Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Zachytávání Bluetooth signálu v testovacím centru PEF ČZU

Petr Dušek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Petr Dušek

Informatika

Název práce

Zachytávání bluetooth signálu v testovacím centru PEF ČZU

Název anglicky

Capturing bluetooth signal in the test center

Cíle práce

Cílem této práce je nalézt finančně a technologicky optimální řešení pro implementaci zařízení, které zachytává Bluetooth signály vysílané mobilními telefony a další nositelnou elektronikou v testovacím centru Provozně ekonomické fakulty.

Metodika

Teoretická část této práce se bude zabývat popisem a charakteristikou Bluetooth signálu, jeho možnostmi využití a definováním jeho výhod a nevýhod.

V praktické části bude popsáno provedené měření Bluetooth signálu pomocí zařízení určeného k zachytávání Bluetooth signálu v prostoru testovacího centra PEF. Součástí této části bude také popis případných kolizí s ostatními signály v daném prostoru.

Na základě výsledků praktického měření budou stanoveny požadavky na množství zařízení, jejich umístění a ekonomický aspekt provozu takového zachytávání.

Výstupem práce bude zhodnocení efektivity tohoto měření a případný návrh implementace zařízení do testovacího centra PEF.

Metodou literární rešerše vznikne potřebný základ na pochopení funkčnosti a využití Bluetooth bezdrátové technologie. Za pomoci metody komparace vznikne rozhodnutí použití zařízení k dosažení cíle. Syntézou pak proběhne zvážení rizik, výhod a nevýhod spojených s měřením a záchytem paketů a na základě toho pak stanovení závěru práce a jejího výstupu.

Doporučený rozsah práce

30 – 40 stran

Klíčová slova

Bluetooth, signál, mobilní telefon, přijímač, vysílač, Bluetooth LE, IoT, Bluetooth zařízení, internet, sniffer, nositelná elektronika, pakety

---

Doporučené zdroje informací

C. Bisdikian, ”An overview of the Bluetooth wireless technology,” in IEEE Communications Magazine, vol. 39, no. 12, pp. 86-94, Dec. 2001, doi: 10.1109/35.968817.

HEYDON, Robin. Bluetooth low energy: the developer’s handbook: the developer’s handbook. Upper Saddle River: Prentice Hall, 2013. Dostupné také z: https://go.exlibris.link/ZspBdzLz

h Square PublishiHURT, Avery Elizabeth. How Bluetooth Works. New York, NY: Cavendisng, 2018. Dostupné také z: https://go.exlibris.link/W5y9FZCs

K. -H. Chang, ”Bluetooth: a viable solution for IoT? [Industry Perspectives],” in IEEE Wireless Communications, vol. 21, no. 6, pp. 6-7, December 2014, doi: 10.1109/MWC.2014.7000963.

Leith, D.J., & Farrell, S. (2020). Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection. ArXiv, abs/2006.06822.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Václav Lohr, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 2. 2024

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 13. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zachytávání Bluetooth signálu v testovacím centru PEF ČZU" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 13.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Václavu Lohrovi, Ph.D. za klíčové návrhy postupu testování technologie a nadhledy do zpracování práce. Dále bych rád poděkoval svým rodičům za jejich neutuchající podporu při studiu a zpracování této práce.

Zachytávání Bluetooth signálu v testovacím centru PEF ČZU

Abstrakt

Tato bakalářská práce je zaměřena na zkoumání možnosti použití bezdrátové technologie Bluetooth LE k zachytávání paketů jako rozšíření technické vybavenosti testovacího centra PEF.

V práci byla prozkoumána funkčnost technologie Bluetooth, zahrnující její výhody a nevýhody, praktické využití a její chování v rámci frekvenčního pásma. Součástí této práce byl rovněž popis chování dalších technologií, které operují ve stejném frekvenčním pásmu. Klíčovým prvkem této práce byl také popis modelu oznamování zařízení, který umožňuje identifikaci přítomnosti zařízení v okolí a zajištění bezpečného bezdrátového přenosu dat.

Za pomoci teoretických předpokladů bylo nakonec provedeno testovací měření za účelem získání a interpretování výsledků, jehož součástí bylo počáteční nastavení zařízení k záchytu paketů, popis a zhodnocení efektivnosti zachytávání paketů v testovacím centru PEF.

Závěrem byly výsledky testovacího měření zhodnoceny a bylo stanoveno doporučení dalšího postupu pro implementaci této technologie.

Klíčová slova: Bluetooth, signál, mobilní telefon, přijímač, vysílač, Bluetooth LE, IoT, Bluetooth zařízení, internet, sniffer, nositelná elektronika, pakety

Capturing Bluetooth signal in the test center

Abstract

This bachelor's thesis is focused on investigating the possibility of using Bluetooth LE wireless technology to capture packets as an extension of the technical equipment of the PEF test center.

The functionality of Bluetooth technology was investigated, including its advantages and disadvantages, practical use, and its behavior within the frequency band. Part of this work was also a description of the behavior of other technologies that operate in the same frequency band. A key element of this work was also the description of the device advertising model, which enables the identification of the presence of devices in the vicinity and the provision of secure wireless data transmission.

Based on the theoretical assumptions, a test measurement was carried out in order to obtain and interpret the results, which included the initial setting of the packet capture device, description and evaluation of the effectiveness of packet capture in the PEF test center.

In conclusion, the results of the test measurement were evaluated and a recommendation for the next procedure for the implementation of this technology was established.

Keywords: Bluetooth, signal, mobile phone, receiver, transmitter, Bluetooth LE, IoT, Bluetooth device, internet, sniffer, wearable electronics, packets

Obsah

1 Úvod

Na základě rozvoje a komplexnosti technologií jsme se rozhodli prozkoumat možnosti rozšíření technologického vybavení testovacího centra Provozně ekonomické fakulty. V rámci této práce byla konkrétně prozkoumána možnost využití technologie Bluetooth LE jako rozšíření technologické vybavenosti opatření v testovacím centru. Využití právě této technologie bylo zvoleno na základě jednoduchého pozorování využití v praxi, rozsáhlé dokumentace nejenom od tvůrců technologie, představení nových funkcí technologie na veletrhu spotřebitelské elektroniky a dalších článků zaměřujících se na rozvíjející se technologii.

V dnešní době, kdy je bezdrátová komunikace nezbytnou součástí našeho každodenního života, je důležité pochopit a zkoumat různé aspekty těchto technologií. Bluetooth, jako jedna z nejrozšířenějších bezdrátových technologií, hraje klíčovou roli v mnoha aplikacích od přenosu dat mezi zařízeními po sledování polohy.

V rámci této práce byly zkoumané aspekty zachytávání Bluetooth signálů, včetně hardwarových a softwarových požadavků a zachytávání signálů. Kromě toho bylo hlavním zaměřením se na praktické testování těchto metod v reálném prostředí testovacího centra.

Cílem této práce je nejen poskytnout teoretický přehled o fungování Bluetooth signálů a jejich zachytávání, ale také představit praktické výsledky a zkušenosti získané během testování v testovacím centru.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této práce je nalézt finančně a technologicky optimální řešení pro implementaci zařízení, které zachytává Bluetooth signály vysílané mobilními telefony a další nositelnou elektronikou v testovacím centru Provozně ekonomické fakulty.

2.2 Metodika

Teoretická část této práce se bude zabývat popisem a charakteristikou Bluetooth signálu, jeho možnostmi využití a definováním jeho výhod a nevýhod.

V praktické části bude popsáno provedené měření Bluetooth signálu pomocí zařízení určeného k jeho zachytávání v prostoru testovacího centra PEF. Součástí této části bude také popis případných kolizí s ostatními signály v daném prostoru. Na základě výsledků praktického měření budou stanoveny požadavky na množství zařízení, jejich umístění a ekonomický aspekt provozu takového zachytávání.

Výstupem práce bude zhodnocení efektivity tohoto měření a případný návrh implementace zařízení do testovacího centra.

Pro správu citací byl použit citační manažer Zotero.

Pro získání výsledků měření byl použit nRF52840 sniffer dongle společně s open-source aplikací Wireshark verze 4.2.2.

Skripty pro zpracování dat ze zachytávání a jejich interpretace byly autorem práce vytvořeny v programu Microsoft Visual Studio Code verze 1.86.2 s doinstalovaným rozšířením pro Python a knihovnou pyshark. Samotné grafy byly pak ručně vytvořeny na základě dat dosažených skripty v Microsoft Excel.

Fotografie pořízené uvnitř testovacího centra byly pořízené při uzavřeném provozu testovacího centra, aby na nich nebyla zachycena žádná konkrétní osoba a vše bylo anonymní.

3 Teoretická východiska

3.1 Bluetooth

Podle Bisdikiana (2001) je bezdrátová technologie Bluetooth specifikace pro krátký dosah, nízkou cenu a malý tvar, která umožňuje uživatelsky přívětivé připojení mezi přenosnými a kapesními osobními zařízeními a poskytuje připojení těchto zařízení k internetu.

Vytvořen byl firmou Ericsson v roce 1994 jako bezdrátová náhrada za sériové drátové rozhraní RS-232 nebo USB. Od roku 1998 řídí Bluetooth SIG (Special Interest Group) vývoj technologie prostřednictvím vývoje otevřené průmyslové specifikace zahrnující jak protokoly, tak scénáře aplikací a kvalifikačního programu navrženého tak, aby zajistil uživatelskou hodnotu pro Bluetooth produkty (Bisdikian, 2001).

Bisdikian (2001) dále uvádí, že Bluetooth nezahrnuje pouze komunikační protokoly, ale také aplikace. To odlišuje bezdrátovou technologii Bluetooth od mnoha dalších komunikačních technologií, které se zaměřují především na fyzické, datové a případně síťové aspekty komunikace. Protože bezdrátovou technologii Bluetooth mají používat především spotřebitelé, musí tato technologie od svých uživatelů vyžadovat minimální technické znalosti.

Technologie je normalizována standardem IEEE[1] 802.15.1 a spadá do kategorie osobních počítačových sítí tzv. PAN (z anglického Personal Area Network).

Podle Bluetooth® (c2023) stojí za zmínku, že název, ačkoliv po vyslovení nebudí dojem technického rázu, není ničeho zkratkou. Jméno je však uděleno této technologii po králi Haraldu I. nebo také Harald Modrozub Gormsson, který se proslavil dvěma věcmi:

1. Sjednotil Dánsko a Norsko v roce 958 n.l. tím, že přinutil válčící kmeny, aby započali diskusi a ukončili tak vzájemné rozepře
2. Jeho mrtvý zub, který měl tmavě modrou až šedou barvu, mu zajistil přezdívku Modrozub

[1] Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství) a jedná se o mezinárodní neziskovou profesní organizaci, která usiluje o růst technologií souvisejících s elektronikou.

3.1.1 **Bluetooth® Classic**

Bluetooth® (c2023) specifikuje rádio Bluetooth Classic, také označované jako Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR), jako nízkoenergetické rádio, které přenáší data přes 79 kanálů v nelicencovaném frekvenčním pásmu 2,4 GHz. Bluetooth Classic, který podporuje komunikaci zařízení typu point-to-point[2], se používá hlavně k umožnění bezdrátového streamování zvuku a stal se standardním rádiovým protokolem za bezdrátovými reproduktory, sluchátky a zábavními systémy v automobilech. Rádio Bluetooth Classic umožňuje také aplikace pro přenos dat včetně mobilního tisku.

3.1.2 **Bluetooth® Low Energy**

Podle Changa (2014) je rádio Bluetooth Low Energy (LE) navrženo s možností provozu s velmi nízkou spotřebou energie. Bluetooth LE přenáší data přes 40 kanálů v nelicencovaném frekvenčním pásmu ISM 2,4 GHz. 3 z těchto 40 kanálů jsou vymezeny pro účely oznamování a zbylých 37 je pro přenos dat. Tomuto procesu oznamování se také odborně říká „advertising“.

Bluetooth® (c2023) specifikuje, že Bluetooth LE podporuje více komunikačních topologií, od point-to-point přes tzv. broadcast[3] a v poslední době i mesh, což umožňuje technologii Bluetooth podporovat vytváření spolehlivých a rozsáhlých sítí zařízení. Bluetooth LE byl zpočátku známý svými komunikačními schopnostmi zařízení a nyní je také používán jako technologie určování polohy zařízení uvnitř budov. Bluetooth LE nyní obsahuje funkce, které umožňují jednomu zařízení určit přítomnost, vzdálenost či směr jiného zařízení (Leith a Farrell, 2020).

Heydon (2012) uvádí, že technologie Bluetooth LE byla znormalizována v roce 2010 do té doby byla pouze součástí Bluetooth Classic jako funkce. Název Low Energy odkazuje na základní koncept této technologie se sníženou spotřebou baterie zařízení, která byla nutná k udržení stabilních nákladů na výrobu a údržbu zařízení používajících tuto technologii a omezení tzv. opportunity costs (náklady spojené s nedostupností zařízení). Zpočátku bylo

[2] Umožňuje přímé spojení dvou síťových uzlů/bodů mezi sebou na linkové vrstvě, která zajišťuje komunikaci mezi zařízeními.

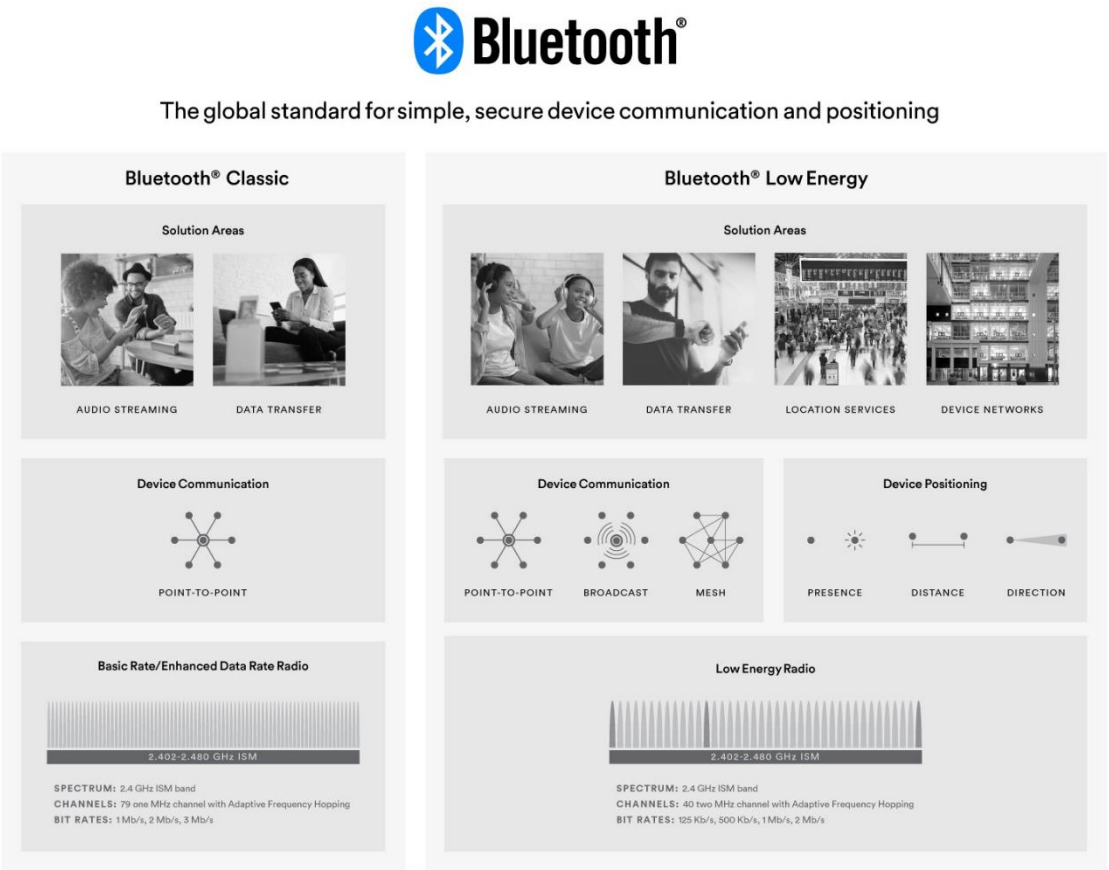
[3] Označení pro masové šíření informací, dat nebo zpráv na více zařízeních současně.

nejefektivnějším způsobem napájet tyto zařízení pomocí klasických AAA baterií ale později se začaly používat knoflíkové baterie (tzv. „button cell“), které oproti klasickým AAA nebo AA bateriím nepotřebují tolik místa z toho důvodu dokáže výrobce ušetřit i na materiálu díky zmenšené velikosti zařízení.

První mobilní telefony používající Bluetooth LE se objevily v letech 2011-12 (např. iPhone 4S) a dnes jsou téměř všechny moderní mobilní telefony touto technologií vybaveny.

Jednou z nevýhod Bluetooth je, že nedokáže odesílat velké soubory. K tomu je nutné použít WiFi (Hurt, 2018).

Obrázek 1 - Grafický přehled rozdílu Bluetooth Classic a Bluetooth LE



Zdroj: (Bluetooth®, c2023)

Zařízení vybavená Bluetooth LE přijímačem mohou prohledávat až tři rádiové kanály a poslouchat přenosy. Když je detekován začátek přenosu, přijímač využívá skutečnost, že úvod je pevný a známý a ladí rádiový přijímač na přicházející signál. V rámci tohoto ladícího procesu je výstupem ukazatel síly přijatého signálu RSSI (Received Signal Strength Intensity).

Bluetooth LE se nezaměřuje na optimalizaci Bluetooth Classic a nefunguje jako jeho náhrada, ale místo toho cílí na nové tržní segmenty, které dříve nepoužívaly existující bezdrátové standardy. Tyto segmenty trhu zahrnují aplikace, které vyžadují, aby zařízení periodicky odesílala několik velmi malé objemy dat, ať už jednou za sekundu či jednou za několik dní. Mezi takové aplikace patří monitorování a řízení úkolů, jako je např. sledování stavu oken v chytrém domě pro účely vytápění, automatické zapínání a vypínání spotřebičů v závislosti na cenových fluktuacích elektřiny nebo přepínání televizních kanálů (Heydon, 2012).

3.2 Typy zařízení BLE

Existují dva hlavní typy Bluetooth Low Energy zařízení:

- single-mode
- dual-mode

Obrázek 2 - Komunikace typů Bluetooth zařízení

	Single-Mode	Dual-Mode	Classic
Single-Mode	LE	LE	none
Dual-Mode	LE	Classic	Classic
Classic	none	Classic	Classic

Zdroj: (Heydon, 2012)

Kromě toho existuje i třetí typ, který ale vůbec nepoužívá Bluetooth Low Energy a spoléhá pouze na Bluetooth Classic (Heydon, 2012). Zařízení podporující dual-mode jsou nejnovější typ a příkladem těchto zařízení jsou chytré mobilní telefony (Symmetry Electronics, 2023).

Heydon (2012) uvádí, že zařízení používající technologii Bluetooth jsou takto klasifikována na základě toho, jaký typ Bluetooth dokážou používat ke komunikaci. Zařízení single-mode dokáže komunikovat pouze skrze Bluetooth LE. Zařízení dual-mode používají oba typy Bluetooth současně a dokážou tak komunikovat se všemi Bluetooth Classic a BLE zařízeními. Třetí typ zařízení, jak už název napovídá, komunikuje pouze se zařízeními, které využívají Bluetooth Classic. Na obrázku 2 je vidět v tabulce přípustná komunikace Bluetooth zařízení a který typ Bluetooth bude použit ke komunikaci, pokud jsou obě technologie, tedy LE i Classic, k dispozici. Pokud jsou obě technologie k dispozici, tedy komunikuje dual-mode zařízení s dual-mode zařízením, preferuje se použití technologie Bluetooth Classic. Pokud je však jedno z komunikujících zařízení single-mode, vyžaduje se použití Bluetooth LE. To neplatí, když je jedno ze zařízení pouze typu Classic.

3.3 **2,4 GHz ISM pásmo**

Pásma ISM (anglicky Industrial, Scientific and Medical) (tzv. bezlicenční pásma) jsou mezinárodně stanovené části rádiového spektra určené pro průmyslové, vědecké a zdravotnické použití (Heydon, 2012). Jedná se o vyhrazené rádiové frekvence, které slouží například k ohřívání v průmyslu nebo pro použití mikrovlnné trouby v domácnostech.

Při používání této rádiové frekvence se do okolí šíří elektromagnetické rušení, které nelze odstranit a ruší rádiovou komunikaci. To je důvod, proč nemůže být toto pásmo pronajímáno státem, v České republice Českým telekomunikačním úřadem, a je deklarováno jako volné pásmo bez licenčních poplatků a bez garance proti rušení. V České republice spravuje využití frekvenčního pásma výše zmíněný Český telekomunikační úřad, který uvádí frekvence k volnému použití schválenými zařízeními a zároveň zakazuje nebo omezuje použití některých frekvencí, které stát používá například pro účely obrany státu. V tabulce 1 je možné vidět rozdělení pásma podle ČTÚ, kde jsou vidět jak obsazené nebo zakázané, tak volné frekvence.

Tabulka 1 - Rozdělení frekvenčního pásma podle ČTÚ

27 MHz	Provozování je možné podle VO-R/10/07.2021-8.
49 MHz	Provozování není přípustné (zařízení ruší rozhlasovou službu a necivilní aplikace).
230–400 MHz	Pásmo je vyhrazeno pro účely obrany státu – žádný civilní provoz není přípustný.
433 MHz	Provozování je možné podle VO-R/10/07.2021-8. (Pouze přenos dat; bezdrátová sluchátka nejsou povolena.)
470−694 MHz, 823–832 MHz	Provozování bezdrátových mikrofonů je možné podle VO-R/10/07.2021-8.
694–823 MHz, 832–862 MHz	Provozování bezdrátových mikrofonů již není povoleno.
863–865 MHz	Provozování akustických aplikací je možné podle VO-R/10/07.2021-8.
863–876 MHz, 915–921 MHz	Provozování je možné podle VO-R/10/07.2021-8.
694–823 MHz, 832–862 MHz, 876–915 MHz, 921–960 MHz	Pásmo provozu mobilních sítí – provozování jiných aplikací není přípustné.
1,2 GHz	V Evropě není možné pro zařízení krátkého dosahu využívat.
1785−1805 MHz	Provozování bezdrátových mikrofonů je možné podle VO-R/10/07.2021-8.
2,4 GHz	Provozování (RLAN, RFID, zařízení krátkého dosahu) je možné podle VO-R/12/11.2021-11 nebo VO-R/10/07.2021-8.

Zdroj: (Český telekomunikační úřad, c2018)

Pásmo 2,4 GHz začíná na frekvenci 2400 MHz a končí na 2500 MHz.

Signál v 2,4 GHz pásmu se šíří podobně jako světlo, tedy v přímé linii a s omezenou viditelností. Tato viditelnost je však chápána v kontextu elektromagnetických vln. Materiály jako suchý papír, dřevo, plast, textilie, keramika nebo suché zdivo mohou být pro lidské oko neprůhledné, ale pro vlny o frekvenci 2,4 GHz jsou snadno prostupné. Na druhou stranu, plné akvárium, které je pro lidské oko průhledné, funguje jako účinná bariéra pro tyto vlny. Obecně platí, že pokud mají antény vzájemnou přímou viditelnost, je možné navázat spojení.

Podle Heydona (2012) existuje mnoho materiálů, které jsou pro signál prostupné méně a jiné více. Materiály, které obsahují vodu jsou obecně předpokládány za větší rušivý element pro elektromagnetické vlny než materiál s nízkou vlhkostí. Elektromagnetické vlny v pásmu 2,4 GHz mají tendenci odrážet se od hladkých kovových povrchů. To znamená, že v prostředí s kovovými budovami nebo místnostmi s kovovými obklady na stěnách a stropních podhledech může dojít k tomu, že signál vykazuje neobvyklé chování, například síla signálu se může zvýšit. Oproti tomu přírodní bariéry jako například lidské tělo jsou obecně neprostupné, a neodrážejí signál.

Délka vlny je přibližně 12 cm, a to je také vzdálenost, v jaké se mohou příjmové podmínky radikálně změnit. Pokud spojení něco stíní, je možné, že o pár decimetrů dál bude vše jinak.

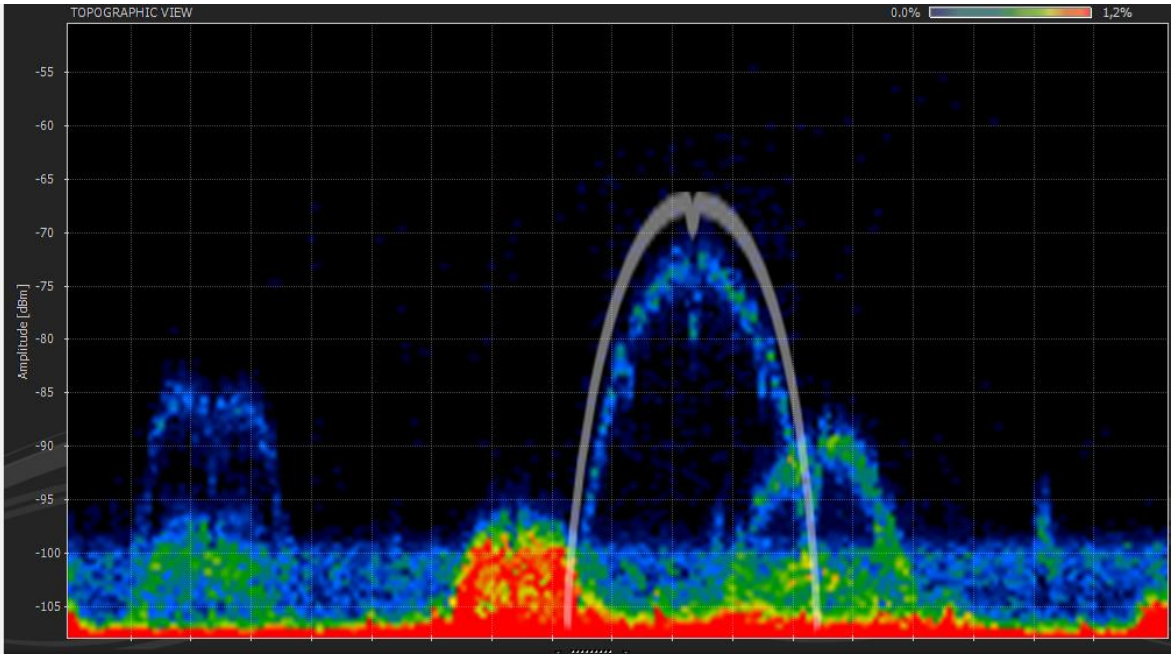
Pásmo 2,4GHz mohou využívat mobilní telefony, bezdrátová sluchátka, chytré hodinky (nutně ty zařízení, která nemají plný operační systém a nedokáží fungovat bez připojení k mobilnímu telefonu), bezdrátové myši, bezdrátové klávesnice. Periferie k počítači jako jsou bezdrátové myši, klávesnice a sluchátka mohou používat k připojení k počítači jeden z IEEE 802.11 standardů, tedy b/g/n nebo přímo spojení pomocí Bluetooth.

Podle Heydona (2012) pásmo 2,4 GHz ISM není dobré místo pro navrhování a používání bezdrátové technologie. Má špatné charakteristiky šíření, přičemž rádiová energie je snadno absorbována vším zejména však vodou. Tyto poměrně významné nevýhody kompenzuje skutečnost, že rádiové spektrum je dostupné po celém světě a neexistují žádné licenční požadavky. Tento volný přístup samozřejmě znamená, že prostor budou využívat i další technologie, včetně většiny Wi-Fi rádií. Stále existuje mnoho pravidel, souvisejících především s omezením výkonu zařízení využívajících spektrum, které tak omezují dosah signálu. Tato omezení jsou však stále atraktivnější než platit vysoké poplatky za licencované spektrum. Volba použití pásma ISM tedy snižuje náklady jak výrobcům zařízení používající tuto technologii a zároveň uživatelům, což je hlavní faktor pro využívání 2,4GHz ISM pásma.

3.3.1 **Wi-Fi na 2.4 GHz pásmu**

Není jedno jediné Wi-Fi, je hned několik norem, které tuto bezdrátovou technologii definují. V daném pásmu je určeno celkem 14 kanálů. První kanál je nastaven na frekvenci 2412 MHz a každý další kanál je o 5 MHz vyšší. Jedinou výjimkou je kanál 14, který je posunut na frekvenci 2484 MHz, jelikož jeho použití není v Evropě povoleno. Nicméně termín "kanál" neimplikuje, že by bylo možné bez vzájemného rušení provozovat 14 Wi-Fi spojení současně.

Obrázek 3 - Wi-Fi 802.11b na kanálu 9 (nejsilnější signál)

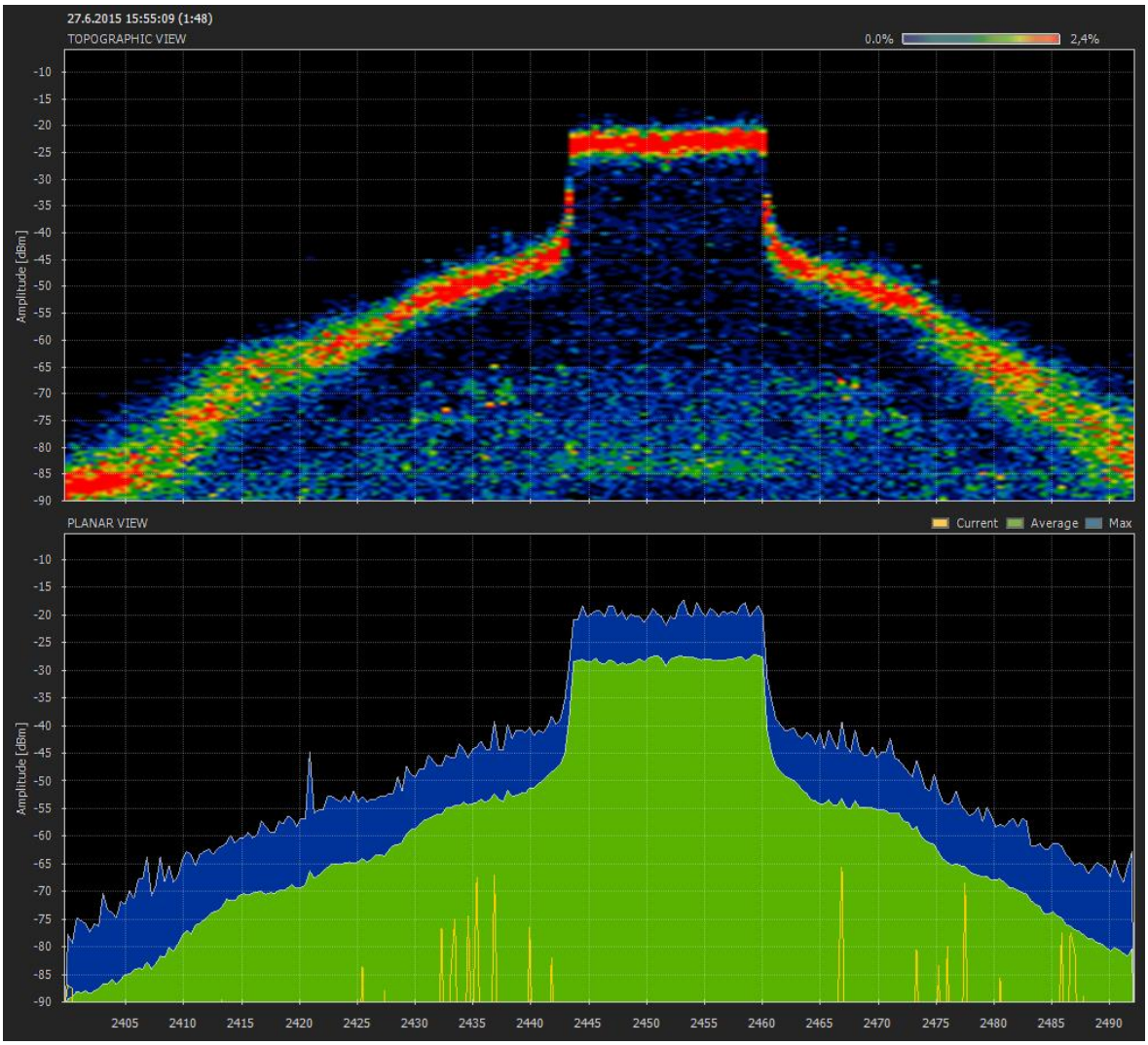


Zdroj: (Černý, 2015)

Černý (2015) specifikuje, že Wi-Fi podle normy 802.11b používá šířku kanálu 22 MHz, zatímco odstup kanálů je 5 MHz, takže při optimálním využití pásma mohou být současně v provozu nejvýše 3 Wi-Fi zařízení, aniž by se vzájemně rušila. Jeden přenos zabere „svůj" kanál a kromě toho ještě dva nahoře a dva dole. Spektrum má podobu kopečku s malým poklesem na vrcholu, jak je vidět na obrázku 3. Vzdálenější Wi-Fi na kanálu 9, to je nejsilnější signál zvýrazněný světlejší rozpoznávací křivkou, vedle něj vpravo je další slabší

(vzdálenější) signál další Wi-Fi 802.11b, který se částečně frekvencemi překrývá.

Obrázek 4 - Wi-Fi 802.11g na kanálu 9

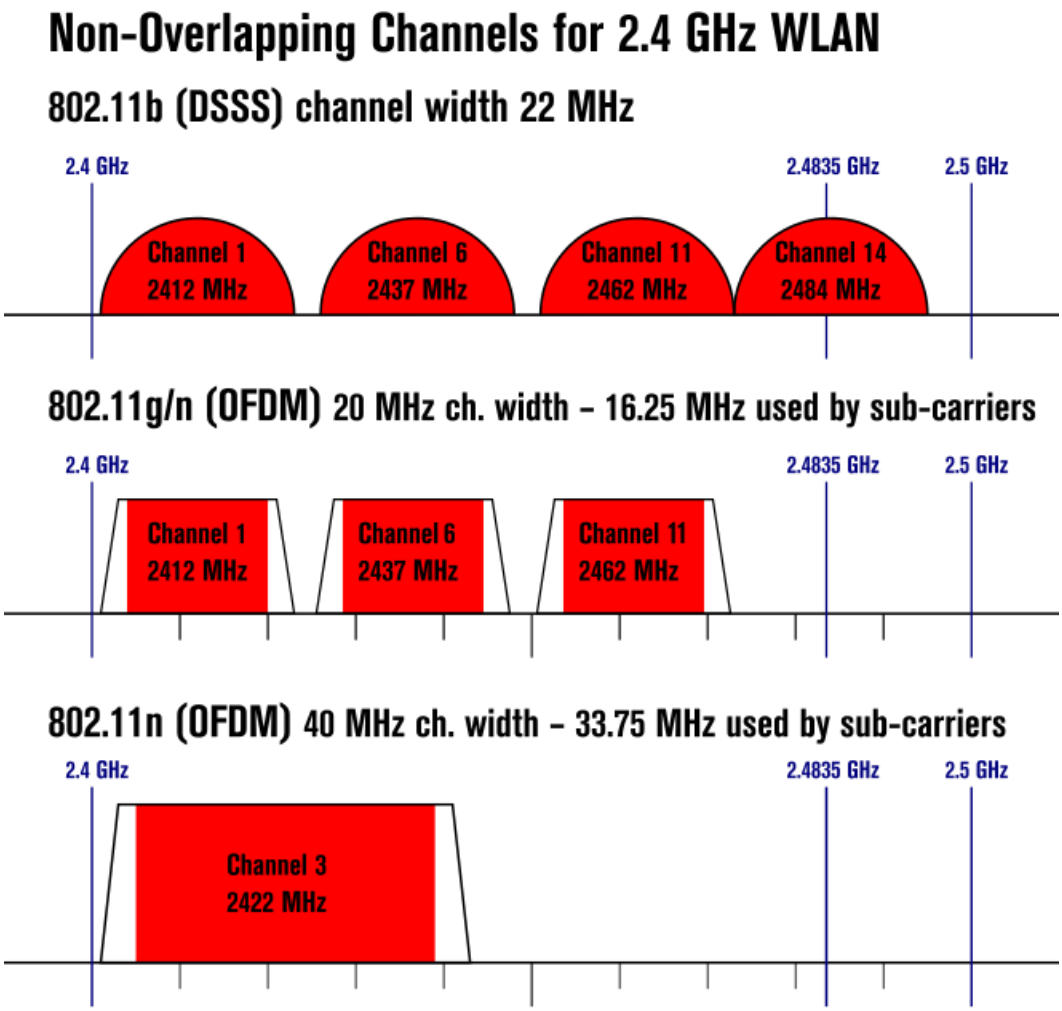


Zdroj: (Černý, 2015)

Černý (2015) uvádí, že Wi-Fi podle normy 502.11g/n má šířku kanálu 20 MHz a na snímku z analyzátoru má vyrovnanou úroveň v šířce pásma a strmé boky, takže tvoří jasně vymezený obdélník o výšce kolem 20 dB (okolí je potlačené z hlediska výkonu zhruba 100x). Také v tomto případě se současně dají provozovat nejvýše 3 zařízení bez vzájemného rušení. Toto chování zobrazuje obrázek 4. Wi-Fi podle normy 802.11n má podobný tvar, ale šířka pásma je 40 MHz, do pásma se současně vejdou nejvíce 2 přenosy tohoto druhu.

Černý (2015) dále uvádí, že k vysílání signálu nedochází nepřetržitě, jde o pulzy v čase v jednom relativně širokopásmovém, ale stabilním úseku pásma. Když spustíme dva přenosy, které se částečně nebo úplně překryjí co do rozsahu frekvencí, ještě to neznamená, že by se oba signály úplně vzájemně rušily a ani jeden z nich by nefungoval. Reálně bude přenos obou zařízení stále probíhat, částečně se bude rušit, ale částečně informace projdou v různé časové okamžiky. Dostupná rychlost přenosu dat se o něco (spíše velmi výrazně) sníží.

Obrázek 5 - Vyobrazení nepřekrývajících se kanálů Wi-Fi v 2,4GHz pásmu



Zdroj: (Liebeskind, 2011)

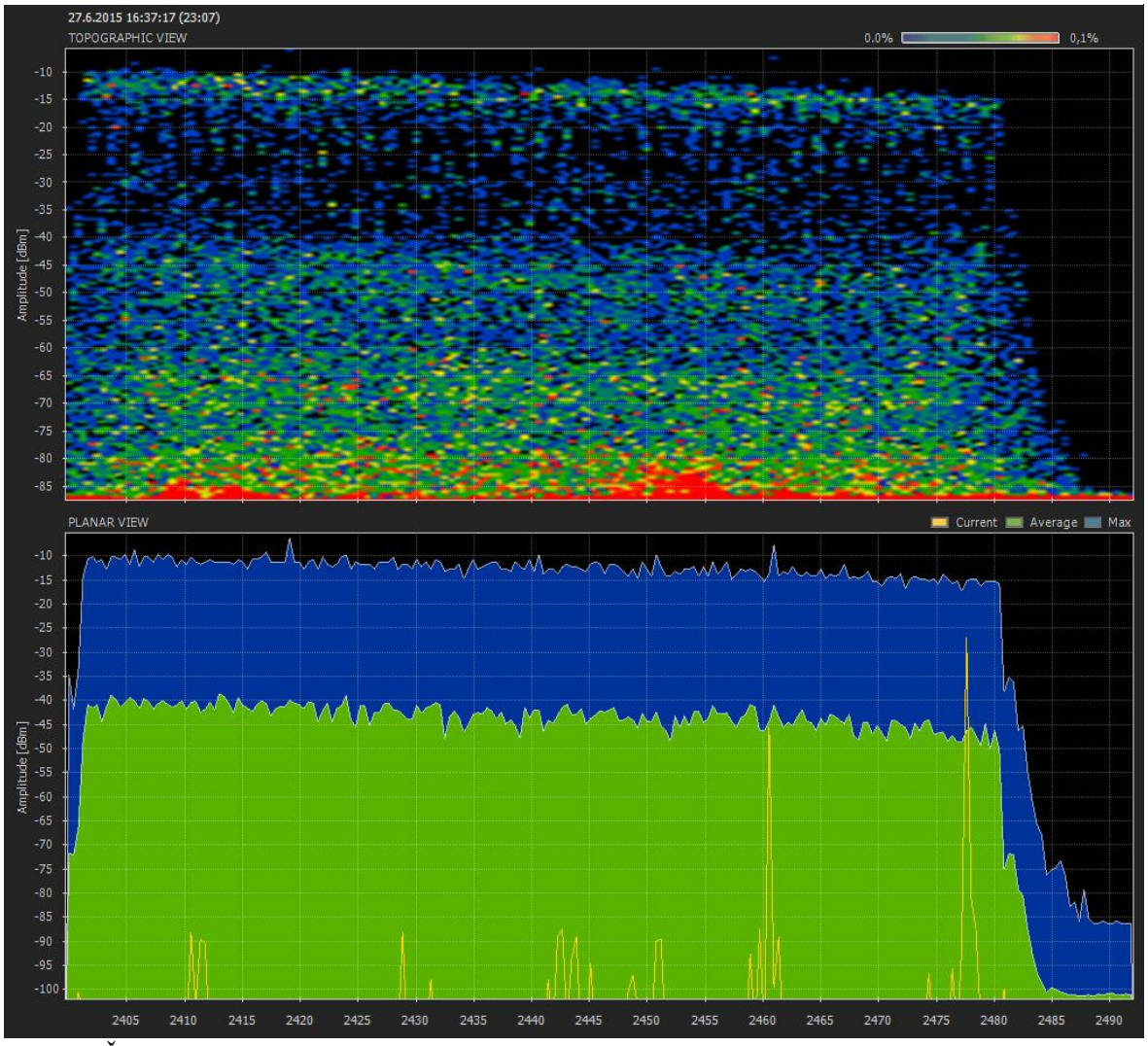
3.3.2 **Bluetooth na 2,4GHz pásmu**

Frekvence, kterou Bluetooth zabírá v 2,4GHz pásmu je v rozmezí 2,400-2,4835 GHz (Afaneh, 2018). Přenos dat pomocí Bluetooth zabírá pásmo úplně jiným způsobem než Wi-Fi a to tak, že neustále střídá frekvence, které využívá (více v kapitole 3.4). Na obrázku 6 je vidět jen souvislý blok signálu od 2,400 do 2,4835 GHz. Žádná z frekvencí

ale není obsazena trvale a když část pásma zabere jiné zařízení, pro přenos dat se využijí jiné volné frekvence s určitým zpomalením přenosu. Při navázání komunikace není třeba vybírat žádný kanál, střídání frekvencí se řídí automaticky. Bluetooth typicky pracuje s malým výkonem pod 15 mA. Uváděný dosah je kolem 10 m a je možné přepínat do různých módů (např. long-range mód typicky dosahuje 10 - 30 m) a v praxi velmi závisí na použitém módu a hlavně okolních podmínkách (Afaneh, 2018).

Vzhledem k omezenému výkonu hrozí rušení od Bluetooth jen na velmi malou vzdálenost a je nepravděpodobné. Rušení Bluetooth jiným zdrojem signálu je v teoreticky možné ale nepravděpodobné, pokud se zařízení nenachází na místě s velkým množstvím zařízení (cca více než 100) různého druhu, které vysílají nebo komunikují skrze 2,4GHz pásmo.

Obrázek 6 - Signál Bluetooth vysílaný z mobilního telefonu



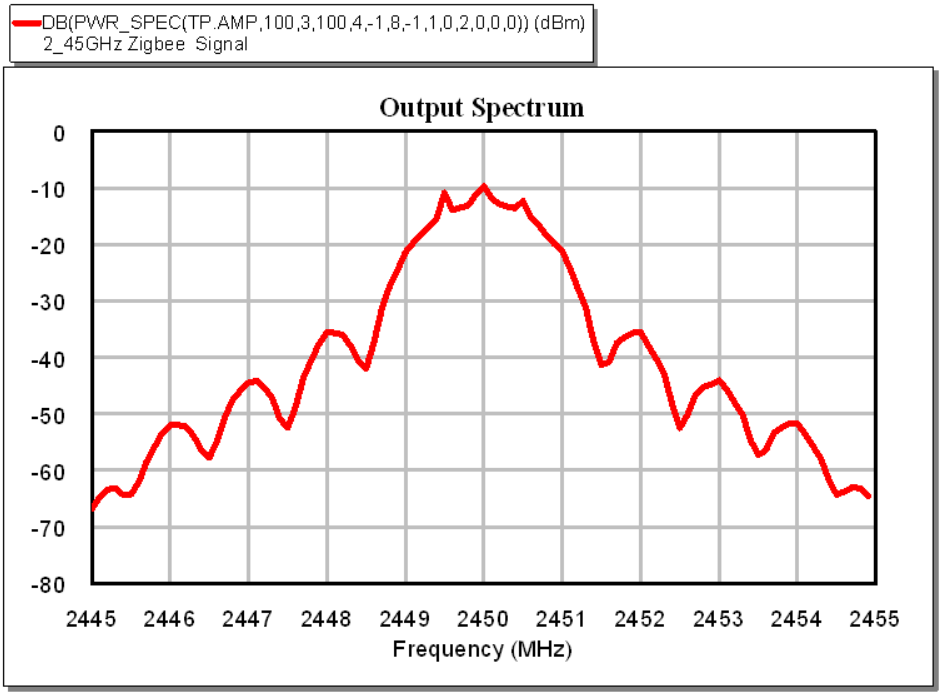
Zdroj: (Černý, 2015)

Zařízení s technologií Bluetooth LE také oznamují svou přítomnost opakovaným (tj. typicky každou vteřinu) vysíláním signálu typu „broadcast“, aby mohla být nalezena ostatními zařízeními. Tato akce se nazývá „advertising“ a je to standardní postup pro všechna BLE zařízení. Pro zmírnění účinků rušení od ostatních uživatelů pásma 2,4 GHz je každý advertising vysílán současně na třech široce rozmístěných rádiových kanálech (Leith a Farrell, 2020) (více v kapitole 3.8 Advertising).

3.3.3 **ZigBee**

Černý (2015) uvádí, že komunikace ZigBee se používá zejména v průmyslových podmínkách, kde není vhodné používat Bluetooth a stačí malý průtok dat. Najdeme ji ale také v dálkovém ovládání počítačových periferií, přenosech dat z čidel, ovládání přístrojů, ve zdravotnictví a podobně. Stejně jako Bluetooth jde o přenosy na menší vzdálenosti kolem 10 m.

Obrázek 7 - Charakteristika spektra ZigBee



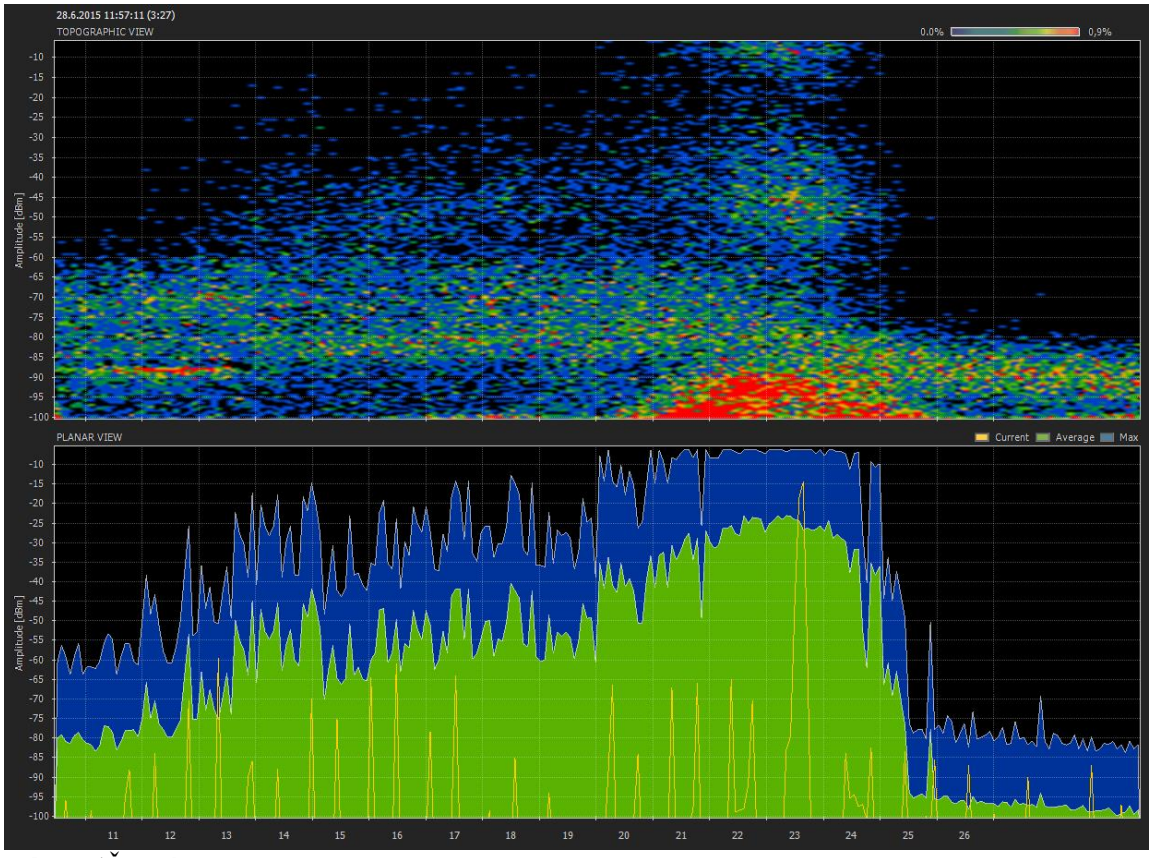
Zdroj: (Černý, 2015)

Obrázek 7 zkresluje dojem, protože nevyužívá celou šířku pásma 2,4 GHz, ale jen 10 MHz, jak je vidět na stupnici na obrázku. V tomto případě se pásmo dělí na celkem 16 kanálů (očíslovaných 11 až 26). Zařízení pracují s malým výkonem (1 mW) a velmi malou spotřebou.

Pravděpodobnost rušení signálem ZigBee je malá kvůli malému výkonu zařízení, velmi úzkému stabilnímu pásmu a zároveň kvůli pulznímu (většinou jen občasnému) provozu. Rušení ZigBee jiným signálem je podstatně pravděpodobnější, pokud by šlo o signál, který trvale vysílá, například mikrovlnné trouby (Černý, 2015).

3.3.4 **Mikrovlnné trouby**

Obrázek 8 - Signál elektromagnetických vln mikrovlnné trouby



Zdroj: (Černý, 2015)

Mikrovlnné trouby také fungují na 2,4 GHz pásmu. Jak je možné vidět na obrázku 8, mikrovlnné trouby nezabírají celou šířku pásma ale pouze výraznou část u středu pásma.

Černý (2015) specifikuje, že mikrovlnná trouba vysílá téměř nepřetržitě. Hlavní rozdíl oproti jiným zařízením na 2,4GHz pásmu je výkon. Zatímco například komunikace ZigBee pracuje s výkony 0,001 W a Wi-Fi 0,1 W, typická trouba pracuje s výkonem až 1000 W. Pokud by tento výkon byl vyzářen celý do vnějšího prostoru (to už by bylo pro osoby nacházející se v blízkosti takového záření velmi nebezpečné), zlikvidoval by prakticky celou komunikaci v pásmu 2,4 GHz v širokém okolí a blízká zařízení by dokonce zničil. To se naštěstí nestává, ale i únik 0,1% energie nedovírajícími dvířky nebo poškozeným stíněním v jejich okně má pořád 10x až 1000x vyšší výkon než výkony, které používáme ke komunikaci u Bluetooth.

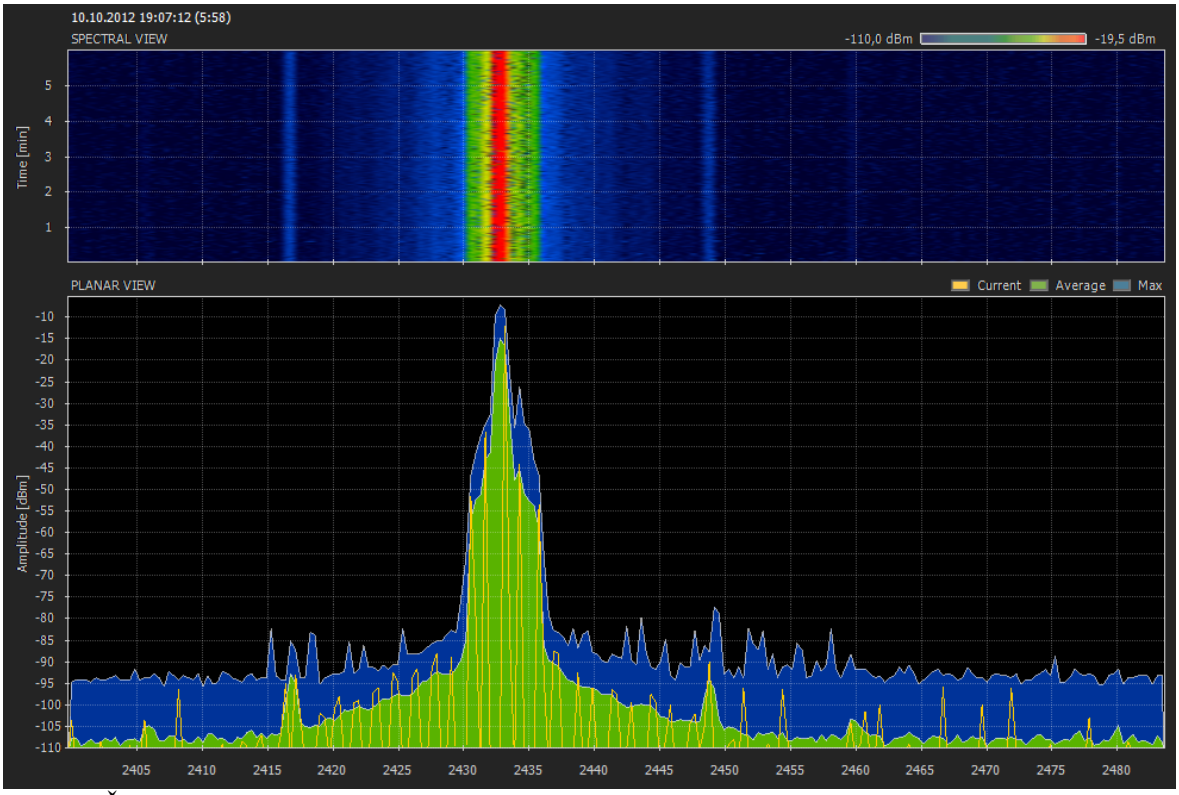
3.3.5 **RC vysílače**

Zařízení, které také ve vysoké míře obsazují 2,4GHz pásmo jsou RC vysílače. U těchto vysílačů se rozlišují dva typy přenosu, které se od sebe liší v obsazení pásma a změně kanálu v pásmu. Výkon těchto vysílačů je obvykle do 100mW, a tudíž je v porovnání s ostatními zdroji signálu nezanedbatelný.

3.3.5.1 DSSS

Černý (2015) specifikuje, že vysílače typu DSSS využívají jeden kanál, který je v čase poměrně silně zatížen (na dané frekvenci často přes 50% času). Tyto vysílače si automaticky zvolí neobsazený kanál, který už po čas jeho využívání nemění. Tyto vysílače jsou tím pádem velmi jednoduše rušitelné. Pokud se na jejich frekvenci po automatickém zvolení kanálu objeví jiný dostatečně silný signál, budou se velmi silně rušit. Dalším případem rušení je také to, že pokud si vysílač nalezne „neobsazený“ kanál a začne ho využívat, náhle se na něj připojí jiné zařízení, které ho už používá (např. pulzně) takovým způsobem, že vysílá signály jen jednou za určitý čas. Pro vysílač se tedy při vyhledávání kanálu jevila frekvence volná i přestože byla obsazená.

Obrázek 9 - využití 2,4GHz pásma DSSS RC vysílačem



Zdroj: (Černý, 2015)

3.3.5.2 FHSS

Černý (2015) dále specifikuje, že vysílače typu FHSS využívají větší počet zřetelně oddělených úzkopásmových kanálů, které se podle určitého algoritmu pravidelně střídají. Těchto kanálů může být mnohem více (např. 80), než můžeme vidět na obrázku 10, kde jich je 16. Tyto vysílače neuhýbají signálům jiných vysílačů, a protože projde třeba jen 10 % datových paketů, je ovládání cíleného objektu s nepatrně delší odezvou bezproblémové jako při volném pásmu. FHSS vysílače je obtížné rušit, protože signál většinou projde a mine se buď frekvencí anebo v čase. Naopak ale FHSS vysílače mohou velmi narušit například analogový videopřenos, u kterého je i 1% ztráta signálu velmi znát.

Obrázek 10 - využití 2,4GHz pásma FHSS RC vysílačem

Zdroj: (Černý, 2015)

3.4 Adaptive Frequency Hopping

Heydon (2012) konstatuje, že pásmo 2,4 GHz, na kterém Bluetooth LE pracuje, je již velmi přeplněné. Na tomto pásmu pracují například technologie založené na standardech IEEE 802.11, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n a IEEE 802.15.4. Kromě toho pásmo využívá také řada proprietárních rádií, včetně video opakovačů X10, bezdrátových alarmů, klávesnic a myší. Řada zařízení také vytváří šum v pásmu, například pouliční osvětlení a mikrovlnné trouby. Je tedy téměř nemožné navrhnout rádio, které bude vždy fungovat se všemi možnými rušivými vlivy, pokud nevyužívá adaptivní frekvenční přeskakování, které se objevilo již u Bluetooth Classic.

Adaptivní frekvenční přeskakování AFH (anglicky Adaptive Frequency Hopping) znamená, že komunikující zařízení nepřetržitě monitorují své prostředí z hlediska rušení signálu a neustále automaticky mění mapu kanálů, aby se rušení signálu vyvarovala (Silicon Labs 2020).

Heydon (2012) dále uvádí, že adaptivní frekvenční přeskakování pomáhá nejen rychlou detekcí zdrojů rušení, ale také tím, že se jim v budoucnu adaptivně vyhýbá. Rychle se také zotavuje z nevyhnutelných zahozených paketů způsobených rušením z jiných rádií. Právě tato robustnost je naprosto klíčová pro úspěch jakékoli bezdrátové technologie v tomto rádiovém spektru. Robustnost také zahrnuje schopnost detekovat a zotavit se z bitových chyb způsobených šumem na pozadí.

3.5 Rušení signálu Bluetooth

Rušení signálu z hlediska obsazení frekvence je u Bluetooth pravděpodobné ale ne zcela stoprocentní, pokud se v okolí nachází zařízení vysílající na stejném kanálu. Díky funkci adaptivního frekvenčního přeskakování (více výše v kapitole 3.4) se dokáží zařízení komunikující přes technologii Bluetooth tomuto rušení vyvarovat (Heydon, 2012). Avšak ne vždy je to funkce na kterou by se dalo spoléhat, protože 2,4GHz pásmo není tak velké a pokud se tyto zařízení nacházejí v prostředí s opravdu velkým provozem bezdrátové komunikace v 2,4GHz pásmu, je rušení signálu skoro zaručené.

Co se týče externích vlivů, které se podílí na rušení Bluetooth signálu, můžeme je považovat za zanedbatelné a relativně snadno překonatelné v závislosti na aplikaci a použití zařízení s technologií Bluetooth. Obecně platí, že rádiový signál se stává slabším s rostoucí

vzdáleností, protože vysílací výkon se rozprostírá na větší plochu. Nicméně na toto základní chování působí mnoho složitých efektů, zejména překážky na cestě mezi vysílačem a přijímačem (nábytek, stěny atp.), které mohou pohltit nebo odrazit rádiový signál a způsobit jeho vyšší nebo nižší sílu. Tělo člověka, které obsahuje 50-75% vody (Krajská nemocnice Tomáše Bati, a.s., 2022), pohlcuje elektromagnetické vlny rádiového signálu, takže síla přijatého signálu se může výrazně snížit, pokud se tělo nachází na přímé trase mezi vysílačem a přijímačem (Leith a Farrell, 2020; Heydon, 2012).

Dále jsou rušivým elementem určité materiály ve zdech, nebo sloupech. Pokud se na trase mezi zařízeními, které komunikují pomocí technologie Bluetooth, nachází tenké stěny (například v panelovém domě), je velmi pravděpodobné, že spojení bude jen velmi málo až nepozorovatelně rušené. Pokud jsou však mezi těmito komunikujícími zařízeními objekty s vysokým objemem kovu (například kovové vyztužení stěn), je zde větší pravděpodobnost, že bude signál vysílajícího zařízení odražen a druhé zařízení nebude schopno signál přijmout.

Dále pak bylo zjištěno, že šum generovaný datovým spektrem USB 3.0 může mít také dopad na rádiové přijímače, pokud je jejich anténa umístěna v blízkosti zařízení s konektorem USB 3.0 (Intel Corporation, 2012). To má pak za následek snížení provozního bezdrátového dosahu zařízení. Tomuto šumu se dá vyvarovat stíněním konektoru USB 3.0 nebo samotné periferie využívající tento port určitými kovovými materiály, které tento šum nepropouští ale odráží.

Aspektů, které se u rušení signálu Bluetooth vyskytuje není mnoho a v celkovém pohledu na rušení signálu jsou zanedbatelné a prakticky relativně snadno překonatelné.

3.6 Síla signálu

Leith a Farrell (2020) konstatují, že důležitým faktorem spolehlivosti bezdrátového přenosu dat a komunikace mezi zařízeními je také síla signálu, která je determinována především sílou vysílajícího zařízení. U mobilních telefonů je to faktor velmi důležitý a je ovlivňován jak vnitřními, tak vnějšími vlivy. Obecným odhadem je, že beacony nelze dekódovat na vzdálenosti větší než přibližně 10 metrů od vysílače. Nicméně v praxi je síla přijatého signálu také silně ovlivněna způsobem, jakým se rádiový signál šíří od vysílače k přijímači a z jakého materiálu jsou překážky na přímé cestě mezi oběma zařízeními.

Základním ukazatelem síly signálu pro Bluetooth je RSSI (Received Signal Strength Intensity). RSSI se měří v jednotkách dBm (decibel-milliwatts). Tuto hodnotu RSSI lze odečíst od Tx Power, který bývá zahrnut v advertising paketech, a poskytnout tak velmi základní odhad ztráty cesty, a tedy odhad vzdálenosti mezi zařízením ze kterého signál zachytáváme a zachytávaného zařízení. Stojí za zmínku, že toto měření RSSI je náchylné na okolní šum s kolísáním ± 5 dBm nebo více i v situacích s jednoduchým rádiovým přenosem v přímé viditelnosti (Leith a Farrell, 2020).

Stupnice pro RSSI je interpretována tak, že 0dBm je dostupná absolutní síla signálu a čím více se RSSI propadá do záporných hodnot, tím vyšší je šum v přenosu a tím slabší je spojení.

Za účelem správné detekce přijatého signálu bezdrátového rádiového přijímače musí být síla přijatého signálu větší než citlivost rádia/přijímače. Citlivost přijímače je ovlivněna minimálním poměrem signálu k šumu (SNR), který je potřebný pro demodulaci[4].

Teoreticky se zvyšující se vzdáleností mezi komunikujícími zařízeními snižuje síla signálu, není to však pravidlem a to například kvůli materiálům v okolí zařízení, které mohou signál naopak posílit nebo úplně odrazit (Leith a Farrell, 2020). Zároveň se zvýšeným výskytem širokopásmového šumu na delší lince klesá skutečný poměr signálu k šumu na přijímači a tím se snižuje bezdrátový dosah. Snížení dostupného SNR na přijímači vyžaduje zvýšení minimální úrovně signálu, aby byla překonána citlivost přijímače.

Pokud je síla přijatého signálu příliš slabá, přenos není vůbec zaznamenán nebo selže ladící proces. Obvykle k tomu dochází, když síla přijatého signálu je pod cca -90 dBm.

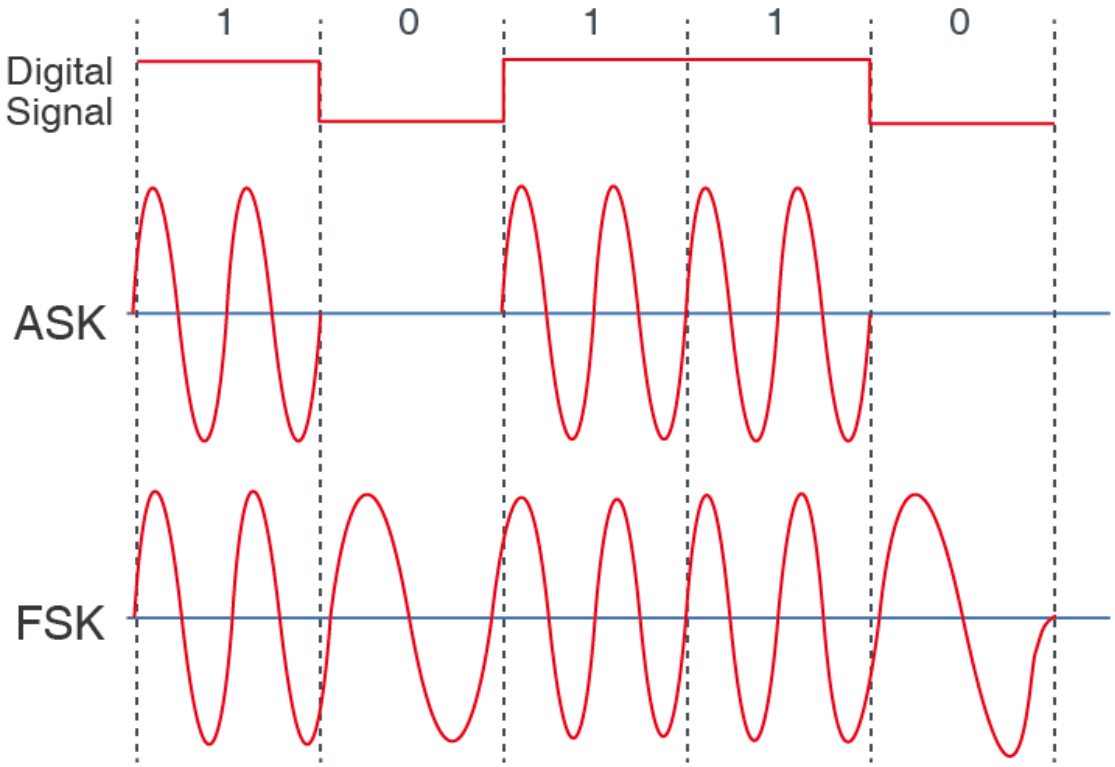
3.7 Modulace signálu

Modulace je proces převodu dat na elektrické signály optimalizované pro bezdrátový přenos. Mezi hlavní typy modulace signálu patří Analogová modulace a Digitální modulace. Analogová modulace se typicky používá pro modulaci a následný přenos signálů pro AM,

[4] Demodulace je proces získávání původního signálu nebo dat z modulovaného nosného signálu z bezdrátového přenosu.

FM rádio a vysílání na krátkých vlnách. Digitální modulace zahrnuje přenos binárních (0 a 1) signálů.

Obrázek 11 - Rozdíl mezi ASK a FSK metodami modulace



Zdroj: (ROHM Semiconductor, c2023)

Technik pro modulaci signálu je několik. Mezi ty hlavní patří ASK a FSK. Obrázek 11 znázorňuje, jak metoda ASK (Amplitude Shift Keying) digitální modulace odesílá přenosová data změnou přítomnosti a nepřítomnosti analogových signálů. Oproti tomu metoda FSK (Frequency Shift Keying) využívá rozdíl v šířce analogových signálů k modulaci digitálních signálů přepínáním mezi nízkou a vysokou frekvencí, aby reprezentovala 0 a 1 (ROHM Semiconductor, c2023).

Bluetooth používá formu modulace signálu GFSK (Gaussian Frequency-Shift Keying) (Heydon, 2012; Chang, 2014). Jedná se o FSK typ modulace signálu, který tvaruje impulsy před jejich modulací. Tento způsob filtrování snižuje výkon postranního pásma, rušení způsobené sousedními kanály nebo šířku pásma signálu FSK. Po přijetí signálu pak přijímací zařízení demoduluje a sestaví bity tak aby utvořilo data ve stejném formátu, než byla modulována pro bezdrátový přenos.

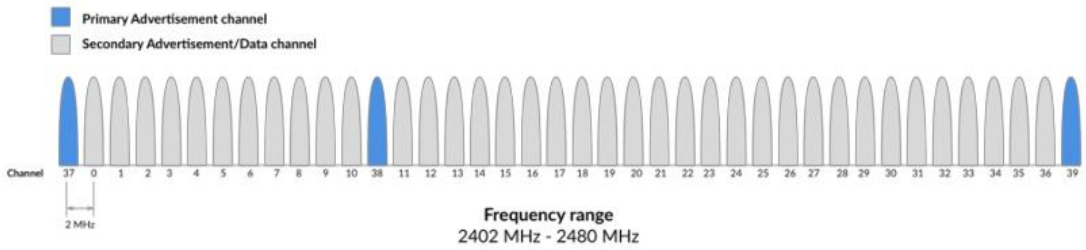
3.8 **Advertising**

Heydon (2012) uvádí, že Bluetooth LE disponuje podporou bezdrátového modelu Přítomnost (z anglického Presence). Přítomnost v tomto smyslu znamená stav nebo skutečnost existence, výskytu nebo přítomnosti na místě nebo věci elektronického zařízení komunikujícího skrze bezdrátovou technologii Bluetooth. Pomocí modelu reklamy nebo také oznamování (z anglického advertising model) mohou zařízení pasivně skenovat na pozadí jiná zařízení, která vysílají.

Model oznamování je relativně nový režim definovaný ve spojové vrstvě ISO/OSI[5] modelu a funguje na základě dosahu určitého obsahu ke specifické skupině. Zařízení používá tento model u Bluetooth tak, že odesílá modulovanou zprávu, která může obsahovat jeho adresu nebo data založená na přítomnosti, bezdrátově prostřednictvím technologie Bluetooth. Tuto zprávu mohou přijmout, demodulovat a zpracovat zařízení, která jsou schopna bezdrátové komunikace prostřednictvím Bluetooth.

Afaneh (2018) uvádí, že v advertising (oznamovacím) stavu odesílá zařízení pakety obsahující užitečná data, která mohou ostatní zařízení přijmout a zpracovat. Pakety jsou odesílány v pevném intervalu definovaném jako reklamní interval. V BLE je 40 kanálů vyhrazených pro advertising. Tyto kanály jsou od sebe odděleny v pásmu frekvencí 2 Hz (od středu ke středu).

Obrázek 12 - Rozdělení kanálů v advertising modelu



Zdroj: (Afaneh, 2018)

Afaneh (2018) také konstatuje, že vzhledem k tomu, že se jedná o tři kanály, na kterých zařízení vysílá advertising pakety, a obvykle mezi nimi přepíná, jsou ve frekvenčním spektru

[5] ISO je zkratka pro organizaci, která se stará o standardy (anglicky International Organization for Standardization) a OSI je zkratka pro model síťové komunikace mezi počítači (anglicky Open Systems Interconnection).

rozprostřeny, aby se zabránilo rádiovému rušení mezi zařízením, které inzeruje na jednom kanálu a druhým, které inzeruje na jiném kanálu. Také umístění těchto primárních kanálů (kanály 37, 38 a 39) byly vybrány v rámci spektra, aby se zabránilo interferenci s nejběžněji používanými WiFi kanály.

3.9 **BLE sniffer**

BLE sniffer, je zařízení známé také jako analyzátor protokolu Bluetooth. Jedná se o pasivní zařízení, které zachytává BLE (Bluetooth Low Energy) pakety vysílané vzduchem z různých zařízení v přímém rádiovém dosahu. BLE sniffer je pasivní zařízení, protože neinteraguje s ostatními zařízeními na základě vysílaných paketů, ale pouze je čte a zpracovává, a ostatní zařízení tedy o existenci snifferu v jejich okolí nevědí (Afaneh, 2022).

Afaneh (2022) uvádí, že BLE sniffer dokáže pracovat ve 2 režimech. Jedním z nich je „advertising mode“, ve kterém sniffer zachytává advertising pakety. Ve druhém režimu „connection mode“ zachycuje sniffer nezpracovaná data v podobě paketů, která si vyměňují 2 zařízení při vzájemné BLE komunikaci.

Sniffery se dají podle funkce rozdělit do 2 kategorií.

3.9.1 **Sniffery BLE založené na vývojové sadě**

Tento typ BLE snifferu dokáže typicky zachytit pakety jen na jednom frekvenčním kanále zároveň ať už se jedná o kanál pro advertising pakety nebo samotný přenosový kanál.

Když sniffer zachycuje advertising pakety, nepřetržitě přepíná mezi třemi primárními advertising kanály (37, 38 a 39), aby se pokusil zachytit co nejvíce advertising paketů. To samozřejmě znamená, že některé pakety nevyhnutelně ztratí, ale čím déle sniffer pracuje, tím větší je pravděpodobnost, že zachytí ztracené pakety.

Pokud zachycuje sniffer pakety z komunikace spojených zařízení, zachytává je ze zbylých 37 kanálů. Pokud jde o zachycení spojení, tyto sniffery jsou obvykle schopné zachytit pouze jedno spojení v daném okamžiku. Mohou detekovat spojení tím, že se přepnou na poslech na konkrétním frekvenčním kanálu, na kterém si dvě komunikující BLE zařízení vyměňují pakety. Když jsou dvě zařízení Bluetooth Low Energy připojena, využívají mechanismus frekvenčního přeskakování (AFH), kde si vyměňují pakety na určitém frekvenčním kanálu,

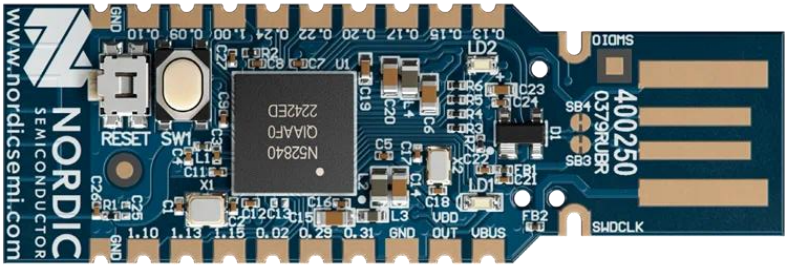
který se v průběhu spojení mění, aby se předcházelo ztracení paketů, kvůli vysokému vytížení jednoho kanálu jinými zařízeními.

Podle Afaneha (2022) jsou tyto sniffery obvykle založeny na existujících vývojových sadách, což znamená, že využívají existující vývojové sady BLE poskytované dodavatelem, který také poskytuje firmware pro BLE sniffer. Obvykle nepodporují všechny nejnovější aktualizace standardu Bluetooth. To je proto, že se nejedná o specializované sniffery a tato funkce je poskytována jako další funkce pro jejich zákazníky. Obvykle využívají open-source software jako rozhraní pro prohlížení zachycených paketů, jako je například aplikace Wireshark.

Cena snifferu je nízká. Často se jedná pouze o náklady na hardware (vývojovou sadu) a firmware pro sniffer BLE je poskytován zdarma. Jsou však výjimky v podobě více komplexnějších řešení, avšak to se projevuje na cenách zařízení.

Příkladem takového snifferu je například Nordic nRF Sniffer (nRF52 PCA10059 USB dongle) který je vidět na obrázku 13. Cena tohoto snifferu se pohybuje okolo $10 (236.27 KČ v přepočtu k 19.2.2024 ze středního kurzu ČNB).

Obrázek 13 - Nordic nRF Sniffer (nRF52 PCA10059 USB dongle)



Zdroj: (Afaneh, 2022)

Výhody takového snifferu jsou:

- velmi nízká cena,
- plná podpora Bluetooth 5,
- integrace s balíčkem aplikací a prostředím od společnosti Nordic Semiconductor,
- aplikace nRF Connect for desktop, která umožňuje velmi snadnou práci se zařízením.

V rozsáhlé dokumentaci ke snifferu lze také nalézt návod k instalaci do prostředí aplikace Wireshark.

Nevýhody takového zařízení jsou:

- zachytávání paketů pouze na 1 frekvenčním kanále,
- občasné zahození paketů,
- pomalá integrace nových Bluetooth funkcí.

3.9.2 **Dedikované BLE sniffery**

Podle Afaneha (2022) jsou tyto typy BLE snifferů jsou obvykle založeny na softwarově definovaném rádiu (SDR), což znamená, že mohou zachytit celé rádiové spektrum zároveň. Tyto typy snifferů jsou určeny jako vyhrazená zařízení, takže jsou mnohem schopnější než sniffery založené na vývojové sadě. Mohou zachytit všechny typy BLE paketů (reklamní a datové) na všech 40 kanálech. Mohou zachytit více připojení současně. Mohou zachytit všechny advertising pakety v oblasti, aniž by museli přeskakovat mezi třemi advertising kanály.

Vzhledem k tomu, že se jedná o specializované sniffery, dodavatelé podporují nejnovější verzi standardu Bluetooth. Počítačový software používaný k propojení se snifferem obvykle poskytuje prodejce a je vyvinut na zakázku, místo aby se spoléhal na software s otevřeným zdrojovým kódem. Náklady jsou obvykle velmi vysoké ve srovnání se sniffery založenými na vývojové sadě, ale to je způsobeno technickými náklady spojenými s vývojem a udržováním funkčnosti snifferu.

Příkladem takového snifferu je Ellisys Bluetooth Tracker, který je vidět na obrázku 14. Je nutné podotknout, že takový sniffer není volně dostupný ke koupi a je nutná konzultace s obchodním zástupcem společnosti Ellisys. Cena takového snifferu začíná na $10,000

(236 270 KČ v přepočtu k 19.2.2024 ze středního kurzu ČNB) a zvyšuje se na základě použití softwarových funkcí (Afaneh, 2022).

Obrázek 14 - Ellisys Bluetooth tracker

Zdroj: (Afaneh, 2022)

Výhodami takového snifferu jsou:

- Kompaktnost a přenosnost,
- podporuje nejnovější vydanou specifikaci Bluetooth low energy,
- podporuje Wi-Fi a další technologie založené na 802.15.4 standardu,
- nižší cena než alternativy jiných výrobců,
- software v počítači je jednoduchý na použití.

Nevýhodou je jednoznačně cena, která činí toto zařízení nedostupné pro většinu a software je pouze na operační systémy Windows (Afaneh, 2022).

Oproti tomu Spanalytics PANalyzr je relativně dostupnější sniffer, u kterého není vyžadována konzultace s obchodním zástupcem společnosti ke koupi. Cena je okolo $8,995 (212 524.865 KČ v přepočtu k 19.2.2024 ze středního kurzu ČNB).

Obrázek 15 - Spanalytics PANalyzr

Zdroj: (Afaneh, 2022)

Mezi výhody tohoto snifferu patří:

- Bluetooth (BR/EDR + BLE), Wi-Fi a 802.15.4,
- relativně malá velikost,
- WIDS modul (volitelný modul bezdrátového systému detekce narušení),
- napájení přes USB,
- snadné nastavení,
- vnitřní paměť (samostatné snímání s napájením z baterie),
- volitelné analytické moduly,
- podpora Windows, Linux a macOS operačních systémů,
- lze zakoupit online bez konzultace s obchodním zástupcem.

3.10 **Bezpečnost**

Bezpečnost je jedním z nejzákladnějších a nejdůležitějších faktorů u bezdrátové technologie a IoT systémů. Zařízení Bluetooth mohou být ověřena a spojení mohou být šifrována.

Vzhledem k ad hoc (dočasnému spojení mezi dvěma rovnocennými prvky) povaze komunikace Bluetooth a skutečnosti, že zařízení Bluetooth nezávisí na komunikačních službách infrastruktury, je autentizace zařízení Bluetooth založena na mechanismu výzva/odpověď na základě běžně sdíleného tajného odkazového klíče generovaného prostřednictvím uživatelem poskytnutého PIN (Heydon, 2012).

Na straně bezpečnosti se u bezdrátové komunikace BLE vyskytují následující nejčastější obavy jako jsou:

- autentizace, kterou rozumíme důkaz, že druhá strana je tím, za koho se vydává;
- autorizace, která je definována jako oprávnění něco dělat, v případě bezdrátové technologie oprávnění provádět určité operace na připojeném zařízení;
- integrita, která zajišťuje, že přijatá data jsou bez poškození a nejsou vystavena neoprávněné manipulaci neoprávněnými zařízeními.
- důvěrná je komunikace, která je čitelná pouze pro oprávněné uživatele nebo zařízení a nikoho jiného;
- soukromí znamená, že zprávy námi odesílané jsou anonymní nebo je obtížné sledovat zařízení, ze kterého jsou zprávy odesílané.

Tyto principy jako celou bezpečnost komunikace u bezdrátového přenosu by nebylo nutné zmiňovat, kdyby nebylo útoků na tuto komunikaci. Mezi nejčastější útoky na bezdrátovou komunikaci řadíme (Afaneh, 2018):

- pasivní odposlouchávání kdy škodlivé zařízení naslouchá komunikaci mezi dvěma zařízeními a je schopno porozumět přenášeným datům, což je obvykle umožněno díky získání přístupu k šifrovacímu klíči, pokud jsou data šifrována;
- aktivní odposlouchávání jako útok také známý jako MITM (z anglického Man In The Middle), kde se škodlivé zařízení vydává za obě zařízení (periferní i centrální) a zachytává jejich komunikaci, kterou pak následně přesměruje správnému zařízení, aby se vyhnulo podezření z útoku na komunikaci, a dokonce i může pozměňovat zprávu;
- sledování soukromí a identity při kterém jsou zařízení a jejich uživatelé sledováni pomocí adresy Bluetooth, což může odhalit jejich polohu.

Heydon (2012) a Afaneh (2018) uvádí, že samotná bezpečnost a její implementace je v BLE spravována pomocí vrstvy bezpečnostního manažeru SM (z anglického Security Manager)

v architektuře BLE. Tento bezpečnostní manažer obsahuje protokoly a algoritmy pro generování a výměnu sdílených tajemství mezi zařízeními. BLE komunikaci mezi zařízeními lze pomocí SM zajistit způsoby:

- párováním, což je proces, kdy si dvě komunikující zařízení vytvoří a vymění sdílená tajemství mezi sebou;
- spojením kdy zařízení vytváří a ukládají sdílená tajemství na každé straně (centrální a periferní) pro použití v následujících dalších spojení mezi nimi;
- autentizací na základě předešlých sdílených tajemství (tj. ověření totožnosti pomocí klíčů);
- šifrováním pomocí 128bitového standardu AES Encryption, což je algoritmus symetrického klíče kde se stejný klíč se používá k šifrování a dešifrování dat na obou stranách;
- integritou zpráv, což je proces digitálního podepisování dat a ověřování podpisu na druhém konci, což ve své podstatě přesahuje jednoduchou cyklickou redundantní kontrolu CRC (z anglického Cyclic Redundancy Check) integrity přenosu.

Specifikace Bluetooth se ale časem postupně rozrůstá a nabývá komplexnosti a bezpečnosti. Konkrétně v BLE ve verzi 4.2 byl představen LESC (z anglického Low Energy Security Connections) koncept, který využívá protokol Diffie-Hellmanovy eliptické křivky při procesu párování. Díky tomuto protokolu je komunikace mezi zařízeními bezpečnější, než tomu bylo v předešlých verzích BLE (Heydon, 2012; Afaneh, 2018).

V BLE je hlavní zařízení (např. mobilní telefon) iniciátorem bezpečnostních procedur. Slave (respondér) může požádat o zahájení bezpečnostní procedury zasláním zprávy s bezpečnostním požadavkem na hlavní zařízení, ale na hlavním zařízení závisí odeslaný paket, který oficiálně spustí proces zabezpečení (Afaneh, 2018).

3.11 **Určování polohy**

Pro běžného uživatele a spotřebitele je GPS (Global Positioning System) nejznámější technologií pro určování polohy elektronických zařízení. Technologií GPS dnes disponují různá zařízení, od mobilních telefonů přes chytré hodinky až po automobily, která tuto technologii využívají například k přesnému určení polohy venku, k nalezení lokace určitého zařízení nebo k navigaci v rámci elektronických map.

Důležité je zde slovo „venku“ jelikož technologie GPS funguje na bázi komunikace zařízení se satelity na orbitu planety Země. Poloha touto technologií se určuje výpočtem trilaterace[6] a doby, za kterou se signál ze zařízení dostane k satelitům a zpět (National Coordination Office for Space-Based Positioning, Navigation and Timing, 2014; Garmin, 2023).

Určení polohy pomocí GPS je tak velmi přesné, pokud zařízení „vidí“ přímo na satelit. Globální systémy navigace pomocí satelitů (GNSS) umožnily přesné určení polohy venku, ale neschopnost těchto signálů proniknout s uspokojujícím výsledkem do budov znamená, že je nutné najít jiné metody pro určení polohy uvnitř.

Dnes nejběžnější technologie používaná spotřebiteli v nepřítomnosti GPS a GNSS je Wi-Fi. Na určení polohy nejen uvnitř se proto začala více používat technologie Wi-Fi. Hrubé určení polohy pomocí Wi-Fi je pevně integrováno do mnoha mobilních platforem a umožňuje lokalizaci v městském prostředí na úrovni desítek metrů (Faragher a Harle, 2015). Algoritmy jsou v podstatě založeny na blízkosti, spoléhající se na relativně krátký prostorový dosah Wi-Fi vysílačů a signálový průzkum.

Podle Faragher a Harle (2015) dalšími kandidáty na snímání rádiových signálů na spotřebitelských zařízeních jsou signály z mobilních sítí a Bluetooth. Zdroje mobilních sítí jsou obvykle příliš řídce rozloženy pro vytvoření dobrých vzorků snímání uvnitř, zatímco praktické problémy omezily hodnotu sledování Bluetooth, zejména velmi dlouhé doby skenování. Nicméně zavedení specifikace Bluetooth 4.0 potenciálně řeší tyto problémy prostřednictvím podsystému Bluetooth Low Energy.

Faragher a Harle (2015) také uvádí, že Bluetooth LE je již podporováno na většině nasazených zařízení u koncových zákazníků a je navrženo pro komunikaci point-to-point[7] s ohledem na Internet věcí. Zařízení BLE jsou malá, levná a navržena tak, aby běžela na baterie po mnoho měsíců nebo let, a očekává se, že v budoucnosti bude mnoho budov obsahovat vysokou hustotu zařízení BLE.

Ukazatelem vzdálenosti od přijímače pro Bluetooth může být RSSI (přijatá síla signálu). Tuto hodnotu lze nalézt v každém přeneseném paketu.

---

[6] Trilaterace je určení polohy bodu na základě znalosti jeho vzdálenosti od alespoň 3 jiných známých bodů.

[7] Název „point-to-point“ označuje přímou formu komunikace mezi dvěma zařízeními bez dalšího zařízení či serveru, který by zprostředkovával komunikaci mezi nimi.

Podle Gao (2015) můžeme na základě kolísání rádiových signálů získat poměrně přesný výsledek trendu RSSI. Snadno poznáme, zda je signál silnější nebo slabší, takže budeme vědět, zda se pohybujeme směrem ke zdroji nebo od něj. Ještě lépe, pokud rozumíme specifickému mapování mezi RSSI a umístěním konkrétního přijímacího zařízení, mohli bychom mít poměrně přesný odhad vzdálenosti.

Leith a Farrell (2020) provedli také testování síly přijatého signálu Bluetooth Low Energy dvou zařízení mezi sebou a na základě toho vyplynulo, že Bluetooth není spolehlivá technologie pro účely zjišťování, jestli mezi sebou přišli 2 lidé nebo 2 zařízení do kontaktu. Teoretický předpoklad, že při zvyšující se vzdálenosti mezi zařízeními dochází ke snížení síly signálu prakticky nebyl naprosto vyvrácen, avšak ani zcela potvrzen. Podle naměřených dat bylo zjištěno, že síla přijatého signálu RSSI (Received Signal Strength Indication) se nemusí nutně snižovat se zvyšující se vzdáleností mezi zařízeními. Faktorů, které ovlivňují tento výsledek je vícero ve vnitřních i venkovních prostorách a vyplynulo, že nevykazují konzistentní chování. Zároveň bylo konstatováno, že v této oblasti trasování kontaktu pomocí Bluetooth Low Energy by bylo náročné a časově velmi zatěžující vyvinout a uskutečnit spolehlivé měření na základě současné technologie. Pro budoucí použití je potřeba další práce, aby bylo možné kvantifikovat chybovost metod detekce blízkosti založených na síle přijímaného signálu Bluetooth LE.

4 Praktická část práce

4.1 Zachytávání paketů

Pro potřeby zachytávání v testovacím centru byla vybrána technologie Bluetooth LE na základě jejích charakteristik. Téměř všechna zařízení, která by se teoreticky mohla vyskytovat v testovacím centru proti jeho řádu jsou schopna Bluetooth LE komunikace.

K zachycení zařízení v testovacím centru je důležité, aby byly zachyceny Bluetooth advertising pakety vysílané zařízeními uvnitř testovacího centra. Tyto pakety obsahují advertising adresy zařízení na základě kterých lze určit přítomnost zařízení v okolí snifferu. Zachytávání advertising paketů výrazně usnadňuje a zrychluje proces zachytávání, protože není potřeba projít procesem párování zařízení.

Pro zkoumání efektivnosti snímání a zachytávání BLE paketů byl vybrán nRF52840 sniffer dongle, který je vidět na obrázku 13. Jedná se o nástroj, pomocí kterého lze relativně jednoduše zachytit bezdrátovou BLE komunikaci procházející v okolí snifferu. Jeho hardwarové vybavení a relativně nízká cena představují omezení v podobě snímání pouze 1 kanálu současně. To však není překážka, jelikož důvodem zachytávání je zjistit, zda se v prostorech testovacího centra pohybuje nějaké zařízení, které vysílá Bluetooth signál. Na základě povahy testovacího centra se budou zařízení v těchto prostorách vyskytovat i v řádu desítek minut. Časová frekvence snímání paketů je však natolik vysoká, že pakety ze zařízení dříve nebo později v rámci několika sekund stejně zachytíme.

Pro interpretaci záchytu paketů byla vybrána open-source aplikace Wireshark, která je velmi flexibilní a nabízí velké množství funkcí ke zpracování dat, v tomto případě paketů.

4.2 Instalace

Pro zachytávání bezdrátové komunikace byla použita aplikace Wireshark ve verzi 4.2.2, která je univerzální, protože je open-source a zároveň funguje na většině operačních systémů. Pro zprovoznění záchytu paketů pomocí externího nRF52840 dongle snifferu bylo nutné do aplikace Wireshark nainstalovat potřebné rozšíření, protože aplikace umožňuje ve výchozím nastavení záchyt pouze z interních rozhraní počítače. Zároveň bylo nutné nainstalovat profil do aplikace Wireshark pro čitelnou interpretaci dat.

Pro veškerou instalaci v dalších kapitolách je potřeba mít administrátorská oprávnění k počítači na kterém je instalace prováděna.

Veškeré soubory níže zmíněné, které byly použity k instalaci jsou dostupné v příloze A. Stažení použitých aplikací vždy vyžaduje aktuální verzi a jsou dostupné ke stažení z webových stránek.

4.2.1 Instalace aplikace Wireshark

Aplikace Wireshark je vždy v aktuální verzi ke stažení zdarma dostupná z webové stránky https://www.wireshark.org/download.html, kde je možné stáhnout aplikaci k instalaci na různé operační systémy. Následující popis instalace aplikace byl proveden na operačním systému Windows 11 Pro verze 23h2 (build 22631.3007) 64bitové architektury.

Po stažení instalačního balíčku pro systém Windows byl spuštěn stažený .exe instalační soubor. Aplikace Wireshark byla nainstalována ve výchozím nastavení s dodatečnou instalací USBcap rozšíření, jehož instalace není nutná, avšak umožní rozšířenější práci s externími zařízeními, která používají USB rozhraní jako je například zmíněný nRF52840 sniffer. Toto rozšíření je součástí instalace aplikace Wireshark jako zaškrtávací možnost.

4.2.2 Instalace aplikace nRF Connect Programmer

Dále bylo potřeba stažení aplikace nRF Connect for Desktop z webové stránky https://www.nordicsemi.com/Products/Development-tools/nRF-Connect-for-Desktop/Download#infotabs. Aplikace nRF Connect obsahuje odkazy na stažení balíčků aplikací, které jsou využity v rámci různých funkcí vývojových sad od společnosti Nordic Semiconductor.

Pomocí menu v aplikaci nRF Connect for Desktop byla stažena aplikace Programmer, pomocí které byl nRF52840 sniffer dongle naprogramován, aby bylo možné v aplikaci Wireshark spustit zachytávání za pomoci tohoto snifferu a správně zobrazit pakety, které zachytil.

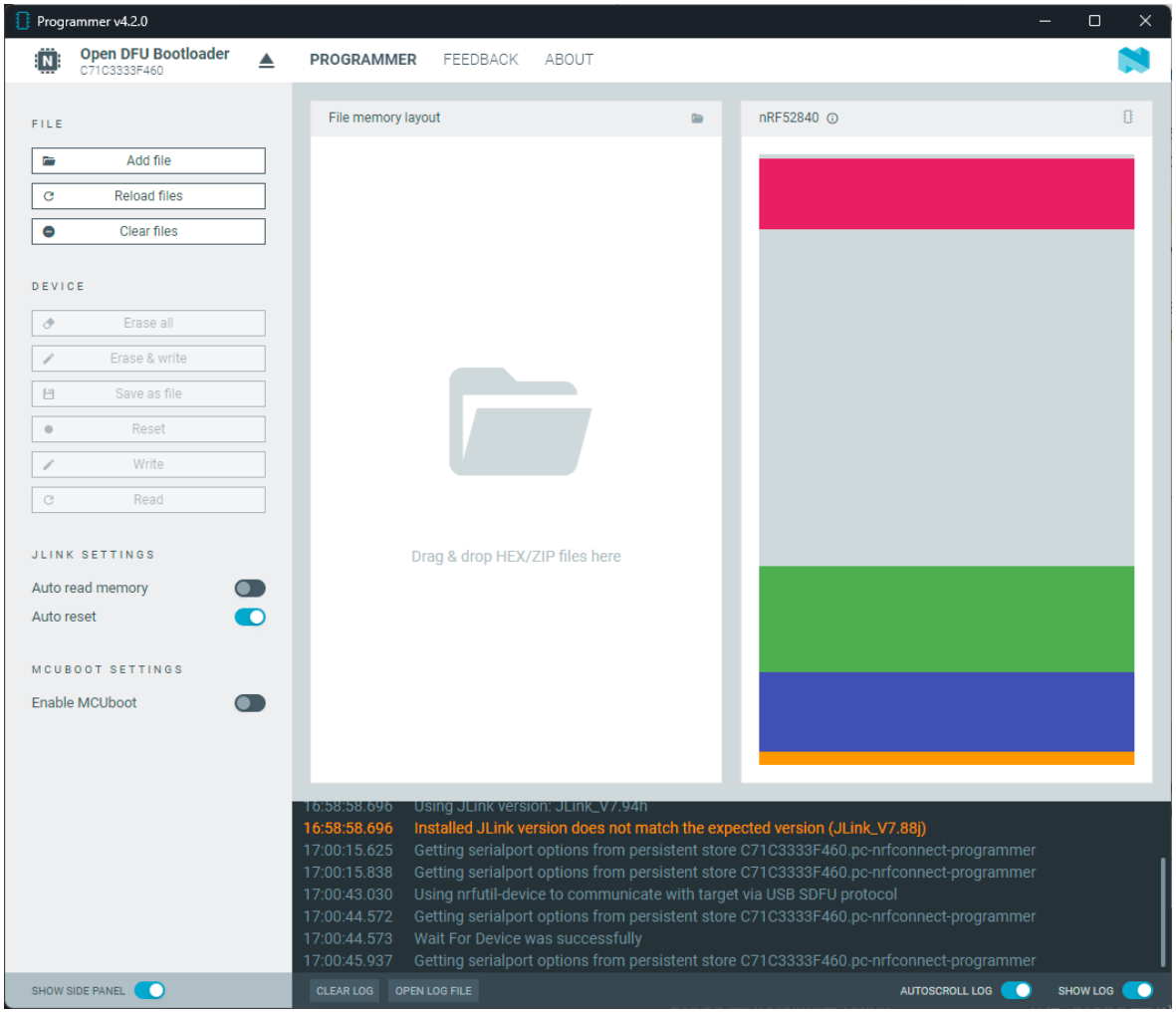
4.2.3 **Programování nRF52840 snifferu**

Programování snifferu proběhlo za pomoci souborů ze stránky výrobce https://www.nordicsemi.com/Products/Development-tools/nrf-sniffer-for-bluetooth-le/download#infotabs které byly po stažení extrahovány do samostatné složky. Na tuto složku se bude v následujících kapitolách odkazovat ještě několikrát, a protože její název je „nrf_sniffer_for_bluetooth_le_4.1.1“ budeme ji nazývat *složka A* v rámci instalace rozšíření. Tato složka se kterou byla provedena konfigurace je také součástí přílohy A.

Ve *složce A* je v podsložce *hex* zahrnutý firmware potřebný k požadovanému fungování nRF52840 snifferu s aplikací Wireshark. Zároveň se v této *složce A* nachází konfigurační soubory a profily, které umožní aplikaci Wireshark použít nRF52840 sniffer jako externí rozhraní a přehledně interpretovat jeho výstup.

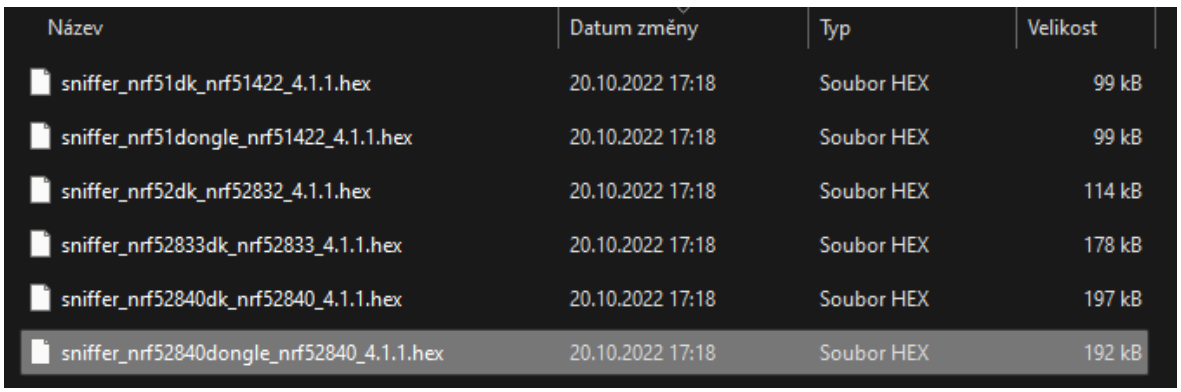
Prvně bylo potřeba otevřít aplikaci Programmer skrze aplikaci nRF Connect for Desktop, připojit nRF52840 sniffer k počítači pomocí rozhraní USB a zvolit ho v levém horním rohu aplikace Programmer jako aktuální zařízení.

Obrázek 16 - Prostředí aplikace nRF Connect Programmer



Do pole „File memory layout“ bylo nutné ze složky od výrobce vložit správný firmware ze složky *hex*. Jelikož se v našem případě jedná o nRF52840 dongle sniffer byl vybrán odpovídající firmware s názvem *sniffer_nrf52840dongle_nrdf52840_4.1.1.hex*.

Obrázek 17 - Firmware snifferu

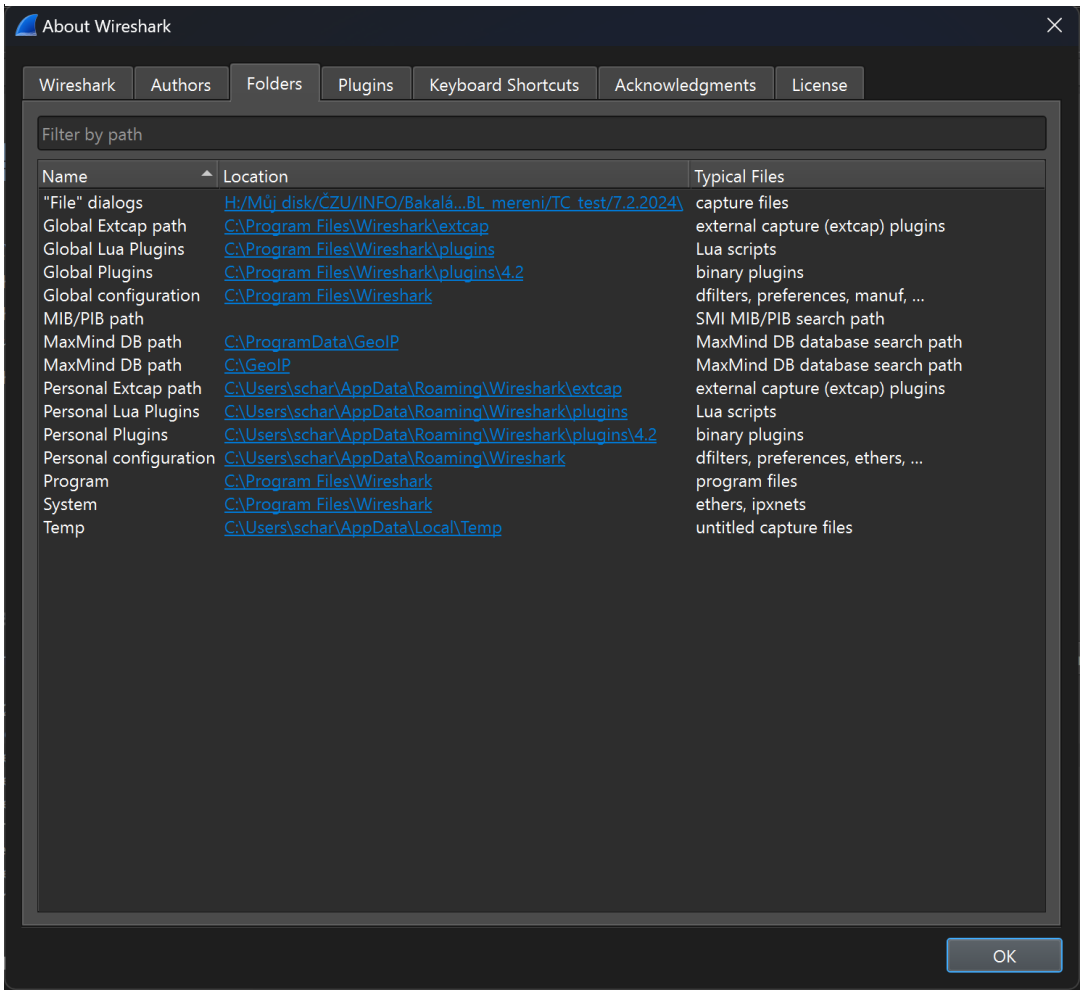


4.2.4 Instalace externího rozhraní do aplikace Wireshark

Abychom mohli nRF52840 sniffer používat jako externí rozhraní na záchyt paketů v aplikaci Wireshark, bylo nutné nainstalovat potřebné soubory ze *složky A*.

Soubory v podsložce *extcap* bylo nutné přesunout do globálního nastavení externích rozhraní aplikace Wireshark. K adresářové cestě tohoto nastavení se dostaneme po otevření aplikace Wireshark následující cestou: Help -> About Wireshark -> Folders.

Obrázek 18 - Kontextové menu aplikace Wireshark s adresářovými cestami k nastavení



Zde byla dvojitým kliknutím otevřena cesta s názvem *Global Extcap Path* k adresáři *C:\Program Files\Wireshark\extcap*, která otevřela složku se soubory globálního nastavení externích rozhraní aplikace Wireshark v Průzkumníkovi souborů. Do této složky byly zkopírovány veškeré soubory ze složky *extcap*.

4.2.5 **Instalace požadavků pomocí příkazového řádku**

Dalším krokem byla instalace požadavků ze složky *extcap* napsaných v Pythonu. Na to byl použit pip (systém správy balíčků napsaných v Pythonu) v příkazové řádce spuštěné pod administrátorským oprávněním. Nejprve bylo potřeba přepnout aktuální adresář v souborovém systému do požadovaného *extcap* adresáře pomocí příkazu *cd C:\Program Files\Wireshark\extcap.*

Následujícím krokem bylo spustit a nainstalovat soubor *requirements.txt* do *extcap* adresáře aplikace Wireshark protože nebyl napsán jako spustitelný .bat soubor. To bylo provedeno pomocí příkazu *pip install -r requirements.txt*.

Obrázek 19 - Instalace požadavků

```
C:\Program Files\Wireshark\extcap>pip install -r requirements.txt
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: pyserial>=3.5 in c:\users\schar\appdata\local\packages\pythonsoftwarefoundation.python.3.
12_qbz5n2kfra8p0\localcache\local-packages\python312\site-packages (from -r requirements.txt (line 1)) (3.5)
Requirement already satisfied: psutil in c:\users\schar\appdata\local\packages\pythonsoftwarefoundation.python.3.12_qbz5
n2kfra8p0\localcache\local-packages\python312\site-packages (from -r requirements.txt (line 2)) (5.9.8)

C:\Program Files\Wireshark\extcap>
```

Na obrázku výše vidíme, že byl tento krok v minulosti již proveden správně, a tedy výstup bude u první instalace vypadat jinak. Avšak pokud se příkaz neprovedl, tak z důvodu absence systému správy balíčků pro Python a bylo nutné ho doinstalovat a poté znovu opakovat tento krok.

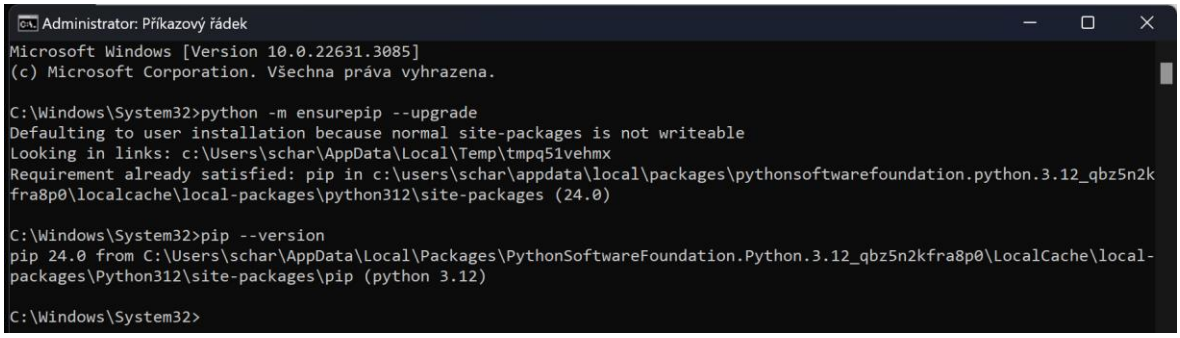
Pro kontrolu správné instalace se provede v příkazovém řádku v adresáři *C:\Program Files\Wireshark\extcap* příkaz: *nrf_sniffer_ble.bat –extcap-interfaces* a pokud výstup nebude obsahovat chybový kód nebo error zprávu, instalace proběhla úspěšně.

4.2.6 **Instalace systému správy balíků pro Python**

Pokud se stalo, že na operačním systému Windows v předchozí kapitole nebyl nalezen systém správy balíků pro Python, bylo potřeba ho doinstalovat. Nejjednodušším řešením bylo doinstalovat Python do Windows prostředí z aplikace Microsoft store.

V příkazové řádce pod administrátorským oprávněním bylo pak příkazem *python -m ensurepip –upgrade* zajištěno, že je Python nainstalován v aktuální verzi.

Obrázek 20 - Úspěšná instalace správy balíků pro Python



Pokud tento postup nefunguje, lze doinstalovat tento systém i skrze Microsoft Store aplikaci. Příkazem *pip --version* bylo v příkazové řádce ověřeno, že je na systému nainstalovaný systém správy balíků pro Python a v jaké verzi.

4.2.7 **Instalace profilu**

V této části byl ze složky A nainstalován profil, který umožňuje správné zobrazení a kategorizaci BLE advertising paketů. K dosažení instalace profilu bylo potřeba přejít do konfigurační složky Wiresharku. K přesné cestě adresáře, kam je potřeba nainstalovat profil se dostaneme přímo z aplikace Wireshark pomocí tlačítek: Help -> About Wireshark -> Folders.

Zde pak můžeme vidět cesty k různým adresářům. V tento moment nás zajímala pouze cesta *Global configuration* anebo *Personal configuration*. Rozdíl mezi nimi je, že pokud bychom nainstalovali profil do Global configuration, BLE pakety by se pak správně zobrazovaly všem účtům, které by spustili Wireshark a zobrazili BLE zachycené pakety. V reálném prostředí tedy záleží na účelu použití. V tomto případě byl profil nainstalován do adresářové cesty *C:\Program Files\Wireshark* s názvem *Global configuration*.

Samotná instalace proběhla pouze v podobě přesunutí složky *Profile_nRF_Sniffer_Bluetooth_LE*, která obsahuje přednastavený nakonfigurovaný profil ze *složky A* do otevřené adresářové cesty *C:\Program Files\Wireshark* globálního konfiguračního profilu aplikace Wireshark.

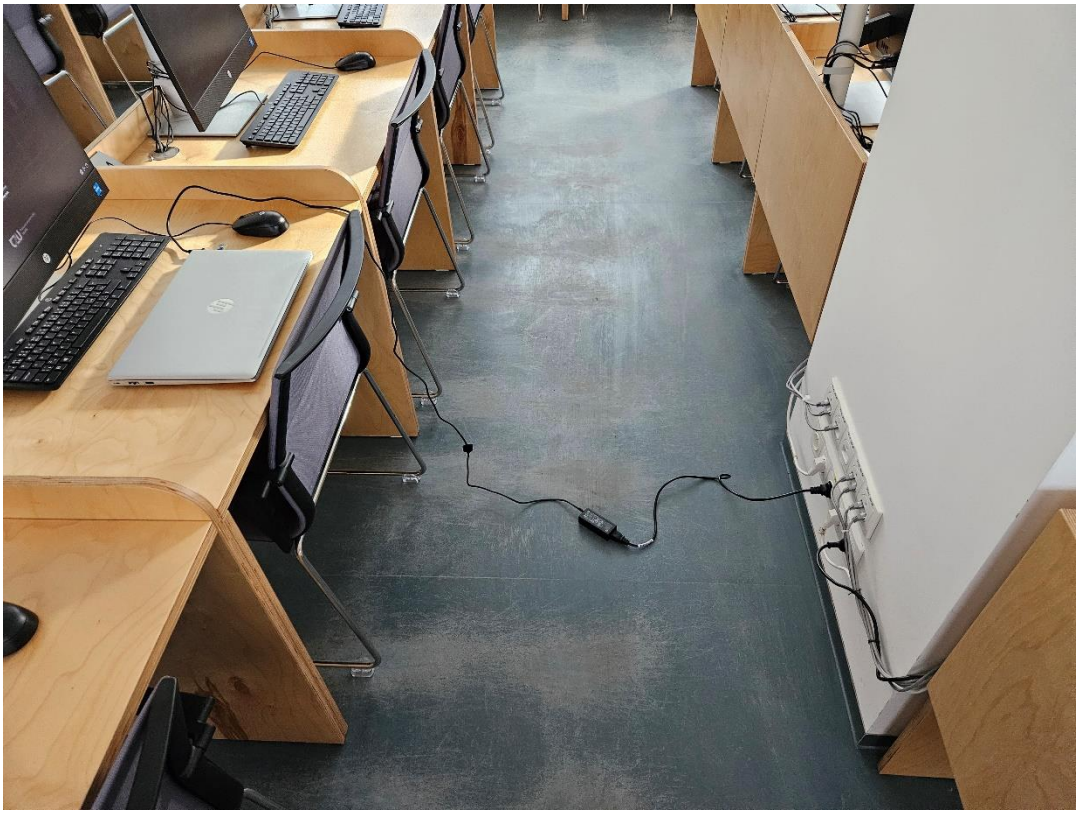
4.3 Zachytávání paketů v testovacím centru

V této části práce zkoumání použití a efektivity zachytávání BLE paketů bylo provedeno testovací měření v testovacím centru PEF. Testovací měření proběhlo dva dny s rozestupem sedm dní vždy po dobu 2 hodin. Delší zachytávání by vyprodukovalo až moc velká data a aktuální výsledky postačují na stanovení zhodnocení efektivity záchytu.

První měření započalo 7.2.2024 se začátkem kolem 11 hodiny dopolední při plně otevřeném provozu testovacího centra. Druhé měření započalo 14.2.2024 v podobném čase s rozdílem, že bylo testovací centrum kompletně uzavřeno pro údržbu a aktualizace.

Testovací měření proběhlo při stejných podmínkách v oba dny. Na stůl č. 35 uprostřed hlavní místnosti s počítači byl položen notebook HP ProBook 450 G10, na kterém byla předtím provedena instalace aplikace Wireshark, externího rozhraní a profilu pro správnou interpretaci zachycených paketů za pomoci nRF52840 sniffer dongle zařízení. Notebook byl nastaven tak, aby běžel bez přerušení (tj. přechod do režimu spánku po určité době) a aby nepřešel do režimu spánku po zavření víka. Zároveň byl počítač zamčený, aby nebylo možné cizím zásahem přerušit měření. Notebook byl také po celou dobu měření připojený ke zdroji elektrické energie, aby se předešlo vybití baterie, a tak i přerušení měření. Okolo počítače byl vyhrazen prostor zhruba 10 cm aby se předešlo manipulaci nebo rušení signálu. Počítač č. 35 byl po tuto dobu vyřazen z provozu pro účely psaní testu, aby mohlo nerušeně proběhnout testovací měření.

Obrázek 21 - Testovací měření v testovacím centru

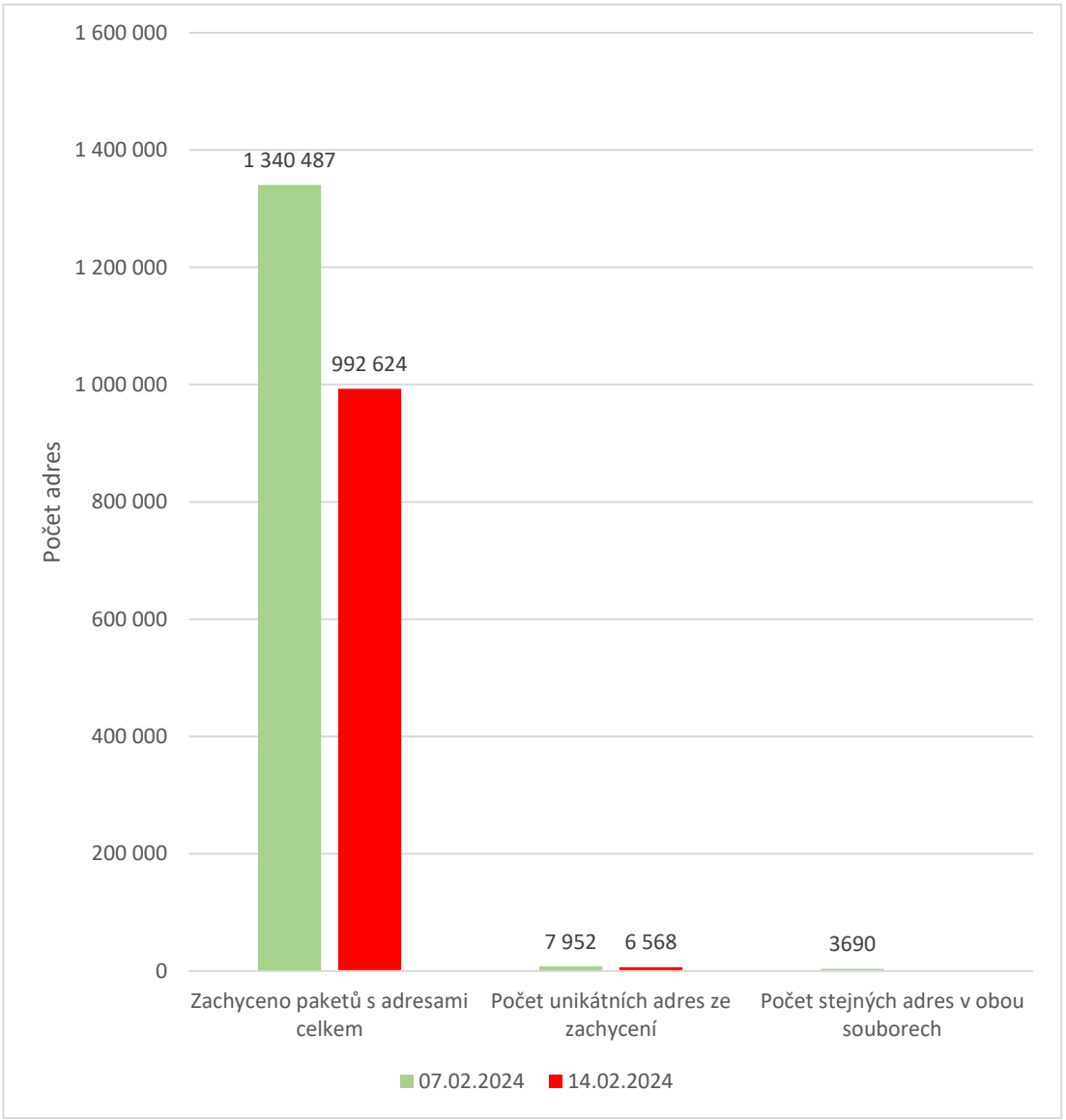


Obrázek 22 - Testovací měření v testovacím centru

Data do grafu byla získána z měření pomocí skriptu *unikatni_a_sdilene_adresy_TC_test.py*, který je dostupný v příloze A. Skript byl napsán v jazyku Python a k jeho správnému fungování bylo třeba doinstalovat knihovnu pyshark do prostředí Windows. Nejjednodušším způsobem je otevřít příkazovou řádku jako administrátor a doinstalovat pyshark pomocí příkazu *pip install pyshark*.

Z testování dne 7.2.2024 kdy bylo testovací centrum otevřené bylo zachyceno 1 340 487 paketů celkem, z toho bylo 7 952 unikátních adres, které se neopakovaly za celou dobu měření. Z druhého testování dne 14.2.2024 kdy bylo testovací centrum kompletně uzavřené pro údržbu bylo zachyceno 992 624 paketů celkem, z toho bylo 6 568 unikátních adres, které se neopakovaly.

Graf 1 - Výsledky zachytávání v testovacím centru PEF



Mezi měřeními bylo také zjištěno 3 690 adres, které byly zachyceny v okolí snifferu v průběhu obou testů zároveň. Tedy 3 690 adres zařízení, které se nacházely v testovacím centru a jeho okolí nezměněné.

Při pohledu na data v grafu je zřejmé, že při zavřeném provozu testovacího centra bylo paketů zachyceno méně avšak stále dost oproti měření, kdy bylo testovací centrum otevřené. Pokud bylo testovací centrum zavřené, zachycených paketů by mělo být výrazně méně, skoro až žádné. To indikuje, že sniffer zachytával i zařízení z okolí testovacího centra (např. pokud někdo se zařízením vysílajícím Bluetooth LE signál prošel v blízkosti testovacího centra). Zároveň také výsledky mohly být ovlivněny statickými vysílači s dlouhým dosahem.

Jaká zařízení jsme zachytili jsou a budou z těchto dat pouze spekulace, protože nedokážeme na základě bezpečnostní povahy Bluetooth LE a pomocí snifferu zjistit o jaká konkrétní zařízení se jednalo, kde se přesně nacházela a komu patří.

4.4 Rušení zachytávání signálu v testovacím centru

Na základě konzultace s Ing. Františkem Jeřábkem z Oddělení rozvoje rektorátu ČZU bylo stanoveno, že se ve sloupu uprostřed místnosti v testovacím centru nenachází žádné objemné kovové části, které by potencionálně narušovaly zachytávání signálu. V příloze B je přiložena stavební dokumentace rektorátní budovy.

Zároveň se v prostoru testovacího centra nenachází žádné objekty, které by významně rušily přenos Bluetooth signálu. Rušení signálu tedy není faktor, který by ovlivňoval výsledky tohoto zachytávání.

4.5 Určení konstantnosti adres

Po dobu jednoho dne proběhlo periodické snímání paketů s cílem určit konstantnost adres zařízení v okolí v průběhu času. Měření probíhalo za podobných podmínek jako při testování zachytávání v testovacím centru s rozdílem použitého zařízení k provozu měření, velikosti místnosti ve které se zařízení nacházelo a času po který měření probíhalo. K provozu měření do místnosti o rozloze 12.311m^2 byl použit notebook Acer ConceptD CN715-72P.

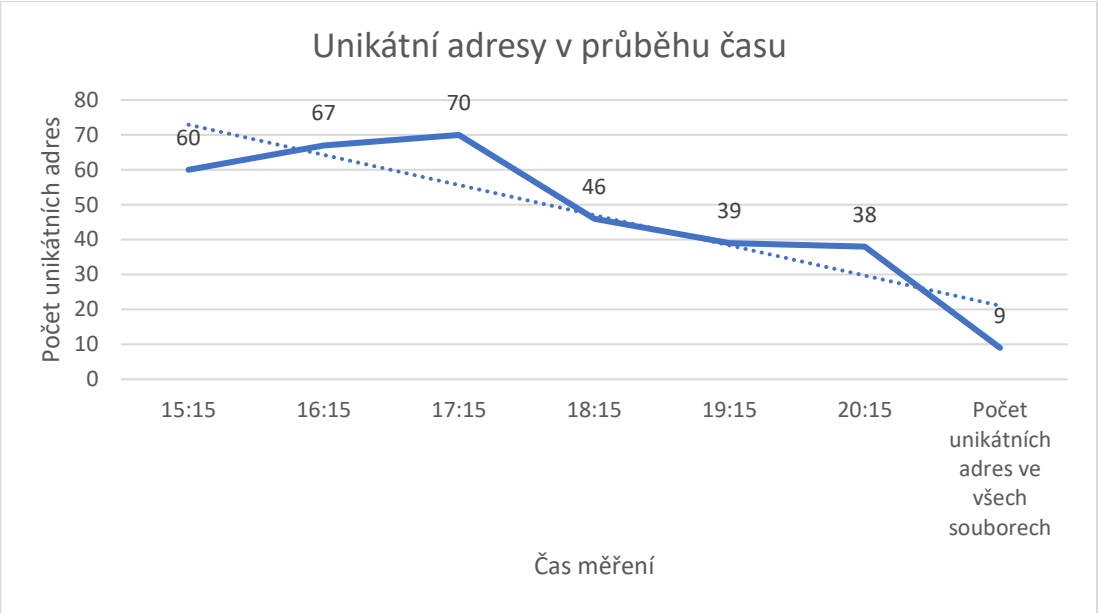
Notebook byl položen na stůl s minimálně 10 cm prostorem okolo snifferu aby se omezilo možné rušení signálu. Pro účely simulace zachycení a zkreslení byl vedle snifferu ve

vzdálenosti 5 cm položen telefon Samsung Galaxy S23. V místnosti se po celou dobu měření pohybovaly 3 zařízení se zapnutým Bluetooth.

Měření proběhlo 24.2.2024 v časovém úseku mezi 15:15 až 20:15 každou hodinu po dobu cca 30 vteřin.

Výpočet dat ze zachytávání pro interpretaci byl vytvořen pomocí skriptu *urceni_konstantnosti_adres_test_skritp.py* v příloze C.

Graf 2 - Výsledky testu konstantnosti adres



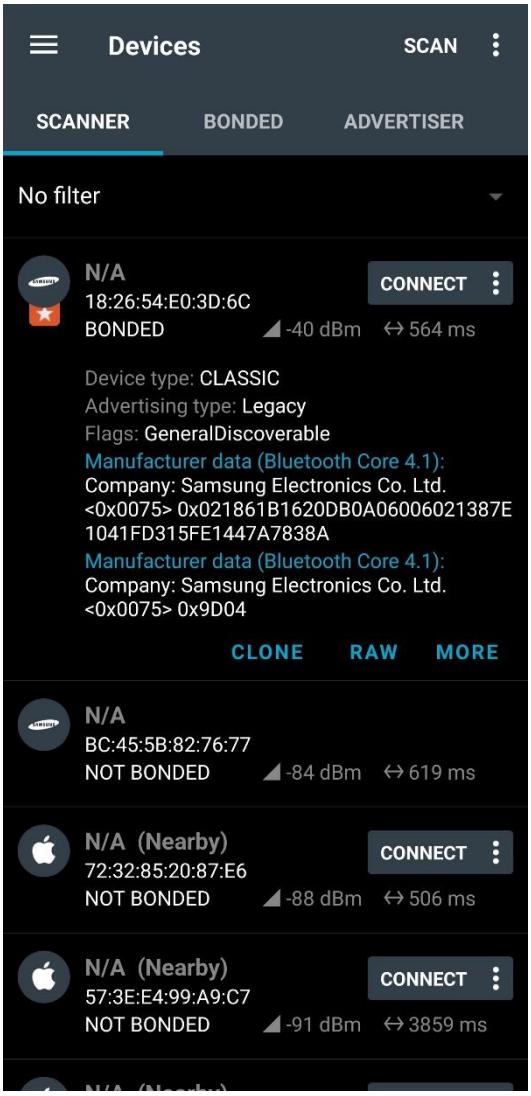
Na grafu založeného na výsledcích měření můžeme vidět klesající trend počtu nalezených unikátních adres. Z logiky zachytávání je to správně, čím více adres zachytíme na začátku měření, tím méně by jich mělo být unikátních ke konci měření. Avšak na úplném konci grafu vidíme údaj, který značí počet unikátních adres nacházejících se ve všech časech měření. Pokud bychom zachytávali identické adresy, které se v okolí vyskytují stále, dávalo by smysl, že tento údaj bude součtem všech počtů unikátních adres z celé doby měření, tedy 320. Na základě skriptu, ve kterém se počítaly i pouze nově zachycené unikátní adresy za celou dobu měření vyšlo, že těchto adres bylo celkem 200.

To nám značí, že 120 adres si zařízení v okolí změnilo v průběhu testu anebo byly zachyceny adresy zařízení, které už se dále nevyskytovali v dalších měřeních (tj. zařízení v kolem projíždějících vozidlech či v kapsách kolemjdoucích). Pouze 9 zařízení se nacházelo v okolí snifferu se statickými nezměněnými adresami. Pokud bychom tedy vyloučili těchto 9 adres zařízení z výsledků měření, zůstalo by nám 191 unikátních adres, které jsme zachytili a

označovaly by zařízení, která buď své adresy změnila v průběhu měření nebo se v okolí snifferu vyskytovala pouze v jednu dobu měření. Zároveň bylo zjištěno, že mezi těmito 9 adresami, které se po celou dobu nezměnily byla jedna televize značky Samsung. S jistotou nemůžeme takové chování konstatovat pro všechny televize, ale jak z pozorování vyplývá z tohoto testu, tak televize nemění svou adresu často jako jiná zařízení, protože jsou staticky umístěné v prostoru a nemají potřebu časté změny adresy kvůli bezpečnosti. Taková teorie by však vyžadovala další test.

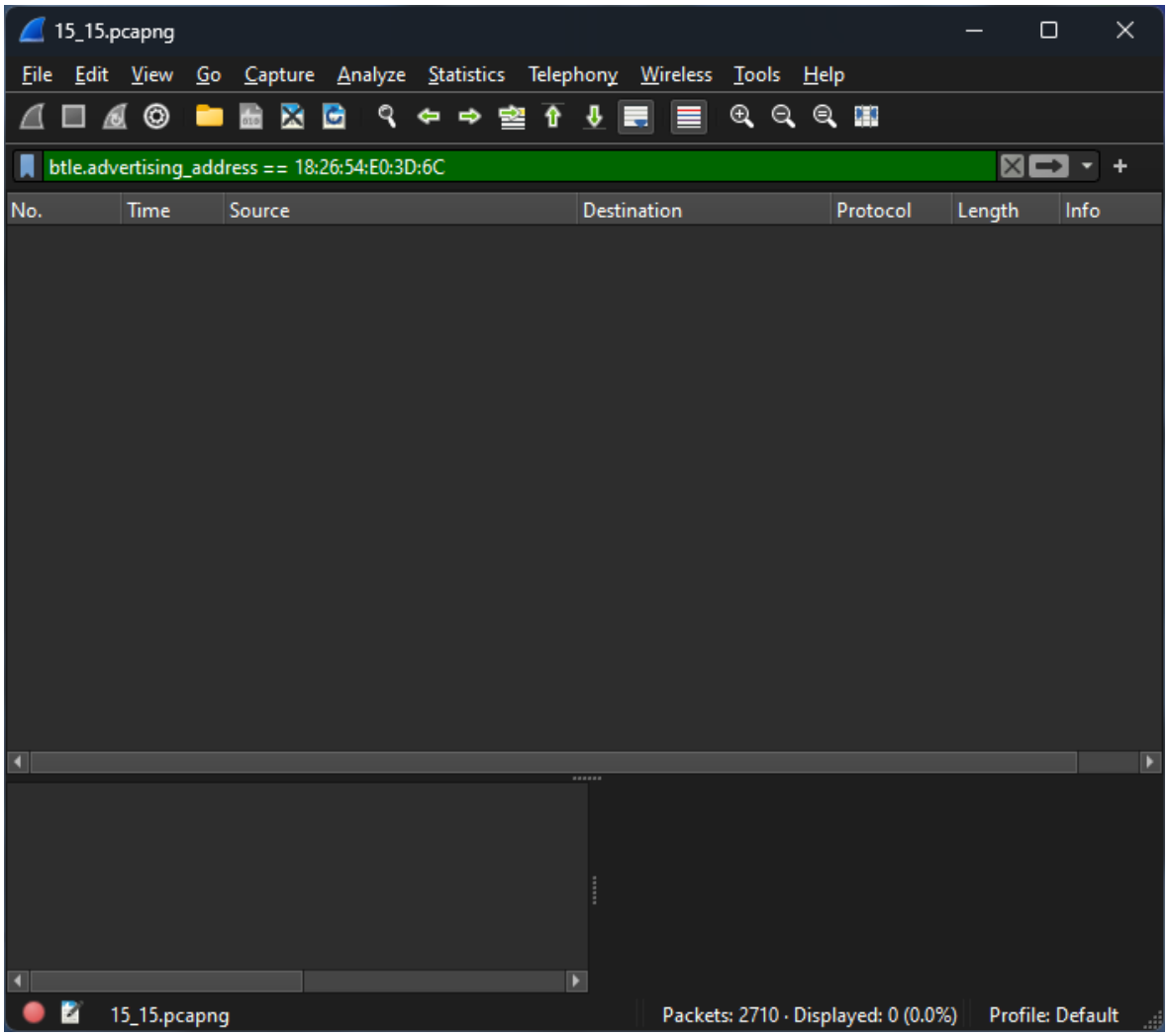
O několik dní později po provedení testu bylo za pomocí mobilní aplikace nRF Connect a telefonu Oneplus 7 Pro určena adresa zařízení Samsung Galaxy S23, které bylo po dobu měření položeno vedle snifferu. Adresa zařízení S23 byla za pomoci aplikace nRF Connect stanovena na 18:26:54:E0:3D:6C.

Obrázek 23 - Stanovení adresy zařízení pomocí nRF Connect



Za pomoci filtru *btle.advertising_address == 18:26:54:E0:3D:6C* bylo z výsledků měření v příloze 3 zjištěno, že se v žádném z výsledků tato adresa nenachází a tím pádem můžeme konstatovat a potvrdit, že si zařízení své adresy opravdu mění. Na obrázku 25 je vidět, že z celkových 2710 zachycených paketů ani jeden neobsahuje požadovanou advertising adresu.

Obrázek 24 - Filtrování adres z měření konstantnosti adres



5 Výsledky a diskuse

5.1 Omezení

Z důvodu vysoké ceny nebylo možné prozkoumat funkčnost dedikovaných BLE snifferů, které nabízí kompletní softwarové podpory a různé funkce pro trasování zařízení. Pro reálné použití dedikovaného BLE snifferu je cena také velmi vysoká a vyžaduje velmi důkladné zvážení nasazení, přestože by mohly fungovat mnohem lépe. Pokud by se vytvořila správná konfigurace softwaru od dodavatele, bylo by teoreticky možné zachytávat zařízení pohybující se v prostorách testovacího centra efektivněji než za pomoci snifferu založeného na vývojářské sadě. Jestli je dedikovaný sniffer tou správnou odpovědí na optimální technologii pro skenování Bluetooth signálů uvnitř testovacího centra nelze na základě této práce s jistotou určit ale pouze předpokládat.

Izolování testovacího centra od signálů příchozích mimo testovací centrum bylo pro toto zkoumání nemožné. Místo izolování testovacího centra by se dal omezit do jisté míry vliv okolních signálů pomocí směrové antény přijímače snifferu, ty jsou ale dostupné pouze pro dedikované sniffery. Toto omezení výrazně ovlivnilo výsledky zkoumání a je nutné ho brát v potaz při dalším zkoumání.

Nelze také spolehlivě určit například počet lidí, kteří se nachází okolo snifferu, protože bez předchozího zjišťování nevíme, kolik má každý člověk u sebe zařízení, která vysílají Bluetooth signál a zároveň nám to částečně znemožňuje změna adres. Nevíme, jak často si každé zařízení mění advertising adresu.

Na základě výsledků měření a chování adres v zachycených paketech z testovacího centra nebylo v této práci provedeno stanovení polohy zařízení v testovacím centru. K takovému určování by bylo potřeba použití softwaru, který je například součástí dedikovaných BLE snifferů. Účelem této práce nebylo vyvinout takový software, který by naměřená data dokázal zpracovat a určit polohu zařízení.

5.2 Výsledky z měření

Z měření, kdy bylo testovací centrum zavřené vyplývá, že signály mimo testovací centrum narušily výsledky měření. Pro stanovení polohy zařízení je potřeba nejprve

najít způsob, jak eliminovat nebo omezit vliv signálů příchozích mimo testovací centrum na zachytávání.

V aktuální podobě bychom ze získaných souborů dokázali pouze hrubým odhadem určit polohu zařízení bez určení směru, ze kterého signál přišel. Například bychom byli schopní říct, že na základě síly signálu přijatého paketu se zařízení nachází zhruba 1 metr od našeho snifferu. Spolehlivost takového odhadu by vyžadovala další testování.

5.3 Konstantnost adres

Na základě výsledku testu z kapitoly 4.5 bylo zjištěno, že zařízení si mění svou advertising adresu. I tento test byl narušen zachytáváním adres z většího okolí, čímž byly výsledky zachycených paketů ovlivněny.

Hledání intervalu pro všechna zařízení, ve kterém si mění svou advertising adresu by bylo zbytečné, protože u každého zařízení nastavuje podmínky a velikost takového intervalu výrobce. Nalezení takového intervalu s dostačující spolehlivostí by vyžadovalo mnohem více času a proto v této práci nebylo hledání tohoto intervalu uskutečněno. Na základě tohoto testu můžeme konstatovat, že retrospektivní trasování zařízení na základě jeho adresy by bylo do určité míry zbytečné. Pouze aktuální trasování v reálném čase by bylo do jisté míry relevantní.

6 Závěr

Bluetooth LE je nejčastěji používaná technologie při trasování zařízení uvnitř budov. Její charakteristika a funkce nativně umožňují určení přítomnosti a směru jiných zařízení v okolním prostoru.

Povaha testovacího centra neumožňuje plné nasazení jednoho jednoduchého BLE snifferu založeného na vývojářské sadě. Testovací centrum není aktuálně izolováno od signálů příchozích mimo prostor testovacího centra, a proto jimi bude jakékoliv zachytávání Bluetooth i jiných signálů ovlivněno.

V aktuální podobě by sniffer BLE založený na vývojářské sadě posloužil pouze k vytváření velmi objemných záznamových souborů, ze kterých by se za pomoci správných příkazů a skriptů dala zjišťovat hrubým odhadem přítomnost zařízení. Toto trasování by však bylo relativně nepřesné a nedala by se určit naprosto přesná poloha zařízení.

Pro nasazení BLE snifferu založeného na vývojářské sadě do testovacího centra by bylo potřeba vyvinout program, který bude ze snímání 3-4 snifferů umístěných po obvodu stěn testovacího centra dopočítávat vzdálenost na základě RSSI (přijaté síly signálu) v paketech. Efektivita takového návrhu však vyžaduje další zkoumání.

Zároveň povaha oznamování přítomnosti na zařízeních je do jisté míry ošetřena proměnlivými advertising adresami v různých náhodných intervalech v závislosti na výrobci zařízení, a proto se bez předchozího zkoumání nedá s jistotou určit, zda se jedná o jedno a to samé zařízení v různých časových úsecích.

Technologie Bluetooth LE je pro takovéto využití velmi zajímavá a vyspělá ale vyžaduje další zkoumání za pomoci jiných prostředků jako jsou například dedikované BLE sniffery a směrové antény.

Použití samotného snifferu založeného na vývojářské sadě, pomocí kterého byly dosaženy výsledky v této práci by bylo možné, avšak ne ideální. Tento samotný sniffer v aktuální podobě potřebuje ke svému fungování počítač nebo notebook s operačním systémem. Nasazení takového zachytávání by posloužilo jako zajímavá komplementarita k detekčnímu rámu a produkovalo by data pro další zpracování.

7 Seznam použitých zdrojů

AFANEH, Mohammad, 2018. *Intro to bluetooth low energy: the easiest way to learn BLE: featuring Bluetooth 5 and an Intro to Bluetooth Mesh*. Fishers: Novel Bits. ISBN 978-1-79019-815-3.

AFANEH, Mohammad, 2022. BLE Sniffer Basics + Comparison Guide. *Novel Bits* [online] [vid. 2024-02-18]. Dostupné z: https://novelbits.io/bluetooth-low-energy-ble-sniffer-tutorial/

BISDIKIAN, C., 2001. An overview of the Bluetooth wireless technology. *IEEE Communications Magazine* [online]. **39**(12), 86–94. ISSN 1558-1896. Dostupné z: doi:10.1109/35.968817

BLUETOOTH®, c2023. Bluetooth Technology Overview. *Bluetooth® Technology Website* [online] [vid. 2023a-08-13]. Dostupné z: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/

BLUETOOTH®, c2023. Origin of the Name. *Bluetooth® Technology Website* [online] [vid. 2023b-08-13]. Dostupné z: https://www.bluetooth.com/about-us/bluetooth-origin/

ČERNÝ, Michal, 2015. *Zařízení v pásmu 2,4 GHz « RoboDoupě - web nejen o robotice* [online] [vid. 2023-08-12]. Dostupné z: https://robodoupe.cz/2015/zarizeni-v-pasmu-24-ghz/

ČESKÝ TELEKOMUNIKAČNÍ ÚŘAD, c2018. *Využívání vymezených rádiových kmitočtů | Český telekomunikační úřad* [online] [vid. 2023-08-12]. Dostupné z: https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu

FARAGHER, Ramsey a Robert HARLE, 2015. Location Fingerprinting With Bluetooth Low Energy Beacons. *IEEE Journal on Selected Areas in Communications* [online]. **33**(11), 2418–2428. ISSN 0733-8716. Dostupné z: doi:10.1109/JSAC.2015.2430281

GAO, Vincent, 2015. Proximity and RSSI. *Bluetooth® Technology Website* [online] [vid. 2024-03-06]. Dostupné z: https://www.bluetooth.com/blog/proximity-and-rssi/

GARMIN, 2023. *What is GPS? | Garmin* [online] [vid. 2023-08-13]. Dostupné z: https://www.garmin.com/en-US/aboutgps/

HEYDON, Robin, 2012. *Bluetooth low energy: the developer's handbook*. Upper Saddle River, NJ: Prentice Hall. ISBN 978-0-13-288836-3.

HURT, Avery Elizabeth, 2018. *How Bluetooth Works* [online]. New York, NY, UNITED STATES: Cavendish Square Publishing LLC [vid. 2024-02-29]. ISBN 978-1-5026-3739-0. Dostupné z: http://ebookcentral.proquest.com/lib/techlib-ebooks/detail.action?docID=5528779

CHANG, Kuor-Hsin, 2014. Bluetooth: A viable solution for IoT? [Industry Perspectives]. *IEEE Wireless Communications* [online]. **21**, 6–7. Dostupné z: doi:10.1109/MWC.2014.7000963

INTEL CORPORATION, 2012. USB 3.0 Radio Frequency Interference Impact on 2.4 GHz Wireless Devices | USB-IF. *USB* [online] [vid. 2023-08-12]. Dostupné z: https://www.usb.org/document-library/usb-30-radio-frequency-interference-impact-24-ghz-wireless-devices

KRAJSKÁ NEMOCNICE TOMÁŠE BATI, A.S., 2022. Voda je pro lidské tělo nesmírně důležitá • Krajská nemocnice T. Bati, a. s. *Krajská nemocnice Tomáše Bati* [online] [vid. 2023-10-16]. Dostupné z: https://www.kntb.cz/voda-je-pro-lidske-telo-nesmirne-dulezita

LEITH, Douglas J. a Stephen FARRELL, 2020. Coronavirus contact tracing: evaluating the potential of using bluetooth received signal strength for proximity detection. *ACM SIGCOMM Computer Communication Review* [online]. **50**(4), 66–74. ISSN 0146-4833. Dostupné z: doi:10.1145/3431832.3431840

LIEBESKIND, 2011. *English: Non-Overlapping Channels for 2.4 GHz WLAN (en)* [online]. 18. březen 2011. [vid. 2024-03-05]. Dostupné z: https://commons.wikimedia.org/wiki/File:NonOverlappingChannels2.4GHzWLAN-en.svg

NATIONAL COORDINATION OFFICE FOR SPACE-BASED POSITIONING, NAVIGATION, AND TIMING, 2014. *GPS.gov: Trilateration Exercise* [online] [vid. 2023-08-13]. Dostupné z: https://www.gps.gov/multimedia/tutorials/trilateration/

ROHM SEMICONDUCTOR, c2023. Modulation Methods | Electronics Basics | ROHM. *ROHM Semiconductor* [online] [vid. 2023-08-12]. Dostupné z: https://www.rohm.com/electronics-basics/wireless/modulation-methods

SILICON LABS, 2020. Adaptive Frequency Hopping - v2.13 - Bluetooth API Documentation Silicon Labs. *Silicon Labs* [online] [vid. 2023-08-12]. Dostupné z: https://docs.silabs.com/bluetooth/2.13/general/system-and-performance/adaptive-frequency-hopping#adaptive-frequency-hopping

SYMMETRY ELECTRONICS, 2023. What is Dual-Mode Bluetooth 5? | Symmetry Blog. *Symmetry Electronics* [online] [vid. 2023-10-20]. Dostupné z: https://www.symmetryelectronics.com/blog/what-is-dual-mode-bluetooth-5-symmetry-blog/

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam grafů

8.4 Seznam použitých zkratek

BLE – Bluetooth Low Energy

LE – Low Energy

PAN – Personal Area Network

RSSI – Received Signal Strength Intensity

GPS – Global Positioning system

GNSS – Global Navigational Satelite Systems

SM – Security Manager

CRC – Cyclic Redundancy Check

LESC – Low Energy Security Connections

ISO – International Organization for Standardization

OSI – Open Systems Interconnection

Přílohy

Příloha A

V této příloze se nachází soubory z testovacího zachytávání signálů, skripty pro výpočty podkladů ke grafům a soubory potřebné ke zprovoznění funkčnosti snifferu.

Příloha B

V této příloze se nachází naskenovaná stavební dokumentace rektorátní budovy ČZU.

Příloha C

V této příloze se nachází soubory a skript z testu určení konstantnosti adres.