako spojovací článek mezi síťovou a linkovou vrstvou OSI modelu. Nejlépe si funkci vysvětlíme na příkladu:

Mějme počítač a mobilní telefon (*PC* a *MT*), které jsou připojeny na stejnou lokální síť, *PC* je připojeno pomocí ethernetového kabelu a *MT* je připojen k přístupovému bodu (AP) technologií WiFi. *PC* chce poslat data *MT*, ale zná pouze jeho IP adresu a pro doručení dat je potřeba MAC adresa. Nyní mohou nastat 2 možné situace:

1. *PC* se podívá, zda k IP adrese *MT* nemá již přiřazenou MAC adresu z předchozí komunikace do *ARP cache*, kde jsou tyto informace po určitou dobu uschovávány pro zrychlení komunikace. Pokud zde nenajde MAC adresu *MT* následuje případ číslo 2.

2. *PC* odešle ARP dotaz (*ARP request*) který obsahuje IP adresu *MT* a broadcastovou MAC adresu (FF:FF:FF:FF:FF:FF) a odešle se tedy všem zařízením které jsou připojené na stejnou lokální síť (WiFi i Ethernet). *MT* jako jediné zařízení odešle zpět ARP odpověď (*ARP response*) a zároveň všechna zařízení které obdrželi ARP dotaz od *PC* si uloží jeho MAC adrasu do *ARP cache* pro zrychlení budoucí možné komunikace.

Nyní již *PC* zná MAC adresu cílového zařízení (*MT*) a může odeslat data.

1.4 Vybrané modulační technologie WiFi

Nyní si trochu podrobněji popíšeme vybrané modulační technologie použité v různých standardech WiFi.

1.4.1 Direct-Sequence Spread Spectrum (DSSS)

DSSS je modulační technologie primárně určená pro snížení celkového signálového rušení. Docíleno je toho tak, že vysílaný signál má větší šířku než samotná původní informace. To znamená, že každý jednotlivý bit určený k přenosu je nejdříve modulován početnější sekvencí bitů kdy tyto sekvence mají pseudonáhodný charakter (např. Barkerův kód) a znalost této sekvence je využita i na přijímači k demodulaci a získání originálních dat. Pod modulací si můžeme představit například i logickou operaci XOR, kdy vysílaná sekvence bitů je výsledkem operace XOR původního bitu a pseudonáhodné sekvence. Výsledná sekvence po modulaci jednoho bitu má stejný počet bitů, jako pseudonáhodná sekvence použitá pro modulaci. [14, 15]

Tab. 1.8: Ukázka modulace jednoho bitu operací XOR

Pseudonáhodná sekvence	1	1	0	1	0
Původní bit	1				
výsledná sekvence	0	0	1	0	1

Další výhodou této modulace je složitost odposlouchávání vysílaného signálu, vzhledem k tomu že data jsou pseudonáhodnou sekvencí zároveň šifrovaná, tak bez znalosti této sekvence je velmi obtížné získat originální data. Samotná detekce takového signálu je složitá, jelikož vysílací výkon je rozprostřen do mnohem širšího frekvenčního pásma a ostatním uživatelům se může jevit jako náhodný šum. [14, 15]

1.4.2 Frequency-hopping spread spectrum (FHSS)

Pro stejný účel jako DSSS byla vyvinuta i modulace FHSS. Tato metoda rozděluje dostupnou šířku pásma kanálu na menší subkanály a vysílaný signál rychle přeskakuje mezi jednotlivými subkanály daném pořadí, které zná jen vysílací a přijímací zařízení. Pokud je některý z použitých subkanálů rušen, tak je vysílací signál ovlivněn tímto rušením jen na krátkou dobu. Podobně jako u DSSS je i zde velmi obtížné odposlouchávat přenášená data bez znalosti pořadí přechodu mezi subkanály. Dále dělíme rychlost přeskakování mezi subkanály na Fast Hopping (FFH) a Slow Hopping (SFH). Při SFH je přeneseno více jak jeden bit na jednom subkanále než přeskočí na další subkanál a při FFH se během přenosu jedno bitu několikrát přeskočí na další subkanály. [16, 17]

Adaptive frequency hopping (AFH)

Je principiálně stejný jako FHSS, pouze implementuje funkci, která klasifikuje jednotlivé subkanály na „Dobré“ a „Špatné“. Subkanál je klasifikovaný jako „Špatný“, pokud se na něm nachází silné rušení. AFH vybírá pro přenos pouze subkanály klasifikované jako „Dobré“. Velkou výhodou tedy je, že se dokáže aktivně vyhýbat subkanálům, které jsou buď přetížené, nebo jinak rušené. [16, 17]

1.4.3 Frequency division multiplex (FDM)

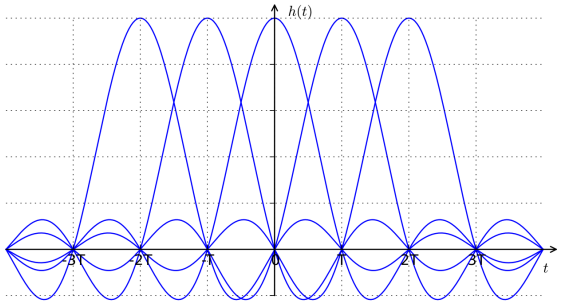
V této modulaci se rozděluje dostupná šířka kanálu na několik nepřekrývajících se subkanálů, které jsou odděleny ochrannými pásmy. Takto je možné přenášet několik nezávislých signálů najednou bez vzájemného rušení a tím je docíleno vyšší přenosové rychlosti. [18]

Orthogonal frequency-division multiplexing (OFDM)

Tato modulace vychází z FDM, ale rozděluje kanál na subkanály které jsou vzájemně ortogonální tzn. maximum každé subnosné frekvence se překrývá s minimy ostatních subnosných frekvencí (viz Obr. 1.2). Tímto rozdělením docílíme větší hustoty subkanálů na stejné šířce kanálu (oproti FDM) bez toho, aby se navzájem rušily. Výsledkem je vyšší přenosová rychost. [19]

Orthogonal frequency-division multiple access (OFDMA)

Je to verze ODFM, která dovoluje přijímat data od více uživatelů zároveň tím, že přiřazuje sety subkanálů pro jednotlivé uživatele kteří pak mohou po těchto přiřazených setech posílat data zároveň, ale s malou rychlostí přenosu. [20]



Obr. 1.2: Ortogonální frekvence [19]

1.4.4 Multiple-input and multiple-output (MIMO) / Single-user MIMO (SU-MIMO)

Tato technologie využívá více antén na vysílacích a přijímacích zařízení, na rozdíl od předchozí technologie SISO (Single-Input Single-Output, tedy jeden vstup jeden výstup), kde byly odrazy signálu od překážek (vícecestné šíření) nežádoucí a představovali rušení, zvýšení chybovosti či snížení rychlosti přenosu, se zde využívá vícecestného šíření rádiového signálu na stejném kanálu pro zvýšení přenosové rychlosti a zvýšení odstupu signál-šum. Dále je nutné aby počet přijímacích antén byl vyšší nebo stejný jako počet vysílacích antén. [21]

Pro zvýšení odstupu signál-šum a dosahu signálu, vysíláme ze všech antén stejnou kopii dat současně a přijímač tak může porovnávat a kombinovat přijímané signály, a tím zmenší chybovost přijímaných dat. [21]

Pro zvýšení přenosové rychlosti, antény paralelně vysílají různá data, a tak vysílá větší množství dat najednou, tedy zvýší přenosovou rychlost. To však vede ke zvýšení chybovosti a není vhodné pro použití v radiově rušeném prostředí. [21]

Tyto dvě konfigurace je možné i kombinovat, například pokud máme vysílač se třemi anténami mohou dvě z nich vysílat totožná data a poslední vysílá jiné data.

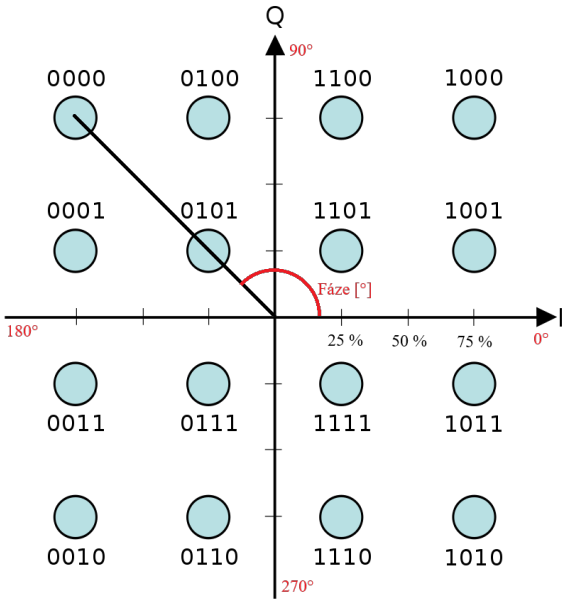
Multi-user MIMO (MU-MIMO)

Tato úprava původního MIMO (SU-MIMO), přidává možnost komunikace jednoho bezdrátového přístupového bodu (AP) s více uživateli zároveň. Tím by mělo být docíleno mnohem lepšího rozprostření dostupné přenosové rychlosti mezi více uživatelů, jelikož nemusí jednotlivá zařízení čekat až budou moci komunikovat s AP jako tomu bylo u SU-MIMO. [22]

1.4.5 Quadrature amplitude modulation (QAM)

QAM je modulační technologie, která pomocí modulace amplitudy a fáze vysílaného signálu mapuje sekvenci bitů, kdy délka této sekvence je závislá na řádu modulace (nejčastěji sudé mocniny 2), na jeden symbol. Pro zvýšení řádu modulace bez zvýšení chybovosti je nutné zvýšení odstupu signál-šum buď zvýšením energie přenosu, snížením okolního šumu nebo obojím.

Pro příklad si zde uvedeme jak by mohla vypadat modulace sekvence bitů 0000 pomocí 16-QAM. Z obrázku 1.3 vidíme, že by výsledný symbol měl 75% velikost amplitudy a fázi 135°.



Obr. 1.3: Konstelační diagram modulace 16-QAM

1.5 Proces navázání spojení zařízení s WiFi sítí [24, 25]

Proces vyhledávání a navazování spojení s WiFi sítěmi se dělí do několika fází, znalost a funkce těchto fází nám usnadní porozumět tomu, jak je možné detekovat zařízení s aktivní WiFi technologií.

Skenování

Ve fázi skenování se provádí aktualizace, nebo potvrzení seznamu dostupných sítí v okolí zařízení, které je vyhledává. Existují dva druhy skenování: aktivní a pasivní skenování.

Aktivní skenování je spouštěno periodicky na skenujícím zařízení, kdy zařízení vysílá takzvané Probe Request rámce, postupně na všech kanálech, a přístupové body (případně jiné zařízení, v případě Ad-Hoc sítí), které tyto rámce „uslyší“, odpoví pomocí Probe Response rámce. Skenující zařízení se také může dotazovat pouze na jedno konkrétní zařízení a cíl požadavku je stanoven pomocí identifikátoru sítě BSSID (MAC adresa cílového zařízení) a SSID (název cílové sítě).

Při pasivním skenování skenující zařízení pouze naslouchá tzv. Beacon rámcům, které periodicky vysílají přístupové body, a zpracovává je, aby zjistil kompatibilitu obou zařízení. Pokud je však síť skrytá (skryté SSID), tak Beacon rámce nevysílá a nelze jí tak pomocí tohoto typu skenování zjistit, ani se k ní připojit.

Asociace

Tato fáze je zásadní pro ověření identity zařízení a navázání spojení s přístupovým bodem. Provádí se pomocí 4 po sobě jdoucích rámců zvaných Authentication request, Authentication response, Association request a Association response. Po přijetí Association response rámce zařízením, je navázáno spojení na Linkové vrstvě (2. vrstva modelu OSI).

Autentizace

Pokud je síť chráněna šifrovacím mechanismem, například WPA2, tak následuje fáze autentizace, která se skládá ze 4 rámců, kdy uživatel musí zadat heslo.

DHCP

V této fázi zařízení bude komunikovat s DHCP serverem, což může být samostatný server nebo je součástí přístupového bodu (AP), vyžádá si od něj IP adresu a DHCP

server mu přiřadí volnou IP adresu. Tím je zařízení úspěšně připojeno k bezdrátové síti.

1.6 Internet of Things (IoT)

IoT označuje zařízení se senzory, akčními členy, softwarem a dalšími technologiemi, která se připojují a vyměňují si data s jinými zařízeními a systémy prostřednictvím internetu, nebo jiných komunikačních sítí. S těmito zařízeními se nejčastěji setkáváme v domácnosti v podobě chytrých žárovek, termostatů, zásuvek, vypínačů, robotických vysavačů a nespočet dalších chytrých zařízení, které dohromady tvoří to, čemu říkáme chytrá domácnost. Mezi další prostředí, ve kterých se IoT zařízení používají, patří například kancelářské, zdravotnické nebo městské. [33, 34]

2 ISM pásma

Industrial, Scientific and Medical (ISM) pásma, jsou bezlicenční rádiová frekvenční pásma a jejich používaní není zpoplatněno. Primárně jsou tyto pásma, jak zkratka napovídá, určeny pro průmyslové, vědecké a zdravotnické účely. Jako příklad netelekomunikačního zařízení, které používá toto pásmo a všichni jej známe, je mikrovlnná trouba, která pracuje na frekvenci 2,4 GHz. Vzhledem k tomu, že taková zařízení ruší rádiovou komunikaci zařízeních na stejné frekvenci, není proto vodné toto pásmo využívat pro tento účel. Navzdory tomu se nyní hojně používá pro vytváření lokálních bezdrátových sítí (WiFi), nebo pro bezdrátovou komunikaci na krátké vzdálenosti (Bluetooth, NFC (near-field communication), ovládání garážových vrat). Mezi nejznámější pásma spadající do ISM jsou 2,4 GHz (2,4 - 2,5 GHz) a 5 GHz (5,725 - 5,825 GHz). [12, 13]

3 Bluetooth

Bluetooth je bezdrátová technologie, která umožňuje zařízením komunikovat mezi sebou. Pro svoji komunikaci používá, podobně jako WiFi, vysokofrekvenční bezlicenční ISM pásmo 2,402 - 2,480 GHz. Technologie Bluetooth se primárně používá pro připojení periferií k počítačům nebo mobilním telefonům, používá k tomu vícero komunikačních topologií, od point-to-point přes broadcast po mesh, což umožňuje vytváření spolehlivých, rozsáhlých sítí zařízení. [26, 27]

Zařízení vybavené technologií Bluetooth, budu dále označovat jako „Bluetooth zařízení“.

3.1 Verze Bluetooth

Technologie Bluetooth od jeho uvedení v roce 1999 prošla mnoha změnami a jednotlivé verze si zde přiblížíme.

3.1.1 Bluetooth 1

První verze, Bluetooth 1.0, byla uvedena v roce 1999 s rychlostí přenosu až 732,2 kbit/s a dosahem 10 m, hned 2 roky nato, v roce 2001, byla vydána verze Bluetooth 1.1, která zlepšovala interoperabilitu, spolehlivost a zpětnou kompatibilitu. Po dalších dvou letech, v roce 2003, přišla verze Bluetooth 1.2, která přinesla rychlejší párování a rychlost přenosu až 1 Mbit/s. Také byla přidána funkce Adaptive Frequency Hopping (AFH), což předcházelo rušení od dalších bezdrátových technologií, jako například WiFi. V této verzi bylo docíleno i zlepšení kvality zvuku, za cenu vyšší latence díky implementování Extended Synchronous Connections (eSCO). [28, 29, 30]

3.1.2 Bluetooth 2

V roce 2004 byla představena verze Bluetooth 2.0, přičemž nejdůležitější bylo přidání podpory pro Enhanced Data Rate (EDR), rychlost přenosu dat tak dosahovala až 2,1 Mbit/s, jako další byla snížena spotřeba oproti 1. verzi. Také se zlepšil dosah až na 30 m. Vylepšení zabezpečení se dočkala verze 2.1, vydána v roce 2007, použitím nového párovacího systému Secure Simple Pairing (SSP), byla také přidána nová funkce, Extended Inquiry response (EIR), která poskytuje při dotazování více informací, a tak zlepšuje filtraci zařízení před připojením. [28, 29, 30]

3.1.3 Bluetooth 3

Bluetooth 3.0 byla vydána v roce 2009, byla přidána podpora funkce High Speed (HS), která využívala standardu IEEE 802.11 (WiFi) pro přenos dat rychlostí až 24 Mbit/s, tato novinka byla označována jako Alternative MAC/PHY (AMP). Avšak tato funkce spotřebovávala, na poměry Bluetooth zařízení, velké množství elektrické energie, proto často nebyla implementována do příslušenství, jako například bezdrátová sluchátka, jelikož by se výrazně snížila jejich výdrž na jedno nabití. [28, 29, 30]

3.1.4 Bluetooth 4

Verze 4.0, představena v roce 2010, také dosahovala rychlosti přenosu až 25 Mbit/s, podobně jako Bluetooth 3.0, avšak zavádí specifikaci Bluetooth Low Energy (BLE), nebo také Bluetooth Smart, která sice disponuje maximální přenosovou rychlostí pouze 1 Mbit/s, ale má velmi nízkou spotřebu elektrické energie, a proto je vhodná pro malé Internet of Things (IoT) zařízení, například fitness tracker nebo naslouchátko. Pro primární zařízení, např. notebook nebo mobilní telefon, zde byla specifikace Bluetooth Smart Ready, kdy se tyto zařízení chovají jako připojovací hub (uzel) pro Bluetooth Smart zařízení. Bylo také zlepšeno zabezpečení díky šifrovací technologii AES. Dosah byl zvýšen až na 60 m. [28, 29, 30]

V roce 2013 byla uvedena na trh verze Bluetooth 4.1, která snížila rušení od 4G/LTE sítí. Nově bylo možné, aby se zařízení chovalo jako BLE příslušenství a hub (uzel) zároveň. [28, 29, 30]

Verze 4.2, vydána v roce 2014, přinesla vylepšení pro IoT zařízení. Mezi hlavní oblasti, které se dočkaly vylepšení patří zásady ochrany soukromí na linkové vrstvě, profil podpory internetového protokolu (IPSP) verze 6 a nízkoenergetické zabezpečené připojení s prodloužením datových rámců. [28, 29, 30]

3.1.5 Bluetooth 5

V roce 2016 byla představena verze 5.0 s maximální přenosovou rychlostí až 50 Mbit/s, pro BLE až 2 Mbit/s. Mnoho vylepšení se zde týkalo zažízení IoT. Poskytuje různé rychlosti přenosu dat, 125 kbit/s - 2 Mbit/s, v závislosti na vzdálenosti zařízení. Dosah připojení byl zvýšen na až 240 m. [28, 29, 30]

Verze 5.1 v roce 2019 představila první Bluetooth Mesh technologii, která změnila připojení z one-to-one (jeden-na-jednoho) na many-to-many (mnoho-na-mnoho). Také se zlepšila možnost sledování polohy zařízení díky AoA (Angle of Arrival) a AoD (Angle of Departure). [28, 29, 30]

Ve stejném roce byla představena verze 5.2. Největší rozdíl mezi touto a předchozí verzí je přítomnost izochronních kanálů (ISOC). Izochronní kanály pracují se

zařízeními s Bluetooth 5.2 a novější, slouží jako základ pro implementaci Low Energy (LE) audia, což snižuje energetickou náročnost pro zařízení přenášející audio signál. Byl představen vylepšený protokol Enhanced Attribute Protocol(EATT) pro více současných transakcí mezi vysílačem a přijímačem. [28, 29, 30]

V roce 2021, byla na trh uvedena verze 5.3. Je zde odebrána funkce AMP, tedy maximální rychlost datového přenosu je 2 Mbit/s, přinesla vylepšenou kontrolu velikosti šifrovacího klíče, což zlepšilo efektivitu a zabezpečení. Bylo zde vylepšeno periodické odesílání reklamy (Periodic Advertisement Interval) pro větší spolehlivost a také může šetřit energii zařízením které tyto rámce přijímají. Nově bylo představeno dílčí hodnocení připojení (Connection Subrating), které má za úkol přepínat mezi vysokými a nízkými pracovními cykly na základě potřeby, kdy vysoký pracovní cyklus nabízí vyšší přenosovou rychlost na úkor energetické náročnosti a nízký pracovní cyklus je méně energeticky náročný, ale nabízí nižší přenosovou rychlost. [28, 29, 31]

3.2 Detekce Bluetooth zařízení

Metoda detekce zařízení s aktivní technologií Bluetooth se liší podle toho zda je detekované zařízení v Discoverable módu, nebo v Non-Discoverable módu, tedy zda je viditelný pro ostatní zařízení, či nikoliv.

Detekce v Discoverable módu

Detekce zařízení v takovém modů spočívá v odesílání Inquiry požadavků a následném „naslouchání“ odpovědi dotazovaného zařízení. Součástí odpovědi je například: název zařízení, výrobce, specifikace Bluetooth a další.[28, 32]

Detekce v Non-Discoverable módu

Detekce zařízení v takovém módu je velmi časově náročná. Jelikož zařízení neodpovídá na požadavky Inquiry ale pouze na Page rámce a abychom mohli poslat Page rámec, tak je nutné znát MAC adresu cílového zařízení. Bez znalosti MAC adresy je možné pouze postupně procházet všechny existující adresy a na ně posílat tyto rámce, tomuto se říká *brute force search*. Takovýmto způsobem bychom v nejlepším případě hledali, pomocí jednoho skenovacího zařízení, cca 1,4 roku. [32]

Zkrátit tuto dobu lze dvěma způsoby: Zmenšit prohledávaný adresní prostor, tím že známe například výrobce, a tedy zkrátí se prohledávaný prostor na polovinu, nebo zvýšíme počet skenovacích stanic.[32]

4 Raspberry Pi

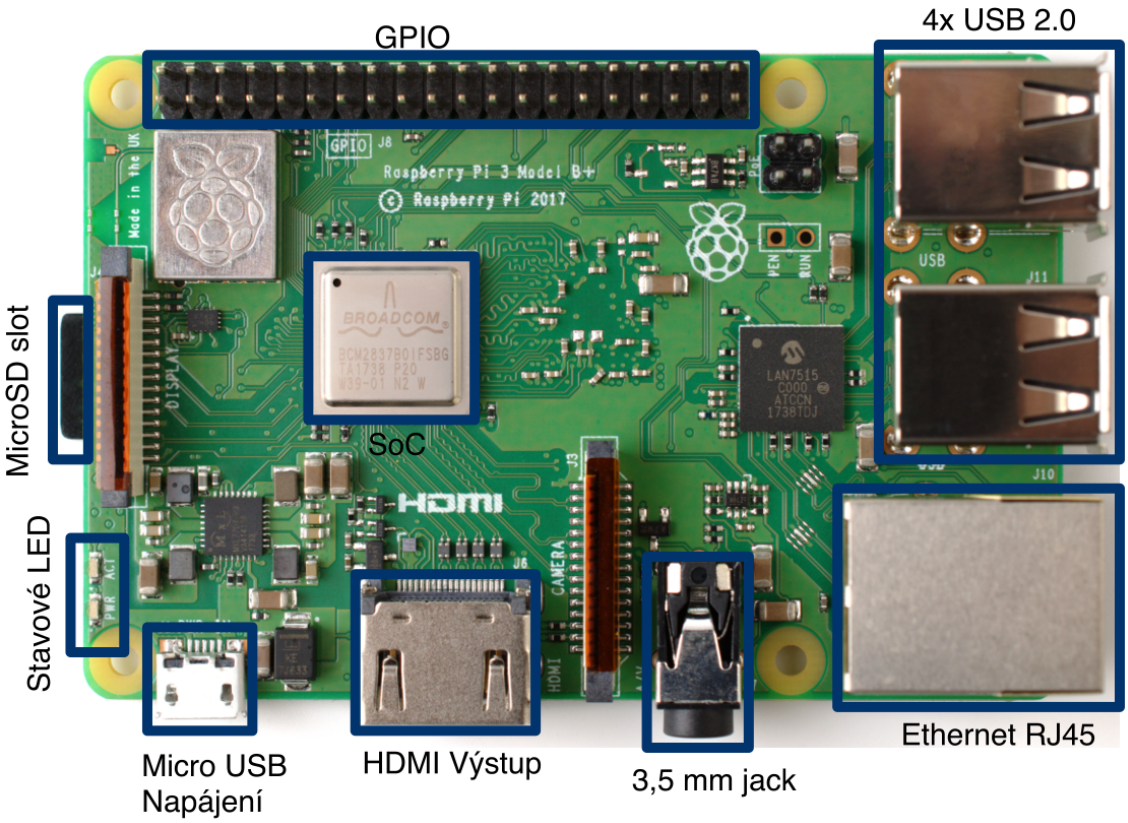
Raspberry Pi je malý jednodeskový počítač, který byl původně vyvinut pro výuku informatiky, ale mnozí nadšenci ho používají v domácnosti i jako malý server, který spolu s externím diskem může sloužit jako vlastní cloudové úložiště, nebo streamovací služba. Díky jeho general-purpose input/output (GPIO), kterým může tento počítač komunikovat s různými senzory a aktuátory, je velmi všestranně použitelný například i v robotice. Počítače Raspberry Pi jsou osazeny, s výjimkou Raspberry Pi Pico, Broadcom SoC (System on Chip) s integrovaným ARM procesorem a grafickou jednotkou, velikost RAM (Random-Access Memory) se pohybuje, v závislosti na verzi, od 264 KB do 8 GB. Jeho Input/Output (I/O) rozhraní se obvykle skládá z USB-A portů, Ethernetového portu, Analogového 3,5mm audio jacku a HDMI. Podporuje také bezdrátové připojení WiFi a Bluetooth. [35, 36]

4.1 Raspberry Pi 3 B+

Bylo vydáno v roce 2018, osazeno SoC BCM2837B0 s čtyřjádrovým, šedesátičtyřbitovým ARM procesorem Cortex-A53 o frekvenci 1,4 GHz a grafickou jednotkou Broadcom VideoCore IV a 1 GB RAM. I/O rozhraní se skládá ze čtyř USB-A portů verze 2.0, jednoho HDMI (rev 1.3), Analogový 3,5 mm audio jack a Gigabitový Ethernetový port s maximální reálnou propustností 300 Mbit/s, kvůli vnitřnímu připojení na USB 2.0. Nalezneme zde podporu pro WiFi IEEE 802.11b/g/n/ac a Bluetooth 4.2 LE. [35, 37]

Tab. 4.1: Porovnání vybraného hardwaru Raspberry Pi 3 B+ a nejnovějšího Raspberry Pi 5 [37, 38]

	Pi 3 B+	Pi 5
Procesor	Cortex-A53	Cortex-A76
Počet jader	4	4
Počet vláken	4	4
Max. frekvence	1,4 GHz	2,4 GHz
Operační paměť	LPDDR2	LPDDR4X-4267
Max. velikost RAM	1 GB	8 GB
WiFi	802.11ac	802.11ac
Bluetooth	4.2 LE	5.0 LE
PCIe	Ne	Ano



Obr. 4.1: Pohled na Raspberry Pi 3 B+ a vyznačení vybraných hardwarových částí

4.2 Raspbian OS Lite

Je operační systém přímo vyvinutý pro zařízení řady Raspberry Pi, založený na linuxové distribuci Debian. Na rozdíl od klasické verse Raspbian OS, není součástí desktopové prostředí, které my potřebovat nebudeme a díky tomu je i méně náročný na velikost paměti SD karty, na kterou je OS nainstalován. [39]

4.3 Kismet

Kismet je bezplatný nástroj pro detekování a sledování bezdrátových sítí a zařízení (WiFi a Bluetooth). Dokáže detekovat a uschovávat informace o síťovém provozu, součástí jsou i informace o adrese zdroje a příjemce rámců. Sledování probíhá pasivně tzn. nevysílá žádně rámce, které by mohly být zachyceny. K tomu je však potřeba síťová karta podporující monitorovací režim. Po spuštění Kismetu můžeme přehledně sledovat detekovaná zařízení i na webovém rozhraní v prohlížeči na adrese: *http://localhost:2501*. [40, 41]

Součástí Kismetu je také takzvaný Remote Capture, to znamená, že je možné odesílat zachycené rámce monitorovacím zařízením na vzdálené zařízení, kde ná-

sledně dochází ke zpracování a uložení těchto rámců. Tento nástroj je velmi užitečný v případě, kdy máme více monitorovacích zařízení, nebo pokud monitorovací zařízení zachytává z většího množství datových zdrojů a není schopen všechny tyto data, z důvodu nízkého výkonu hardwaru, zpracovat a uložit. [41]

4.3.1 Monitorovací režim [42]

Umožňuje WiFi kartě zachytávat rámce bez toho, aby byla připojena k přístupovému bodu nebo ad-hoc síti. Tak můžete monitorovat specifický kanál a není třeba posílat žádné rámce. Pro přepnutí WiFi karty do monitorovacího režimu v operačním systému Linux, můžeme použít tyto příkazy:

```
sudo ifconfig {název_rozhraní} down
sudo iwconfig {název_rozhraní} mode monitor
sudo ifconfig {název_rozhraní} up
```

5 Implementace

V této části bakalářské práce budeme diskutovat o procesu přípravy Raspberry Pi 3 B+ pro detekci zařízení s aktivními technologiemi WiFi a Bluetooth. Dále se zaměříme na funkci Remote Capture programu Kismet, popíšeme důvody použití a způsob, jakým byla tato funkce implementována.

5.1 Hardwarové prostředky detekce

Jelikož integrovaný kombinovaný čip v Raspberry Pi nepodporuje monitorovací mód, a navíc bych jej chtěl využít pro připojení k mé síti, aby nebylo nutné použít ethernetový port, tak jsem pro detekci WiFi zařízení použil externí USB WiFi kartu.

Vzhledem k tomu, že Kismet dokáže pracovat s několika datovými zdroji technologie WiFi najednou, dokonce i sám nakonfiguruje sekvenci přeskoků mezi kanály takovým způsobem, aby spolupracovali co nejefektivněji, tak jsem se rozhodl, že by bylo výhodné použít alespoň dvě externí karty, abych docílil lepšího pokrytí kanálů a byla menší šance, že by nějaké zařízení nebylo detekováno.

První byla externí karta TP-Link Archer T3U Plus s čipem Realtek RTL8812BU která podporuje IEEE 802.11ac a pracuje v pásmu 2,4 a 5 GHz. Druhou byla karta TP-Link TL-WN722N s čipem Qualcomm Atheros AR9271 s podporou IEEE 802.11n, ale pracuje pouze v pásmu 2,4 GHz.

5.2 Instalace Raspbian OS Lite

Pro instalaci operačního systému Raspbian OS Lite do Raspberry Pi 3 B+, jsem následoval několik kroků.

Prvním krokem bylo stažení nejnovější verze Raspberry Pi Imager z oficiálních stránek projektu Raspberry Pi. Po stažení, jsem spustil instalátor (Raspberry Pi Imager) k vytvoření bootovatelné microSD karty a následně jsem byl přivítán průvodcem instalace.

V prvním kroku jsem vybral cílové zařízení, tedy Raspberry Pi 3 B+. Dále jsem pokračoval výběrem operačního systému, což byl výše zmíněný Raspbian OS Lite (64-bit).

Poté jsem pokračoval ve výběru úložiště, kam se měl operační systém nainstalovat. Zde jsem zajistil, aby bylo vybráno správné úložiště, tj. paměťová karta, kterou jsem předem připravil k instalaci.

V dalším kroku jsem provedl úpravy nastavení podle mých potřeb. Nastavil jsem WiFi připojení tím, že jsem zadal jméno (SSID) a heslo zvolené sítě na kterou se má po spuštění Raspberry Pi připojit. Dále jsem vytvořil administrátorský účet

a přiřadil zařízení jméno. V nastavení jsem rovněž povolil SSH a zvolil autentifikaci pomocí hesla, což bylo klíčové pro pozdější vzdálený přístup a správu zařízení.

S potřebnými úpravami provedenými v nastavení jsem spustil instalaci, čímž byl aktivován proces nahrávání operačního systému na paměťovou kartu.

Po vložení microSD karty do Raspberry Pi a spuštění, jsem se pomocí SSH přihlásil do terminálu a provedl aktualizaci balíčků pomocí příkazů `sudo apt update` a `sudo apt upgrade` zajišťujících, že operační systém má nejnovější verze všech potřebných komponent.

5.3 Instalace Kismetu na Raspbian OS Lite

Při instalaci jsem postupoval podle návodu přímo na oficiálních stránkách Kismetu, využil jsem při tom automatically-build úložišť, a to hlavně z důvodu rychlosti instalace, jelikož by kompilace na Raspberry Pi trvala velmi dlouho. Bylo nutné abych správně vybral repozitář, který se volí podle operačního systému a architektury. V mém případě se jednalo o Debian Bullseye (arm64).

Následovalo pouze postupné kopírování příkazů z oficiálních stránek pro instalaci dané verze Kismetu. Během instalace se Kismet zeptá zda chcete nainstalovat jako *Suid-root*, či nikoliv. To znamená, že bude možné spouštět Kismet bez toho, aby byl uživatel *root*. Jde zde o bezpečnostní opatření, jelikož Kismet je rozdělen na dvě části, a to *Kismet server*, který zpracovává zachycené rámce a *Kismet packet datasources*, který zachytává rámce a konfiguruje daná zařízení (WiFi karty) pro zachytávání. Právě konfigurace těchto zařízení často vyžaduje *root* práva. Z toho vyplývá, že pokud Kismet nainstalujeme jako *Suid-root*, tak *root* práva bude mít pouze *Kismet packet datasources* a nikoli *Kismet server*,což je mnohem bezpečnější než abychom spouštěli Kismet se `sudo` a měl tak *root* práva celý Kismet. Zvolíme tedy, že chceme nainstalovat Kismet jako *Suid-root*.

Tímto byla instalace úspěšně dokončena. Už jen zbývalo přidat do skupiny *kismet* můj účet, abych mohl spouštět Kismet bez *sudo* pomocí příkazu:

```
sudo usermod -aG kismet user
```

5.4 Konfigurace Kismetu na Raspberry Pi

Kismet obsahuje několik konfiguračních souborů, které jsou umístěny `/etc/kismet`, ale my se budeme primárně zabývat soubory *kismet.conf* a *kismet_logging.conf*, které obsahují všechny důležité parametry jež bude třeba upravit podle našich potřeb. Všechny parametry jsou přehledně popsány přímo v konfiguračních souborech.

Jako první si v souboru *kismet.conf* nadefinujeme *sources*, což jsou naše zdroje pro zachytávání rámců. Nejdříve, však potřebujeme zjistit jaký název jim přidělil systém, to můžeme zjistit pomocí příkazu `nmcli`. V mém případě to jsou: *wlan1* (první externí WiFi karta), *wlan2* (druhá externí WiFi karta) a *hci0* (integrovaný Bluetooth čip). Do souboru *kismet.conf* tedy připíšeme:

```
source=wlan1:name=WiFi1
source=wlan2:name=WiFi2
source=hci0:name=Bluetooth
```

Jako další jsem si změnil místo kam se mají záznamy z Kismetu ukládat, toto nastavení není nutné, ale pokud to necháme beze změny, tak se záznam uloží do složky, ze které byl Kismet spuštěn, což nemusí být ideální a je možné, že později zapomenete v jaké složce jste Kismet pustili. Toto nastavení se provádí v souboru *kismet_logging.conf* kdy změníme parametr `log_prefix` na celou adresu složky do které chceme ukládat záznamy, já jsem si vytvořil složku *Logs* na adrese `/home/user/Logs` a upravený parametr vypadá takto:

```
log_prefix=/home/user/Logs
```

Toto bylo vše co jsem upravoval. Samozřejmě je možné toho upravit mnohem více, jako je frekvence přeskakování kanálů, v jakém formátu se bude záznam ukládat, filtrování rámců atd., ale pro mé potřeby to takto stačilo.

5.5 Spuštění Kismetu a problémy

Spuštění, po nastavení, se provádí jednoduše příkazem `kismet`. Po inicializaci a nakonfigurování zdrojů, které provede sám Kismet, začne zachytávat rámce pomocí výše nadefinovaných zdrojů. Problém nastal cca 10 minut po spuštění, kdy se začala objevovat tato chyba pro všechny zdroje:

```
Source wifi1 (5FE308BD-0000-0000-0000-984827D50805)
has encountered an error (IPC connection closed)
Kismet will attempt to re-open the source in 5 seconds.
(1 failures)
```

a následovalo toto upozornění:

```
Source wifi1 (5FE308BD-0000-0000-0000-984827D50805)
successfully re-opened
```

Toto se pak začalo periodicky opakovat po cca každé minutě. Při restartování programu se problém objevil znovu a nyní cca 4 minuty po spuštění. Začal jsem tedy hledat zdroj problému. Jako první jsem zkusil restartovat celé Raspberry Pi a pustit

Kismet pouze s jednou WiFi kartou a Bluetooth. První chyba se objevila znovu cca 10 minut po spuštění programu a zase se opakovala, ale s delší periodou oproti prvním testu.

Vzhledem k tomu, že jsem pouze občasně dostal i hlášku, že se Kismet snaží zapsat do logu nové data, ale stále se zapisují ty staré, tak jsem zkusil spustit Kismet bez logování, což se provádí příkazem `kismet -n`. V tomto případě se žádná chyba neobjevila ani po hodině a usoudil jsem tedy, že by mohla být již degradovaná použitá SD karta, či nějaké jiné omezení použitého hardwaru.

Rozhodl jsem se tedy pro to, aby Raspberry Pi konalo pouze funkci zachytávání rámců, které následně bude odesílat na můj server s operačním systémem Ubuntu Server, kde dojde ke zpracování a uložení přijatých rámců. Využiji proto funkci Kismetu *Remote Capture* (viz sekce 4.3). Toto navíc umožní použití více měřících stanovišť, což využiji v kapitole 6.

Konfigurace Remote Capture na serveru

Po instalaci Kismetu na server, která probíhala stejně jako u Raspberry Pi (viz sekce 5.3), je potřeba v konfiguračním souboru *kismet.conf* se ujistit, že je povolený *Remote Capture* (`remote_capture_enable=true`) a nastavený na IP adresu *localhost* (`remote_capture_listen=127.0.0.1`). Jediné co zbývá, je vytvořit SSH tunel z Raspberry Pi (localhost:3501) na server (ip_adresa_serveru:3501), příkaz by vypadal takto:

```
ssh user@10.0.20.3 -L 3501:localhost:3501
```

5.5.1 Spuštění Kismet remote capture

Po vytvoření SSH tunelu spustím Kismet na serveru pouze příkazem (`kismet`). Na straně Raspberry Pi však musíme využít speciálních příkazů pro spuštění *Remote Capture*:

Pro Bluetooth: kismet_cap_linux_bluetooth
Pro WiFi: kismet_cap_linux_wifi

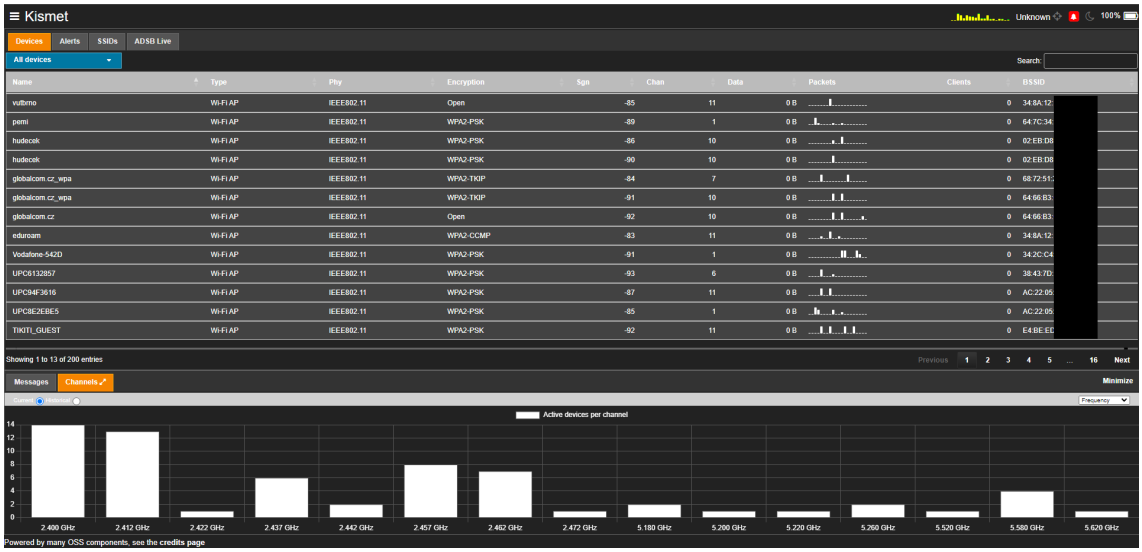
Pro každý zdroj je potřeba jednotlivě spustit *Remote Capture*, tedy v mém případě to budou tři příkazy. Proto bylo vhodné vytvořit skrip, který bude spouštět všechny tři zdroje najednou. Můj skrip vypadá následovně:

```
#!/bin/bash
kismet_cap_linux_bluetooth --connect localhost:3501
--source hci0:name=bluetooth1 --tcp --fixed-gps & \
```

```
kismet_cap_linux_wifi --connect localhost:3501
--source wlan1:name=wifi1.1  --tcp --fixed-gps & \
kismet_cap_linux_wifi --connect localhost:3501
--source wlan2:name=wifi1.2 --tcp --fixed-gps &
```

5.6 Zobrazení a práce s naměřenými daty

Kismet nabízí dvě možnosti jak sledovat měřená data, buď přímo v terminálu, což je při nejmenším nepřehledné, nebo má svoje webové rozhraní, které je přístupné na adrese *http://localhost:2501*. To nám umožňuje přehledně sledovat detekovaná zařízení a můžeme je zde třídit například podle zdroje, který zařízení zachytil, času prvního objevení zařízení, na jaké sítě se již dříve připojilo a mnoho dalšího.



Obr. 5.1: Ukázka webového rozhraní Kismet

Z Obr.5.1 vidíme jak vypadá webové rozhraní. Ve spodní liště je graficky zobrazeno vytížení kanálů v reálném čase, ale je možné přepnout i pro zobrazení historie vytížení kanálů a v podstatě celý zbytek prostoru je vyhrazen pro zobrazení detekovaných sítí či zařízení a jejich popisu. Webové rozhraní se dá jednoduše upravit podle představ uživatele.

5.6.1 Ukládání dat pro další zpracování

Kismet zároveň vše ukládá do svého logu, který má příponu *.kismet*, jedná se o SQL databázi založenou na SQLite3. S touto databází dále pracuji v MATLABu, abych si mohl zobrazit i statistiky, které Kismet nezobrazuje. Je zde i možnost ukládat celé hlavičky zachycených rámců ve formátu *.pcapng*, které se dají nadále zkoumat v programech jako Wireshark, Tshark a další. Tuto funkci jsem však nevyužil.

5.7 Metodika rozmisťování měřících stanic v prostoru

Ideální rozmístění stanic by bylo takové, že by v místě kde by již první měřící stanice nedokázala zachytit rámce by bylo další stanoviště umístěno tak, aby tyto rámce již dokázalo zachytit.

V reálných podmínkách je rozmístění mnohem složitější, jelikož bychom musíme zjistit dosah antén v daném prostředí (tedy kdy zohledňujeme překážky a rušení), a to nejspíše metodou pokus-omyl. I kdybychom přesně změřili ideální vzdálenost mezi měřicími stanovišti tak, aby co nejlépe splňovala podmínky výše, musíme stále brát v potaz realizovatelnost takového rozmístění, tedy zda je pro to dostatečný prostor a přístup k němu, dostupnost internetu pro odesílání rámců serveru, přístup k elektrické energii a ochrana proti přírodním vlivům.

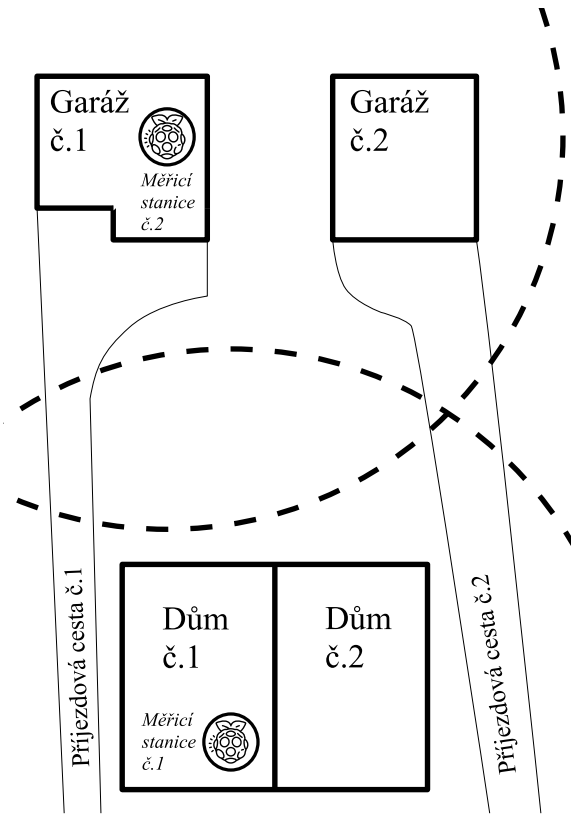
6 Průběh měření a zpracování dat

V této kapitole si ukážeme a popíšeme výsledky tří různých měření.

6.1 Měření č.1

První měření se konalo na pozemku s dvoupatrovým dvojdomem a spojenou zahradou, probíhalo od neděle 24. 3. 2024 18:32 do čtvrtka 28. 3. 2024 16:13.

6.1.1 Rozmístění měřících stanovišť v 2D prostoru



Obr. 6.1: Plánek rozmístění měřících stanovišť v prostoru pro měření č.1

Pro toto měření jsem zvolil rozmístění vyobrazené v Obr.6.1. Čárkované čáry představují odhadovaný dosah měřících stanovišť.

6.1.2 Statistiky a grafy

Počet detekovaných zařízení

Typ zařízení	Počet
BTLE	5169
BR/EDR	8
WiFi Client	7052
WiFi AP	111
WiFi Ad-Hoc	20
WiFi Bridged	74

Tab. 6.1: Počet detekovaných zařízení před filtrací dat

Typ zařízení	Počet
BTLE	4729
BR/EDR	7
WiFi Client	7038
WiFi AP	111
WiFi Ad-Hoc	20
WiFi Bridged	74

Tab. 6.2: Počet detekovaných zařízení po filtraci dat

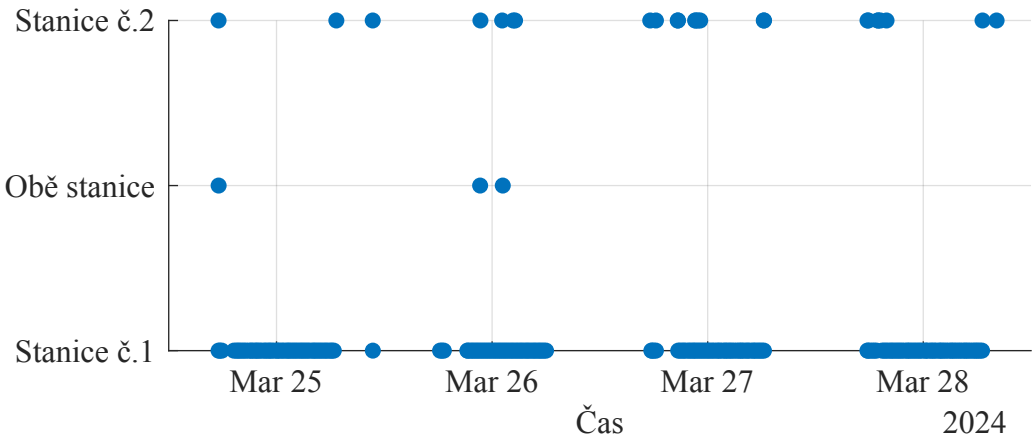
Z tabulky 6.1 vidíme velký počet zařízení Bluetooth, který vzhledem k obecně malému dosahu antén a měřenému prostoru, není reálný. To to je pravděpodobně způsobeno častou změnou MAC adres zařízení, které jsou v dosahu. Po každé, když zařízení změní MAC adresu, kterou odpovídá na inquiry požadavky, je považováno za nové zařízení. Frekvence změn MAC adresy je závislá na výrobci. Ve snaze zredukovat počet těchto duplikátů jsem se pokusil filtrovat zařízení tak, že jsem smazal ty, které za celou dobu měření odeslali pouze jeden rámec. Výsledek vidíme v tabulce 6.2.

Počet WiFi klientů by se také mohl zdát vysoký, avšak toto číslo by reálné být mohlo. WiFi MAC adresy velké většiny zařízení se mění pouze při skenování, nebo změně sítě (viz sekce 1.2.1). Vzhledem k tomu, že v současné době téměř každá domácnost s alespoň jedním chytrým zařízením, které se připojuje k internetu prostřednictvím WiFi, má svou vlastní síť, je pravděpodobnost výskytu duplicitních záznamů minimální.

Zařízení WiFi Bridged představují ty zařízení, které jsou do sítě připojeny ethernetovým kabelem. Mohlo by se jednat i o zařízení které je připojené ke stejné síti kterou detekuje měřící stanice, ale je připojeno přes např. WiFi Extender, kde nevidíme daný WiFi Extender ani přímo zařízení.

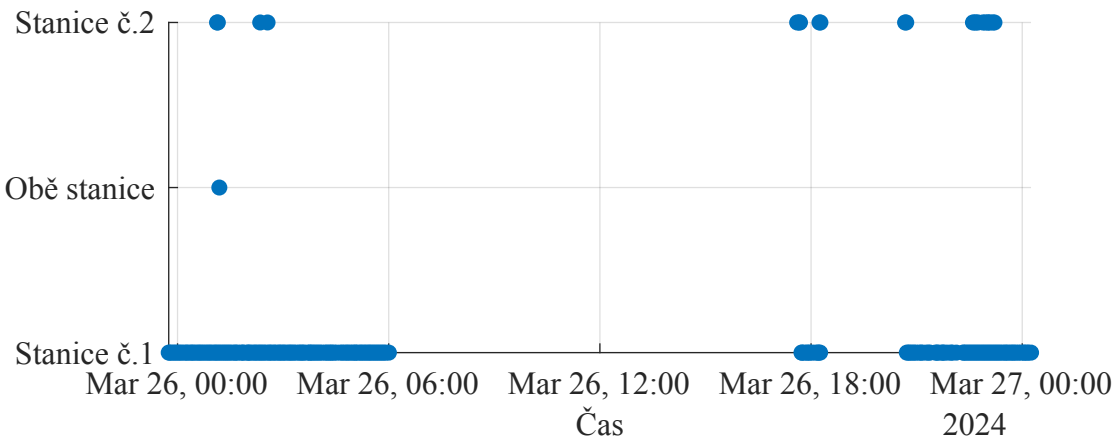
Sledování polohy zařízení

Pro určení polohy zařízení jsem použil zachycené rámce z WiFi komunikace.



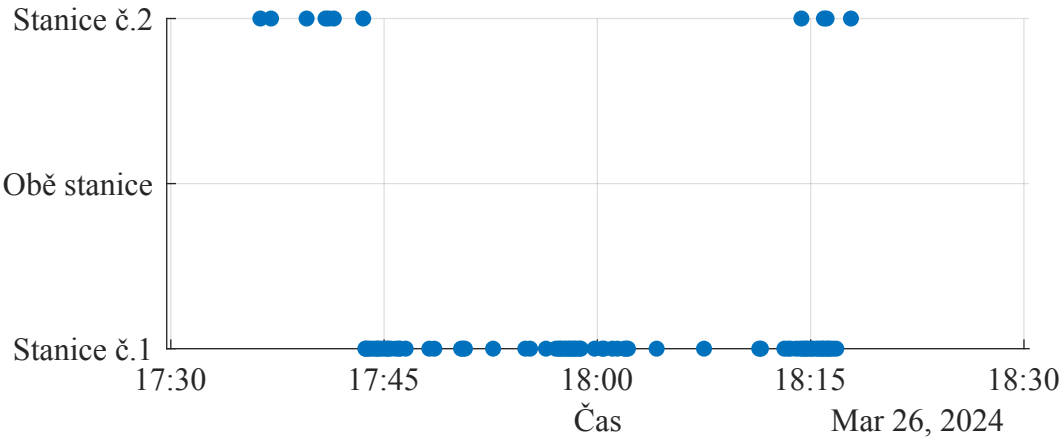
Obr. 6.2: Sledování pohybu zařízení

V obrázku 6.2 vidíme pohyb zařízení v čase mezi stanicemi. Každá modrá tečka představuje zachycený rámec ze zařízení, rámec je klasifikován podle toho, jaká stanice jej zachytila, popřípadě pokud byl stejný rámec zachycen oběma stanicemi.



Obr. 6.3: Sledování pohybu zařízení (přiblížené na 1 den)

Z obrázku 6.3 dokážeme poznat, že zařízení kolem 6. hodiny opustí měřený prostor a vrátí se až kolem 18. hodiny. Můžeme tedy usoudit že osoba nosící toto zařízení odchází na tuto dobu do práce, jelikož se toto chování opakuje pro každý den měření.

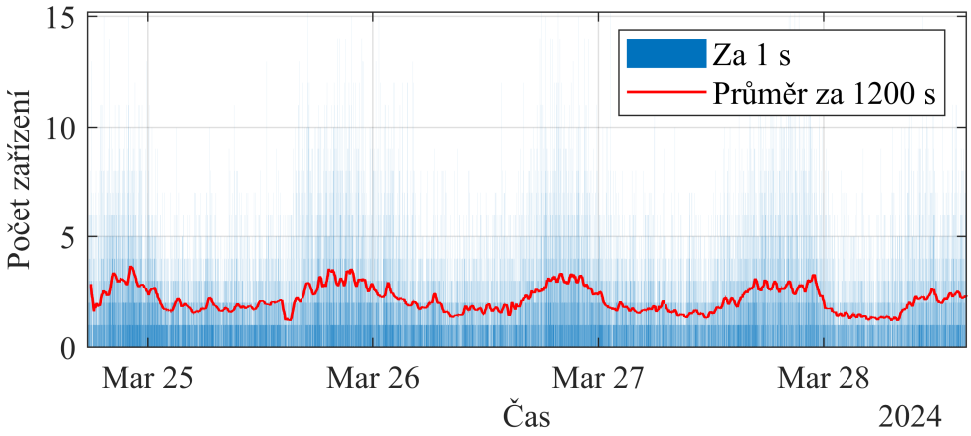


Obr. 6.4: Sledování pohybu zařízení (přiblížené na 1 hodinu)

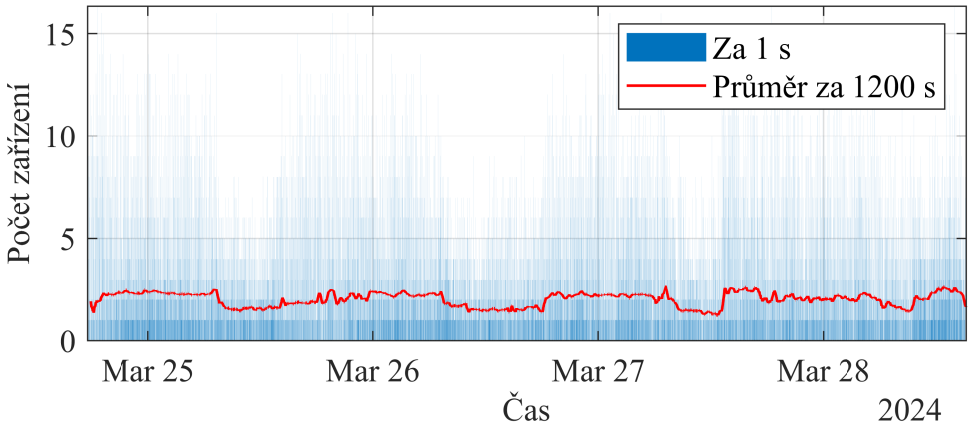
Po dalším přiblížení na čas příchodu z práce (viz Obr. 6.4), vidíme, že je zařízení nejdříve zachyceno stanicí č.2, která se nachází v garáži (viz Obr. 6.1) až poté stanicí Domě. Z toho se dá dále vyvodit, že osoba přijela osobním vozem z práce, které zaparkovala v garáži a následně se vrátila domů.

V cca 18:17 bylo zařízení znovu zachyceno stanicí č.2 a následně opustilo měřený prostor, což nám naznačuje že osoba opět osobním vozem opustila měřený prostor.

Počet aktivních zařízení



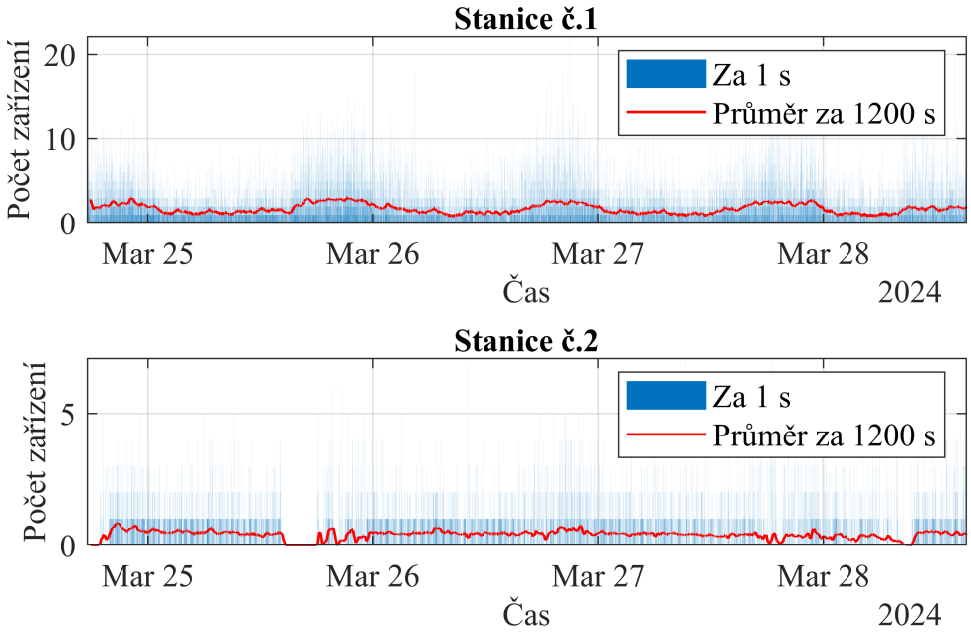
Obr. 6.5: Graf počtu aktivních WiFi zařízení v průběhu měření



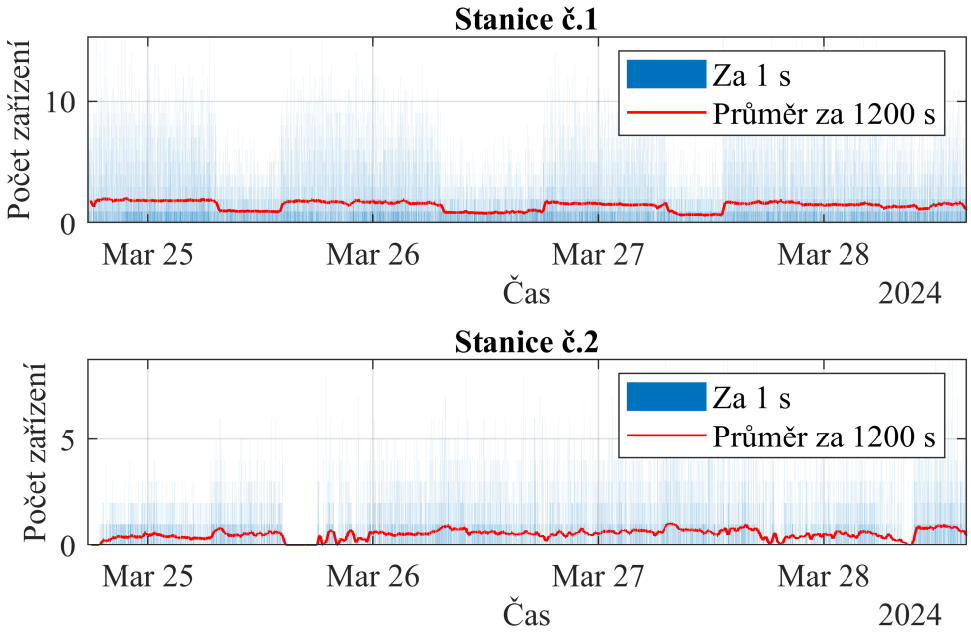
Obr. 6.6: Graf počtu aktivních Bluetooth zařízení v průběhu měření

Na grafu v obrázku 6.5, podle očekávání, pozorujeme pokles počtu aktivních WiFi zařízení okolo 6. hodiny ranní, kdy většina lidí odchází do zaměstnání nebo školy a nárůst počtu aktivních zařízení kolem 15. hodiny, kdy se tito lidé zase vrací domů.

V případě počtu aktivních Bluetooth zařízeni (viz Obr. 6.6) to není tak jednoznačné. Sice zde také pozorujeme pokles počtu aktivních zařízení v podobném časovém okně jako v případě počtu aktivních WiFi zařízení, avšak ne tak zřetelně.



Obr. 6.7: Grafy počtu aktivních WiFi zařízení v průběhu měření (rozlišeno podle stanice)



Obr. 6.8: Grafy počtu aktivních Bluetooth zařízení v průběhu měření (rozlišeno podle stanice)

V obrázku 6.7 vidíme, že aktivita v okolí měřící stanice č.1 je podle předpokladu významně vyšší, než je tomu u stanice č.2 a taky nám dává mnohem větší představu o pohybu lidí.

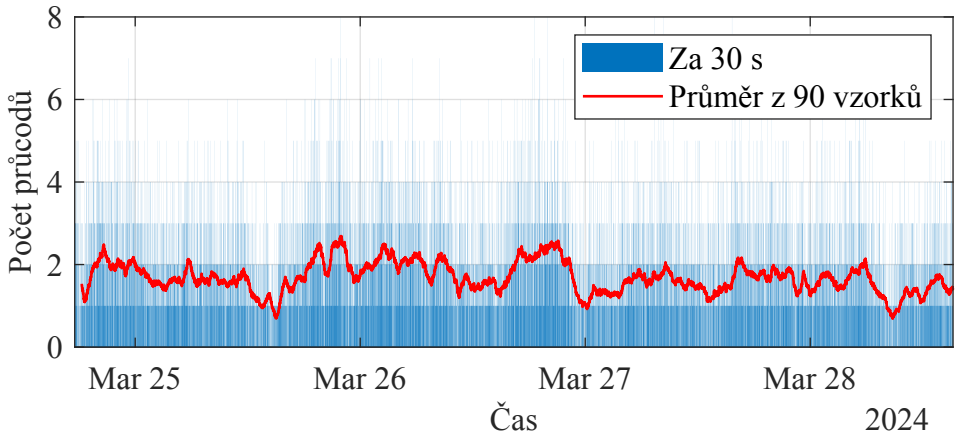
Z grafů v obrázku 6.8 opět pozorujeme předpokládaný rozdíl počtu aktivních zařízení v okolí stanic a z grafu pro stanici č.1 je zřejmé, že existuje pravidelný vzorec poklesu a nárůstu aktivních Bluetooth zařízení, který se opakuje každý den měření s výjimkou posledního dne.

Tento vzorec je pravděpodobně také spjatý s pohybem osob, který jsem popsal výše.

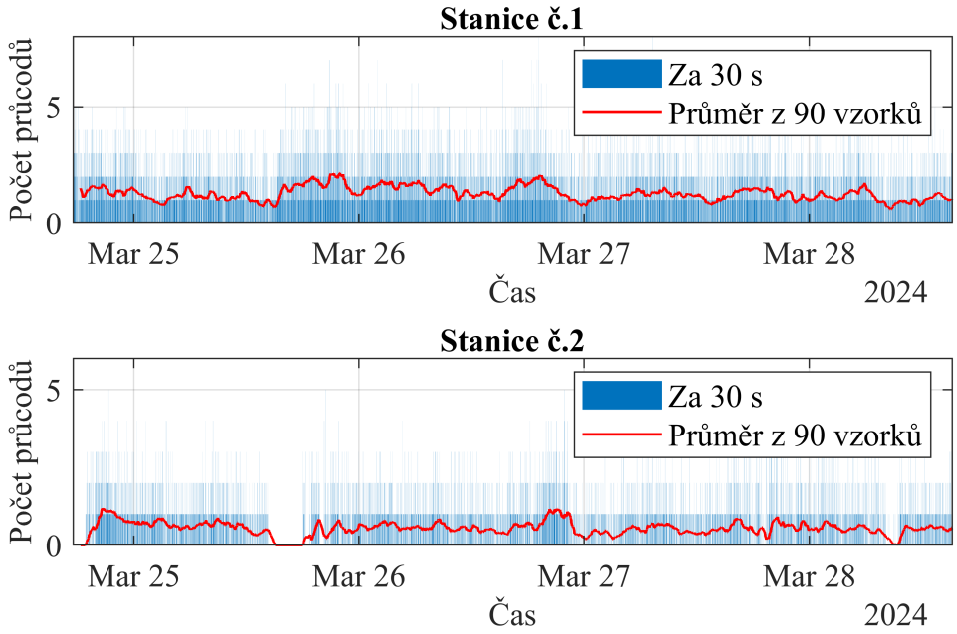
Počet průchodů stanovišti

Jako průchod, jsem definoval takové chování, při kterém stanice zachytí alespoň jeden rámec od zařízení v zadaném časovém bloku (v tomto případě 30 sekund) a v následujících dvou časových blocích (následujících 60 sekund) už žádný rámec od tohoto zařízení nezachytí. Toto chování by mělo představovat zařízení, které vstoupí do měřeného prostoru a následně neprodleně jej opustí.

Tento způsob klasifikace má za úkol vyřadit zařízení, které periodicky odesílají rámce, ale zůstávají dlouhodobě v okolí měřících stanic. Stále se však může stát, že nějaké nehybné zařízení v prostoru měření bude odesílat rámce odesílat periodicky rámce s periodou větší než tři časové bloky (v tomto případě větší než 180 sekund), kdy tento algoritmus nedokáže rozpoznat, že se nejedná o průchod.

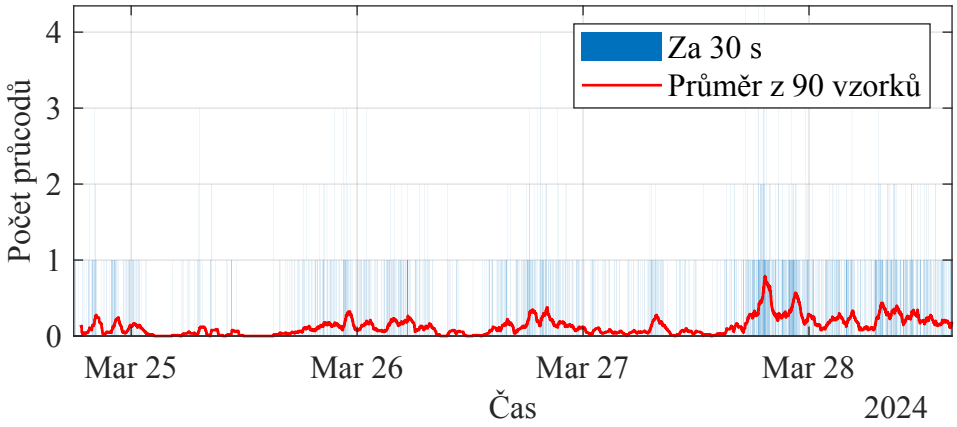


Obr. 6.9: Graf počtu průchodů WiFi zařízení měřícími stanovišti

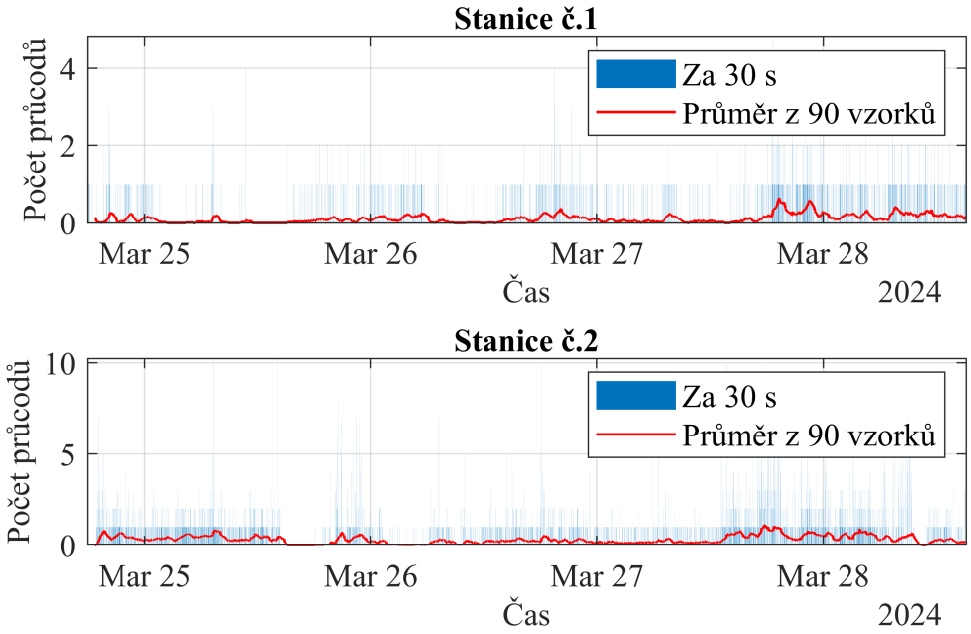


Obr. 6.10: Graf počtu průchodů WiFi zařízení měřícími stanovišti

Jak je vidět z grafů v obrázcích 6.9 a 6.10 tak i přes moje snahy se pravděpodobně nějaké nehybné zařízení stále započítávalo jako průchody, jelikož je nepravděpodobné, že by mezi půlnocí a 5. hodinou ranní konstantně procházely stanovišti průměrně 2 zařízení. V grafech lze pozorovat pravidelné vzory, které naznačují denní cykly. Zvýšený počet příchodů v určitých časech odpovídá pracovním hodinám, zatímco nižší počet příchodů odpovídá nočním hodinám.



Obr. 6.11: Graf počtu průchodů Bluetooth zařízení měřícími stanovišti



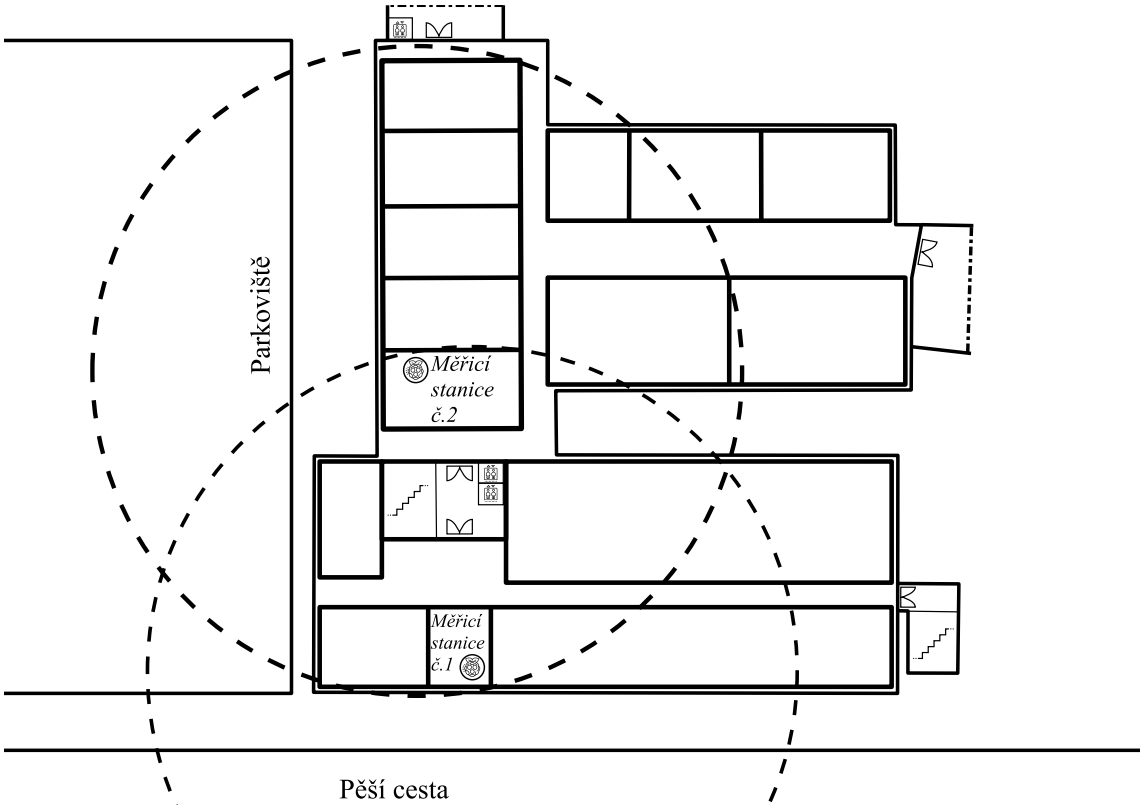
Obr. 6.12: Graf počtu průchodů Bluetooth zařízení měřícími stanovišti(rozlišeno podle stanice)

Stejně jako v případě průchodů WiFi zařízení i zde se nacházejí špatně klasifikované průchody, ze stejných důvodů.

6.2 Měření č.2

Druhé měření se konalo v části 2. patra budovy VUT FEKT T12. Měření probíhalo od pátku 10. 5. 2024 14:52 do středy 15. 5. 2024 15:01.

6.2.1 Rozmístění měřících stanovišť v 2D prostoru



Obr. 6.13: Plánek rozmístění měřících stanovišť v prostoru pro měření č.2

6.2.2 Statistiky a grafy

Počet detekovaných zařízení

Typ zařízení	Počet
BTLE	35484
BR/EDR	140
WiFi Client	43512
WiFi AP	1425
WiFi Ad-Hoc	67
WiFi Bridged	1625

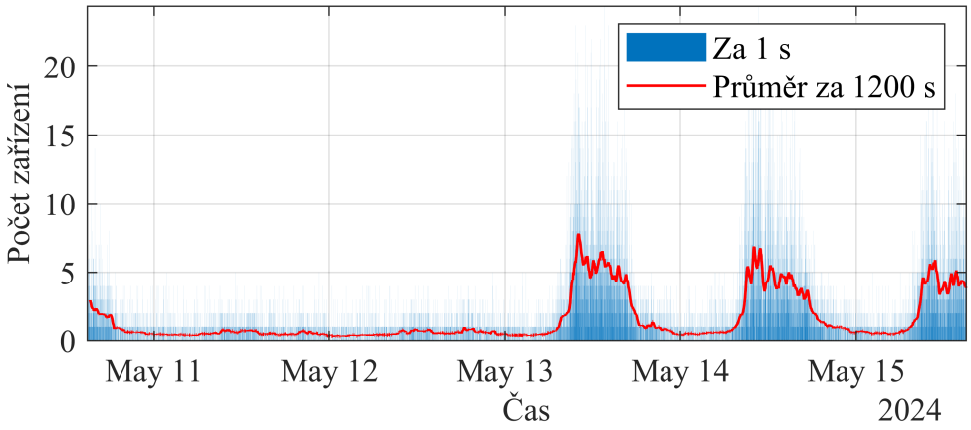
Tab. 6.3: Počet detekovaných zařízení před filtrací dat

Typ zařízení	Počet
BTLE	24757
BR/EDR	109
WiFi Client	43446
WiFi AP	1425
WiFi Ad-Hoc	67
WiFi Bridged	1625

Tab. 6.4: Počet detekovaných zařízení po filtraci dat

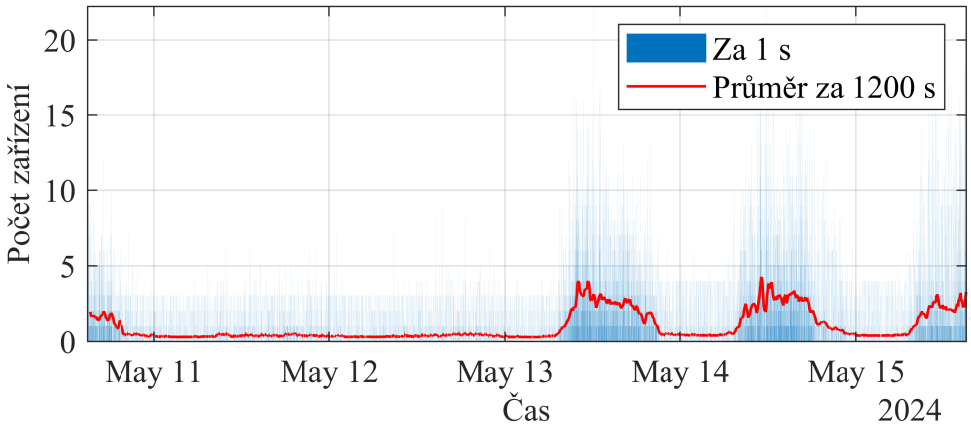
Podobně jako v 1. měření i zde bylo nalezeno velké množství Bluetooth zařízení, kdy i po vyfiltrování dat, kde bylo odstraněno přes 10 000 Bluetooth zařízení, stále značné množství zůstává a je pravděpodobné, že se i zde nacházejí duplikované záznamy zařízení.

Počet aktivních zařízení



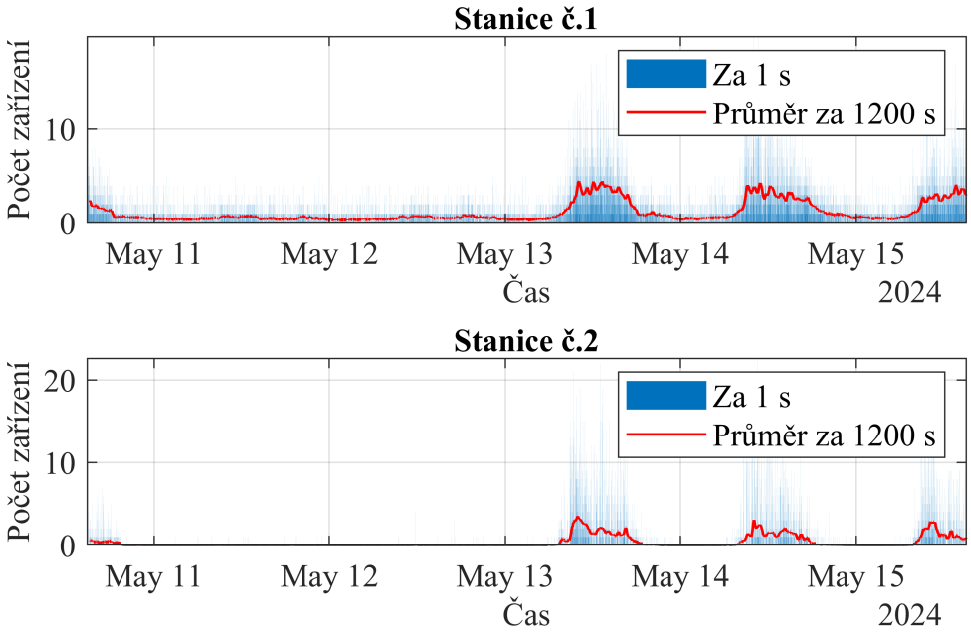
Obr. 6.14: Graf počtu aktivních WiFi zařízení v průběhu měření

Z grafu v obrázku 6.14 podle předpokladu vidíme, že v pracovních dnech, během běžných pracovních hodin, je počet aktivních zařízení několika násobně zvýšen oproti víkendu či noci. Můžeme si všimnout, že se jedná v podstatě o inverzi grafu v obrázku 6.5 z prvního měření.

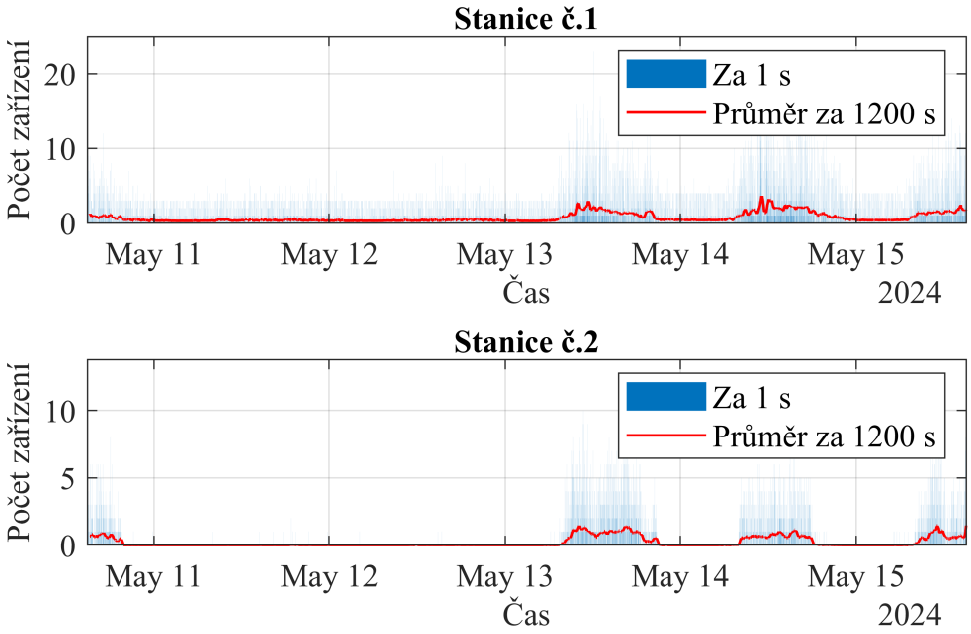


Obr. 6.15: Graf počtu aktivních Bluetooth zařízení v průběhu měření

Stejný trend vidíme i zde, v případě Bluetooth zařízení.



Obr. 6.16: Grafy počtu aktivních WiFi zařízení v průběhu měření (rozlišeno podle stanice)

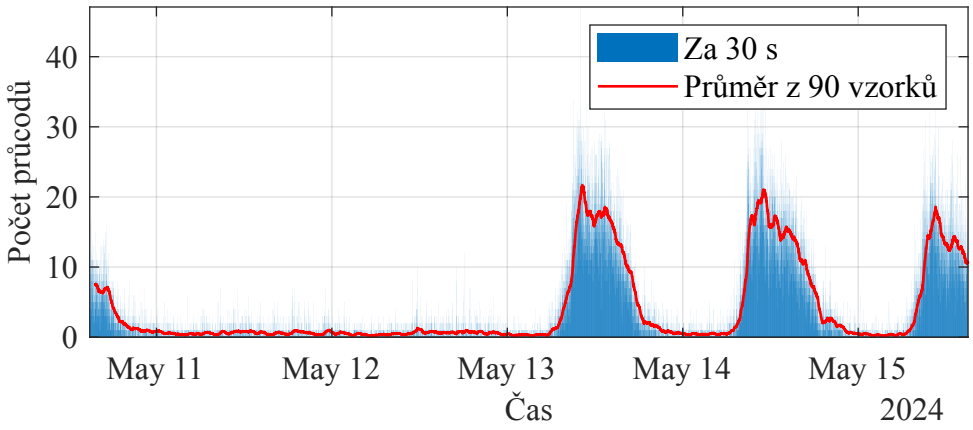


Obr. 6.17: Grafy počtu aktivních Bluetooth zařízení v průběhu měření (rozlišeno podle stanice)

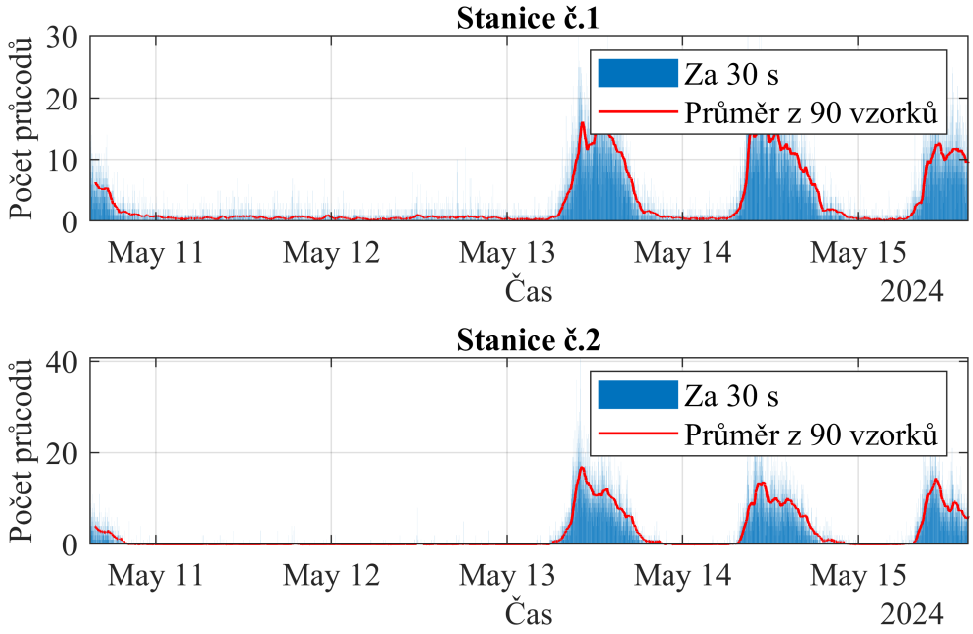
Na rozdíl od prvního měření, je zde rozdíl aktivity v okolí jednotlivých stanic

menší (viz Obr. 6.16 a 6.17). Z části to může být zapříčiněno menší vzdáleností mezi měřícími stanicemi, oproti prvnímu měření, ale také poměrem pohybu osob okolo jednotlivých stanic, který bude vyrovnanější než v případě prvního měření.

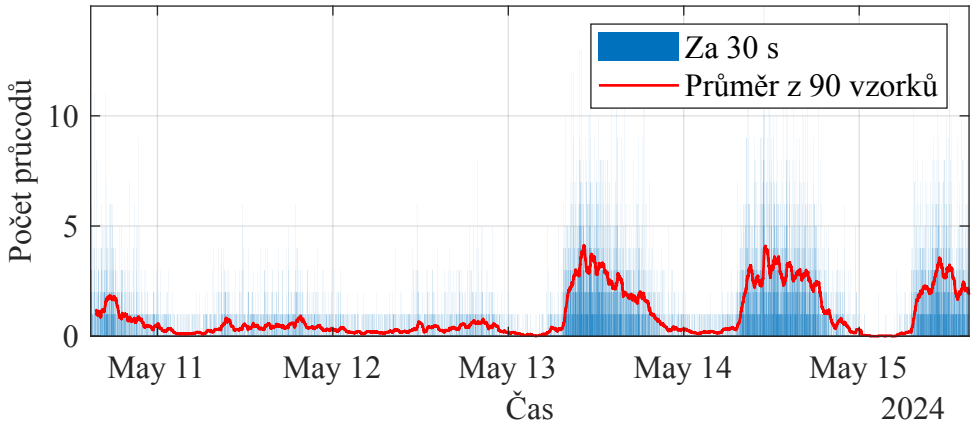
Počet průchodů stanovišti



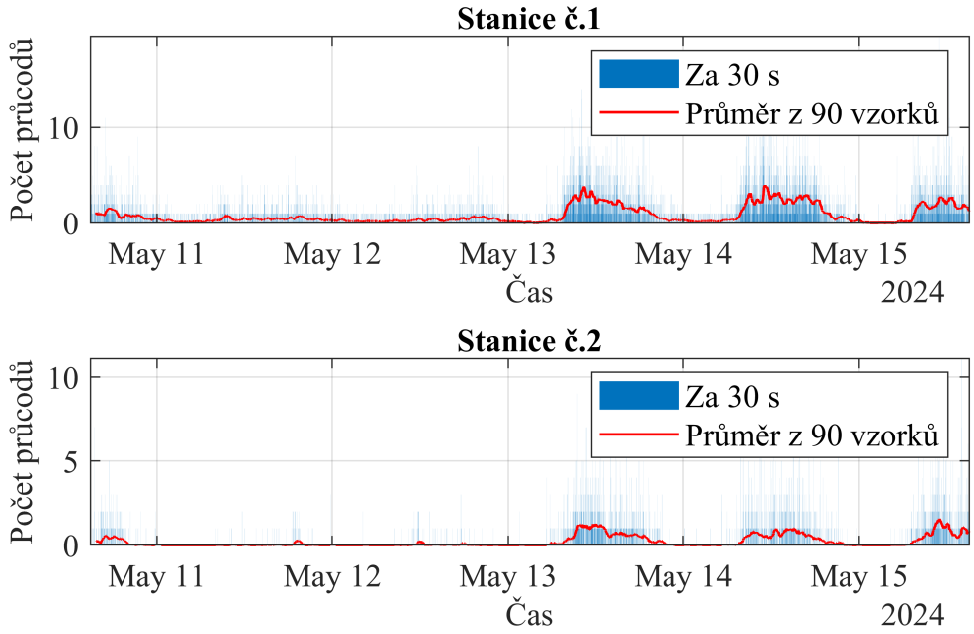
Obr. 6.18: Graf počtu průchodů WiFi zařizení měřícími stanovišti



Obr. 6.19: Graf počtu průchodů WiFi zařizení měřícími stanovišti (rozlišeno podle stanice)



Obr. 6.20: Graf počtu průchodů Bluetooth zařízení měřícími stanovišti



Obr. 6.21: Graf počtu průchodů Bluetooth zařízení měřícími stanovišti (rozlišeno podle stanice)

Z grafů počtu průchodů pozorujeme, zvýšený počet průchodů v časových úsecích, které se shodují časovými úseky se zvýšenou aktivitou zařízení v grafech z obrázků 6.14 a 6.15. Ve špičkách mohlo projít až 40 zařízení za 30 sekund, pravděpodobně to bude méně z důvodů popsaných v sekci 6.1.2.

6.3 Měření č.3

Třetí měření probíhalo v autobuse na trase Brno, Královo Pole až Vysoké Mýto.

6.3.1 Statistky a grafy

Počet detekovaných zařízení

Typ zařízení	Počet
BTLE	1114
BR/EDR	44
WiFi Client	24
WiFi AP	11
WiFi Ad-Hoc	5
WiFi Bridged	5

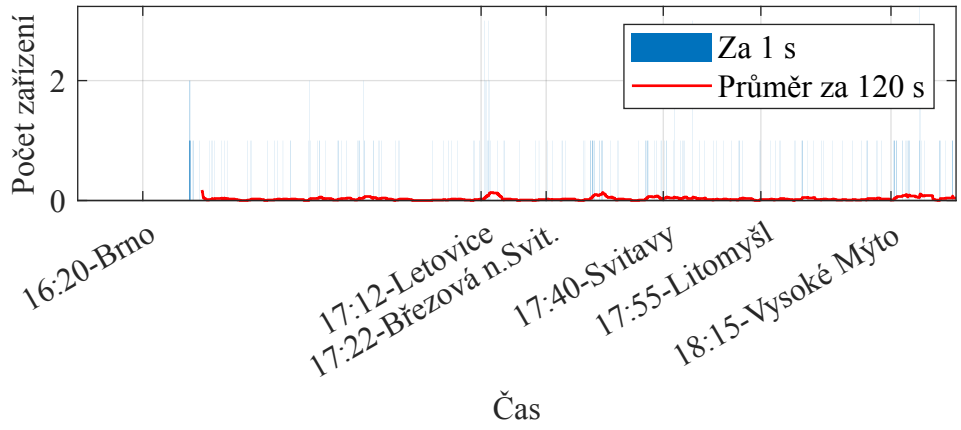
Tab. 6.5: Počet detekovaných zařízení před filtrací dat

Typ zařízení	Počet
BTLE	466
BR/EDR	7
WiFi Client	12
WiFi AP	11
WiFi Ad-Hoc	4
WiFi Bridged	5

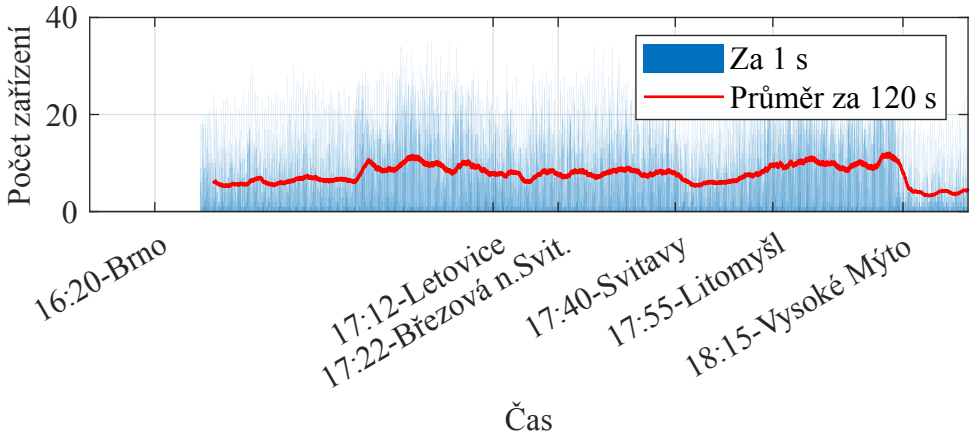
Tab. 6.6: Počet detekovaných zařízení po filtraci dat

Z tabulky 6.6 vidíme, že i přes absenci bezdrátové sítě v autobuse, byly detekovány přístupové bod (WiFi AP). Přístupové body byly detekovány na autobusových zastávkách ale je možné, že některé byly mohly být detekovány když detekovaná zařízení prováděli skenování ve snaze najít svoje známé sítě (viz sekce 1.5).

Počet aktivních zařízení



Obr. 6.22: Graf počtu aktivních WiFi zařízení v průběhu měření



Obr. 6.23: Graf počtu aktivních Bluetooth zařízení v průběhu měření

Data grafech začínají s cca 10 minutovým zpožděním, jelikož jsem měření zapnul až po nástupu do autobusu.

Vzhledem k absenci bezdrátové sítě v autobusu, ve kterém bylo prováděno měření, tak dat z WiFi karet bylo velmi málo a jsou nicneříkající. Pro změnu byly data zachycené pomocí Bluetooth užitečnější, a dávají nám alespoň představu o počtu osob v autobusu. Bohužel nemám přesný počet osob který byl přepravován, ale dovolil bych si odhadnout, z mého pozorování přímo v autobuse, že počet osob by mohl odpovídat průměru v obrázku 6.23 s odchylkou ±30%

Závěr

Během práce jsem zjistil, že detekce Bluetooth a WiFi zařízení není náročná. S dostatečnými znalostmi o základních principech fungování těchto technologií a jejich detekce, lze s vhodným výběrem hardwaru a softwaru efektivně detekovat zařízení využívající tyto komunikační technologie.

Je však důležité poznamenat, že metoda zachytávání bezdrátové komunikace není absolutně spolehlivá. Nejsou-li zařízení aktivně zapojena v bezdrátové komunikaci, není tato metoda schopna jejich detekce, i když mají aktivní technologie Bluetooth nebo WiFi. Při sledování WiFi komunikace jsem odhalil i zařízení připojená k síti ethernetovým kabelem (WiFi Bridged, viz např. Tab. 6.2), tomuto vděčíme protokolu ARP (viz sekce 1.3).

V průběhu práce jsem využil serveru a dvou jednodeskových počítačů Raspberry Pi 3 model B+ (viz kapitola 4), kde byl nainstalován software Kismet pro detekci zařízení. I přesto, že Kismet je kvalitní software, limituje ho schopnost detekce Bluetooth zařízení pouze prostřednictvím odesílání inquiry požadavků (viz sekce 3.2).

Díky tomu, že jsem pro detekci použil dva WiFi adaptéry na každé Raspberry Pi, tak jsem mohl sledovat dvě frekvence současně. Stále se však může stát, že nějaké zařízení nebude detekováno. Toto by mohlo být vyřešeno použitím více adaptérů (nebo adaptér s více anténami), pak bychom mohli ale narazit na hardwarové omezení použitého Raspberry Pi, zejména výpočetní výkon.

Během prvního měření (viz sekce 6.1) došlo ke ztrátě spojení mezi serverem a měřící stanicí č.2, proto se v grafech, kde jsou data rozlišena podle stanic, nachází občasné mezery mezi daty.

Jelikož schopnost zachytit rámce dané komunikace na jistou vzdálenost závisí na mnoha okolnostech, a několik jich je i proměnných v čase (například rušení od okolních zařízení, počasí v případě venkovních prostor) tak je možné, že vzdálenější stanice občas zachytí komunikaci a pak se muže jevit, že se zařízení pohybuje, i když tomu tak není. Příklad této události můžeme pozorovat v obrázku 6.3, kdy to vypadá že zařízení, kolem 3. hodiny ranní, cestovalo mezi stanicemi. Toto je však nepravděpodobné a spíše se jedná o chybu, kdy okolní rušení mohlo být v tyto momenty velmi nízké a stanice č.2 tak dokázala zachytit komunikaci tohoto zařízení. Řešením takovýchto „anomálií“ by bylo zvětšením vzdálenosti mezi stanicemi, nebo umělým snížením dosahu antén. Pak bychom ale mohli přijít o důležitou komunikaci během zvýšeného rušení od okolních zařízení.

Z obrázku 6.2 vidíme, že při odjezdu sledované osoby do zaměstnání (kolem 6. hodiny ranní) nebylo zařízení, které osoba nosí, zachyceno těsně před odjezdem stanicí č.2, i když už víme že by to tak mělo být. Toto je s velkou pravděpodobností případ, kdy nebyla zachycena komunikace z důvodu přeskakování mezi kanály.

To znamená že zařízení, se nezdrželo v okolí měřící stanice č.2 dost dlouho na to, aby se právě sledovaný kanál stanice shodoval s kanálem, který využívalo sledované zařízení a také v tu dobu i toto zařízení aktivně komunikovalo. Řešením by bylo, jak jsem popsal výše, použitím více adaptérů (antén).

Ve třetím měření (viz sekce 6.3), by se dalo pro účel počítání osob v přepravě použít i jiná, pravděpodobně přesnější, metoda zahrnující bezdrátové sítě. Vytvořením otevřené (nezabezpečené) bezdrátového sítě, by se, za předpokladu, že se všichni účastníci hromadné dopravy připojovali, docílilo získání přesného počtu zařízení (tedy i cestujících, pokud by každý připojil pouze jedno zařízení k síti). Bohužel jsem tuto metodu, z časových důvodů, nevyzkoušel.

Odhad počtu osob je, z naměřených dat nacházejících se v kapitole 6, obtížné určit. Osoba totiž může nosit více jak jedno Bluetooth či WiFi zařízení, dále je zde otázka, zda je možné tyto zařízení detekovat (viz výše) a také nám to ztěžují nehybné zařízení, které zůstávají v měřeném prostoru. V tomto případě bych považoval vyobrazené průměry v grafech, které zahrnují WiFi zařízení, v kapitole 6 za nejpřesnější aproximaci počtu osob v okolí stanice či počtu průchodů osob kolem stanic.

Webové rozhraní Kismetu umožňuje vizualizaci získaných dat a dále byla tato data systematicky ukládána do databází pro následné zpracování v MATLABu.

Pokud bych měl vybrat pouze jednu technologii, která je výhodnější pro sledování a detekci zařízení, byla by to technologie WiFi. Z vlastních zkušeností, které mi potvrdily i statistiky sledování v tabulkách 6.2 a 6.4, je jasné, že více zařízení využívá tuto technologii, je jednodušší zachytávat přenášená data a nabízí nám více příležitostí je detekovat.

Tento analyzátor by v praxi mohl být nasazen na místa, kde není potřeba velké přesnosti, například do obchodních center, kde jsou již bezdrátové sítě běžně dostupné a tak by z naměřených dat mohli získat například kdy a kde se koncentruje největší množství zákazníků atp., nebo by mohl být využit pro sledování drahého přenosného vybavení pokud by disponovalo WiFi modulem, který pouze periodicky odesílá rámce podobné WiFi Beacon rámcům (viz sekce 1.5) a tyto rámce by byly monitorovány. V případě, že takto sledované vybavení odešlo z měřeného prostoru (např. z budovy firmy) monitorovací stanice by přestaly dostávat tyto rámce a v důsledku by například mohl být odeslán varovný e-mail vybraným osobám.

Literatura

[1] BEAL, Vangie. *Wi-Fi*. Online. Webopedia. 2001, Updated on: January 4, 2022. Dostupné z: https://www.webopedia.com/definitions/wifi/. [cit. 2023-10-08].

[2] *What Is Wi-Fi?* Online. Cisco. ©2023. Dostupné z: https://www.cisco.com/c/en/us/products/wireless/what-is-wifi.html. [cit. 2023-10-08].

[3] *The Evolution of Wi-Fi Technology and Standards*. Online. In: IEEE SA - The IEEE Standards Association. ©2023. Dostupné z: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/. [cit. 2023-10-08].

[4] *What are the WiFi IEEE 802.11 Standards?* Online. In: Signal Boosters. ©2023. Dostupné z: https://www.signalboosters.com/blog/what-are-the-wifi-ieee-80211-standards/. [cit. 2023-10-08].

[5] *IEEE 802.11*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 27 September 2023. Dostupné z: https://en.wikipedia.org/wiki/IEEE_802.11. [cit. 2023-10-08].

[6] HIERTZ, Guido; DENTENEER, Dee; STIBOR, Lothar; ZANG, Yunpeng; COSTA, Xavier et al. The IEEE 802.11 universe. Online. *IEEE Communications Magazine*. 2010, roč. 48, č. 1, s. 62-70. ISSN 0163-6804. Dostupné z: https://doi.org/10.1109/MCOM.2010.5394032. [cit. 2023-11-13].

[7] *MIMO, Multiuser MIMO and Massive MIMO*. Online. In: Verkotan. ©2023. Dostupné z: https://verkotan.com/2023/mimo-mu-mimo-and-massive-mimo-mimo-testing-at-verkotan/. [cit. 2023-10-09].

[8] YASAR, Kinza. *MAC address (media access control address)*. Online. In: TechTarget. 2023, December 2022. Dostupné z: https://www.techtarget.com/searchnetworking/definition/MAC-address. [cit. 2023-10-10].

[9] TAN, Jiajie a GARY CHAN, S.-H. Efficient Association of Wi-Fi Probe Requests under MAC Address Randomization. Online. *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications*. 2021, s. 1-10. ISBN 978-1-6654-0325-2. Dostupné z: https://doi.org/10.1109/INFOCOM42981.2021.9488769. [cit. 2023-11-28].

[10] *MAC Randomization Behavior*. Online. In: GOOGLE. Android Open Source Project. 2024. Dostupné z: https://source.android.com/docs/core/connect/wifi-mac-randomization-behavior. [cit. 2024-05-14].

[11] *Address Resolution Protocol*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 31 October 2023. Dostupné z: https://en.wikipedia.org/wiki/Address_Resolution_Protocol. [cit. 2023-12-22].

[12] *ISM radio band*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 23 August 2023. Dostupné z: https://en.wikipedia.org/wiki/ISM_radio_band. [cit. 2023-10-10].

[13] *What are the ISM Bands, and What Are They Used For?* Online. In: Military Aerospace. ©2023. Dostupné z: https://www.militaryaerospace.com/directory/blog/14059677/what-are-the-ism-bands-and-what-are-they-used-for. [cit. 2023-10-10].

[14] *Direct-sequence spread spectrum*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 30 July 2023. Dostupné z: https://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum. [cit. 2023-11-14].

[15] LATIF, Shahid; KAMRAN, Muhammad; MASOUD, Fahad a SOHAIB, Muhammad. Improving DSSS transmission security using Barker code along binary compliments (CBC12-DSSS). Online. *2012 International Conference on Emerging Technologies*. 2012, s. 1-5. ISBN 978-1-4673-4451-7. Dostupné z: https://doi.org/10.1109/ICET.2012.6375426. [cit. 2023-11-14].

[16] *Frequency-hopping spread spectrum*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 6 August 2023. Dostupné z: https://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum. [cit. 2023-11-14].

[17] LIU, Yang. Frequency hopping spread spectrum: An effective way to improve wireless communication performance. *Advanced Trends in Wireless Communications*, 2011, 187.

[18] *Frequency-division multiplexing*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 8 May 2023. Dostupné z: https://en.wikipedia.org/wiki/Frequency-division_multiplexing. [cit. 2023-11-27].

[19] *Orthogonal frequency-division multiplexing*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 8 November 2023. Dostupné z: https://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing. [cit. 2023-11-27].

[20] *Orthogonal frequency-division multiple access*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-, 27 November 2023. Dostupné z: https://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiple_access. [cit. 2023-11-27].

[21] *MIMO*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 26 November 2023. Dostupné z: https://en.wikipedia.org/wiki/MIMO. [cit. 2023-11-27].

[22] *Multi-user MIMO*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 26 November 2023. Dostupné z: https://en.wikipedia.org/wiki/Multi-user_MIMO. [cit. 2023-11-27].

[23] *Quadrature amplitude modulation*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 21 November 2023. Dostupné z: https://en.wikipedia.org/wiki/Quadrature_amplitude_modulation#. [cit. 2023-11-27].

[24] PEI, Changhua; WANG, Zhi; ZHAO, Youjian; WANG, Zihan; MENG, Yuan et al. Why it takes so long to connect to a WiFi access point. *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*. 2017, s. 1-9. ISBN 978-1-5090-5336-0. Dostupné z: https://doi.org/10.1109/INFOCOM.2017.8057164.

[25] LOCHMAN, Matěj. Detekce a sběr dat z mobilních zařízení v budovách. Diplomová práce. Plzeň: Západočeská univerzita v Plzni.

[26] *Bluetooth® Wireless Technology*. Online. Bluetooth. ©2023. Dostupné z: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/. [cit. 2023-10-10].

[27] INTEL. *What Is Bluetooth® Technology?* Online. INTEL. Intel. Dostupné z: https://www.intel.com/content/www/us/en/products/docs/wireless/what-is-bluetooth.html. [cit. 2023-10-10].

[28] *Bluetooth*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 10 October 2023. Dostupné z: https://en.wikipedia.org/wiki/Bluetooth. [cit. 2023-10-10].

[29] G., Andy. *Different Bluetooth Versions: What You Need to Know*. Online. In: Headphonesty. ©2016-2023, May 2, 2023. Dostupné z: https://www.headphonesty.com/2021/01/bluetooth-versions/. [cit. 2023-10-10].

[30] *How Bluetooth 1.0, 2.0, 3.0, 4.0, and 5.0 Compare*. Online. In: Dusun IoT: Embedded Hardware Vendor | IoT Gateway Sepcialist. ©2023, May 5, 2023. Dostupné z: https://www.dusuniot.com/blog/how-bluetooth-1-0-2-0-3-0-4-0-and-5-0-compare/. [cit. 2023-10-10].

[31] *Bluetooth 5.3 – Features and applications*. Online. In: RF Page - RF & Wireless technology, Tools and Instruments. ©2023, September 20, 2023. Dostupné z: https://www.rfpage.com/bluetooth-5-3-features-and-applications/. [cit. 2023-10-14].

[32] CROSS, Daniel; HOECKLE, Justin; LAVINE, Michael; RUBIN, Jason; SNOW, Kevin et al., GOETZ, Eric a SHENOI, Sujeet (ed.). Detecting Non-Discoverable Bluetooth Devices. Online. In: *Critical Infrastructure Protection. ICCIP 2007. IFIP International Federation for Information Processing*. Vol 253. Springer, Boston, MA, 2008, s. 281-293. Dostupné z: https://link.springer.com/chapter/10.1007/978-0-387-75462-8_20#citeas. [cit. 2023-11-28].

[33] *Internet of things*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 13 October 2023. Dostupné z: https://en.wikipedia.org/wiki/Internet_of_things. [cit. 2023-10-15].

[34] *What is the Internet of Things?* Online. In: Global management consulting | McKinsey. © 1996-2023. Dostupné z: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-the-internet-of-things. [cit. 2023-10-15].

[35] *Raspberry Pi*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 14 October 2023. Dostupné z: https://en.wikipedia.org/wiki/Raspberry_Pi. [cit. 2023-10-16].

[36] *What is a Raspberry Pi?* Online. Opensource.com. ©2023. Dostupné z: https://opensource.com/resources/raspberry-pi. [cit. 2023-10-16].

[37] *Raspberry Pi 3 Model B+*. Online. Raspberry Pi. Dostupné z: https://www.raspberrypi.com/products/raspberry-pi-3-model-b-plus/. [cit. 2023-10-16].

[38] *Raspberry Pi 5*. Online. Raspberry Pi. Dostupné z: https://www.raspberrypi.com/products/raspberry-pi-5/. [cit. 2023-12-18].

[39] *Raspberry Pi OS*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 16 October 2023. Dostupné z: https://en.wikipedia.org/wiki/Raspberry_Pi_OS. [cit. 2023-11-01].

[40] *Kismet (software)*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2023, 24 July 2023. Dostupné z: https://en.wikipedia.org/wiki/Kismet_(software). [cit. 2023-10-31].

[41] *Kismet*. Online. Kismet - Wi-Fi, Bluetooth, RF, and more. Dostupné z: https://www.kismetwireless.net/docs/readme/intro/kismet/. [cit. 2023-10-31].

[42] *Difference - Promiscuous vs. Monitor Mode (Wireless Context)*. Online. High on wires: Interesting concepts in the world of Computer Netowrking. 2008, OCTOBER 13, 2008. Dostupné z: http://lazysolutions.blogspot.com/2008/10/difference-promiscuous-vs-monitor-mode.html. [cit. 2023-10-31].

Seznam symbolů a zkratek

MAC	Media Access Control
IoT	Internef of Things, Internet věcí
ARM	Označení architektury procesoru
FHSS	Frequency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
CKK	Complementary Code Keying
ODFM	Orthogonal Frequency Division Multiplexing
ODFMA	Orthogonal frequency-division multiple access
MIMO	Multiple-input and multiple-output, více vstupů a více výstupů
SU	Single-User, jeden uživatel
MU	Multi-User, více uživatelů
QAM	Quadrature amplitude modulation
IR	Infrared
MHz	Megaherz
GHz	Gigahertz
THz	Terahertz
Mbit/s	[Megabit za sekundu]
BSSID	Basic Service Set Identifier
SSID	Service Set Identifier
DHCP	Dynamic Host Configuration Protocol
AP	Access Point, přístupový bod
OSI	Open Systems Interconnection
WPA	WiFi Protected Access, chráněný přístup k WiFi
NFC	Near-Field Communication, Blízkopolní komunikace

AFH	Adaptive Frequency Hopping
eSCO	Extended Synchronous Connections
EDR	Enhanced Data Rate
EIR	Extended Inquiry Response
SSP	Secure Simple Pairing
HS	High Speed
AMP	Alternative MAC/PHY
BLE	Bluetooth Low Energy
AES	Advanced Encryption Standard
AoA	Angle of Arrival
AoD	Angle of Departure
ISOC	Isochronous Channels, izochronní kanály
EATT	Enhanced Attribute Protocol
SoC	System on Chip
GPIO	General-Purpose Input/Output, Univerzální vstupní/výstupní pin
RAM	Random-Access Memory, pamět s náhondým přístupem
USB	Universal Serial Bus
WSL	Windows Subsystem for Linux, windowsový podsystém pro Linux
SSH	Secure Shell
SQL	Structured Query Language, standardizovaný strukturovaný dotazovací jazyk
FEKT	Fakulta elektrotechniky a komunikačních technologií