VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2020 Bc. Martin Štrajt

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA BEZDRÁTOVÉ KOMUNIKACE POMOCÍ SOFTWAROVĚ DEFINOVANÉHO RÁDIA
WIRELESS COMMUNICATION ANALYSIS USING SOFTWARE DEFINED RADIO

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Martin Štrajt

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Jiří Pokorný

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**

Ústav telekomunikací

Student: Bc. Martin Štrajt ***ID:*** 186581

Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Analýza bezdrátové komunikace pomocí softwarově definovaného rádia

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce bude analýza komunikace bezdrátových technologií na standardech IEEE 802.11 b/g/n převážně na frekvencích 2,4 a 5 GHz. K zachycení komunikace bude nejprve zvolen vhodný HW, v začátcích bude uvažována jednoduchá bezdrátová karta, následně bude využito některé z dostupných softwarově definovaných rádií (SDR), např. LimeSDR mini, LimeSDR, BladeRF 2.0. K řízení HW bude sloužit příslušný SW, kde doporučeným nástroj bude GNU rádio. Komunikace bude zachycena na dvou místech v síti, na jednom rozhraní uvnitř sítě a na jednom mimo síť. Po zachycení zpráv budou oba typy komunikace porovnány a úkolem bude dokázat, že zachycené proudy sobě odpovídají. K zachycení budou použity vhodné nástroje, např. Wireshark, Aircrack-ng, LimeSuite, CubicSDR, GQRX nebo podobné. Výstupem diplomové práce bude sonda postavená na některém z dostupných SDR.

DOPORUČENÁ LITERATURA:

[1] WYGLINSKI, Alexander M., Don P. OROFINO, Matthew N. ETTUS a Thomas W. RONDEAU. Revolutionizing software defined radio: case studies in hardware, software, and education. IEEE Communications Magazine [online]. 2016, 54(1), 68-75 [cit. 2019-09-15]. DOI: 10.1109/MCOM.2016.7378428. ISSN 0163-6804. Dostupné z: http://ieeexplore.ieee.org/document/7378428/

[2] CHEN, Dong. A Survey of IEEE 802.11 Protocols: Comparison and Prospective. In: 2017 5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCE 2017). Atlantis Press, 2017.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 1.6.2020

Vedoucí práce: Ing. Jiří Pokorný

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Práce se zabývá využitím softwarově definovaného rádia jako sondy pro monitoring provozu bezdrátové komunikace podle standardu IEEE 802.11a/g. V teoretickém úvodu je představen koncept softwarově definovaného rádia jako hardwarového zařízení se softwarově programovatelnými obvody umožňující vysílat, či přijímat signály v teoreticky jakémkoliv kmitočtovém pásmu. Úvod dále obsahuje popis vybraných zařízení a protokolu IEEE 802.11 s jeho nejpoužívanějšími dodatky a využívanými modulacemi.
V první části praktické části práce je bezdrátová komunikace zachycena pomocí bezdrátové síťové karty v monitorovacím režimu. Zachycená komunikace byla dešifrována a tento dešifrovaný provoz byl srovnán s daty zachycenými sondou uvnitř sítě. Tyto výsledky pak sloužily jako srovnávací podklad pro zachytávání pomocí softwarově definovaného rádia. Těžištěm této práce je ověřit schopnosti softwarově definovaného rádia a jeho využití pro odposlech bezdrátové komunikace ve frekvenčním pásmu 2,4 GHz a 5 GHz. Snaha použít zde softwarově definované rádio vyplývá z možností rozšiřitelnosti a přizpůsobitelnosti, které bezdrátová karta kvůli pevně daným hardwarovým parametrům nemůže nabídnout. K zachytávání byly postupně využity zařízení LimeSDR mini, LimeSDR a bladeRF 2.0. Nejprve je popsána konfigurace operačního systému, instalace ovladačů a programů pro ovládání a práci s vybranými zařízeními. Po ověření funkčnosti softwarově definovaného rádia byl zprovozněn model dekodéru signálu s parametry standardu IEEE 802.11g zachyceného z rádiového spektra. Nakonec byly vedle sebe srovnány datové toky zachycené softwarově definovaným rádiem a bezdrátovou síťovou kartou. Výsledky ukázaly, že softwarově definované rádio v použité konfiguraci zachytává pouze zlomek z celkového objemu vyslaných rámců.

KLÍČOVÁ SLOVA

Analýza bezdrátového spektra, bladeRF, GNU Radio, GQRX, IEEE 802.11, LimeSDR, LimeSDR mini, Linux, SDR, Softwarově definované rádio, Sniffing, Ubuntu, Wireshark.

ABSTRACT

The work deals with the use of software-defined radio as a probe for monitoring the operation of wireless communication according to the IEEE 802.11a/g standard. In the theoretical introduction, the concept of software-defined radio as a hardware device with software programmable circuits enabling the transmission or reception of signals in theoretically any frequency band is introduced. The introduction also contains a description of selected devices and the IEEE 802.11 protocol with its most used additions and modulations.

In the first part of the practical part of the work, wireless communication is captured using a wireless network card in monitoring mode.

The intercepted communication was decrypted and this decrypted traffic was compared with the data captured by the probe within the network. These results then served as a comparative basis for software-defined radio capturing. The focus of this work is to verify the capabilities of software-defined radio and its use for sniffing wireless communication in the frequency band 2.4 GHz and 5 GHz. The attempt to use a software-defined radio here results from the scalability and adaptability that a wireless card cannot offer due to fixed hardware parameters.

LimeSDR mini, LimeSDR and bladeRF 2.0 devices were used for capture. First, the configuration of the operating system, the installation of drivers and programs for control and work with selected devices are described. After verifying the functionality of the software-defined radio, a model of a signal decoder with the parameters of the IEEE 802.11g standard captured from the radio spectrum was put into operation. Finally, the data streams captured by the software-defined radio and the wireless network card were compared side by side. The results showed that the software-defined radio in the used configuration captures only a part of the total volume of transmitted frames.

KEYWORDS

bladeRF, GNU Radio, GQRX, IEEE 802.11, LimeSDR, LimeSDR mini, Linux, SDR, Software defined radio, Sniffing, Ubuntu, Wireshark, Wireless spectrum analysis.

ŠTRAJT, Martin. *Analýza bezdrátové komunikace pomocí softwarově definovaného rádia*. Brno, 2020, 80 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Jiří Pokorný

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Analýza bezdrátové komunikace pomocí softwarově definovaného rádia“ jsem vypracoval samostatně pod vedením vedoucího diplomové 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 diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové 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

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Jiřímu Pokornému za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Díky inovacím v oblasti bezdrátových technologií je dnes bezdrátová komunikace stále více využívána. Pro uživatele je bezdrátové řešení v porovnání s tím drátovým často snadnější a dostupnější alternativou, díky tomu je jeho využití stále častější. Rozmach bezdrátových sítí dokládá také koncept Internetinternet věcí. Ten si klade za cíl propojit miliardy zařízení do jedné globální sítě. Tato zařízení jsou často jen malé senzory, například ve výrobní hale, nebo v květináči, které jsou připojeny nejčastěji bezdrátově [1]. S tímto záměrem přicházejí nové bezdrátové technologie typu LPWAN (Low Power Wide Area Network), které umožňují bezdrátovou komunikaci s velmi nízkými napájecími nároky a velikým dosahem [2]. Při tak velkém počtu zařízení sdílejících stejné bezdrátové médium může docházet k těžko identifikovatelným problémům a bezpečnostním hrozbám. Tyto problémy by mohly být odhaleny analýzou bezdrátových sítí, například s využitím softwarově definovaného rádia (SDR) [3].

SDR je hardwarové zařízení umožňující softwarově naladit programovatelné obvody tak, aby bylo schopné vysílat, či přijímat signály v podporovaném rádiovém spektru. O ovládání a modulaci se stará software a hardware připojeného počítače. Jinými slovy lze teoreticky SDR využít pro komunikaci jakýmkoliv bezdrátovým standardem. Stačí jen použít zařízení podporující dané frekvenční spektrum a softwarově implementovat standard.

S příchodem cenově dostupných zařízení již není SDR doménou výzkumných center a armádních laboratoří. SDR je dnes možné pořídit za jednotky tisíc korun. SDR si svou všestranností získalo velkou komunitu lidí vytvářejících nespočet implementací. Příkladem neomezených možnosti využití je projekt zachytávající údaje o poloze z leteckých odpovídačů [4], další možností je vytvořit LTE síť [5], sledovat pozemní televizní vysílání [6], poslouchat rádio, stahovat satelitní snímky počasí [7], nebo komunikovat standardem IEEE 802.11.

Použít SDR pro komunikování standardem IEEE 802.11 je i cílem této práce. Bezdrátová sonda schopná detekovat provoz přenášený standardem IEEE 802.11 by otevřela možnosti pro analyzování problémů v bezdrátových sítích, zkoumání funkcí protokolu, jeho snadnou modifikaci, nebo odhalení útoků na síť jako například spoofing (záměna odesílatele zprávy). Vzhledem k šířce pásma SDR, která u většiny zařízení dosahuje řádu desítek MHz a frekvenčního rozsahu v oblasti desítek MHz až jednotek GHz, by měl být uskutečnitelný záměr odposlouchávat komunikaci splňující standard IEEE 802.11b/g/n, který využívá frekvence 2,4 GHz a 5 GHz s šířkou pásma 20 MHz.

1 Teoretický úvod

V této části práce budou obecně popsány protokoly a zařízení, které budou v následujících kapitolách využity k monitorování bezdrátové komunikace.

1.1 Softwarově definované rádio

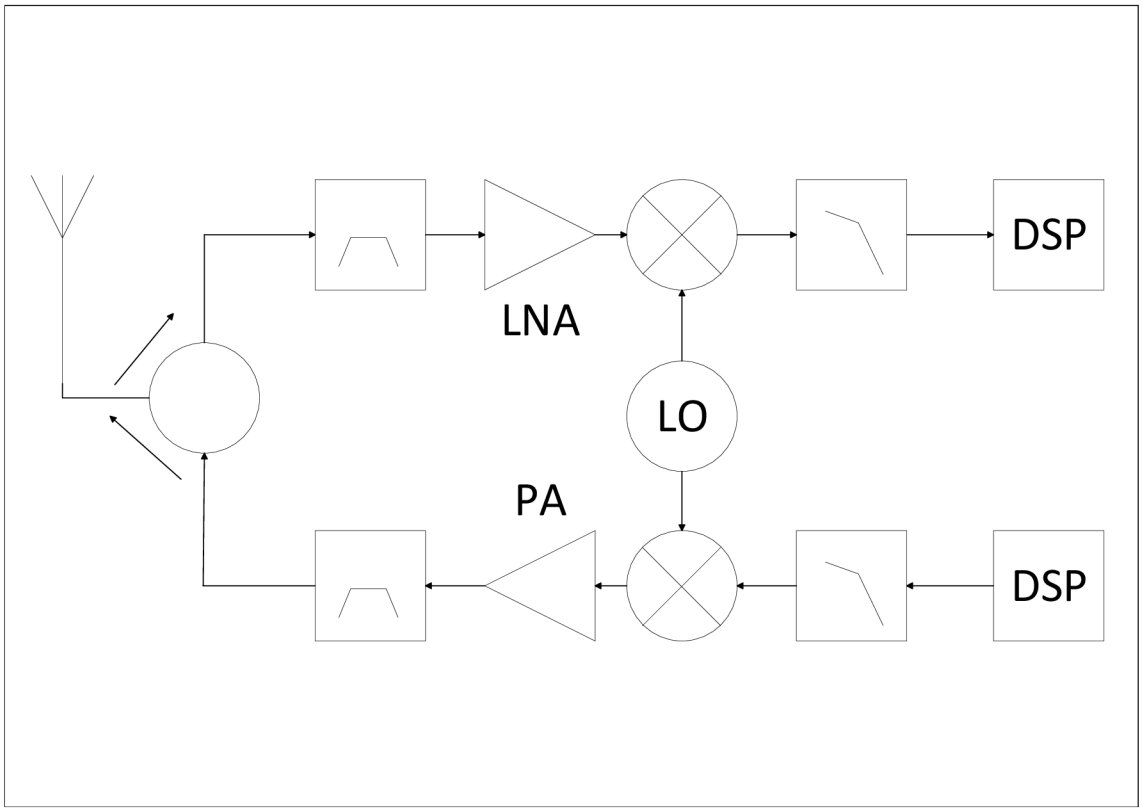
Softwarové rádio je hardwarové zařízení, které se v základu skládá z antény a AD převodníku v přijímací části a DA převodníku v části vysílací. O zpracování surového signálu se v principu stará software. Softwarové rádio má však své omezení ve zmíněných převodnících. Dostupné převodníky jsou schopny pracovat maximálně v řádu stovek MHz. Softwarově definované rádio je tak oproti softwarovému rádiu vybaveno směšovači, které konvergují signál do frekvencí se kterými již mohou pracovat AD převodníky. Přidáním obvodů pro číslicové zpracování signálů se může přijímané spektrum upravit na požadovaný signál. Jinými slovy je softwarově definované rádio full-duplex transceiver s vysokým frekvenčním rozsahem. Často se pro softwarově definované rádio využívá zkratka SDR. Oproti obecnému radiopřijímači není SDR hardwarem fixně omezeno na specifickou část radiového spektra. Díky FPGA je možné matematicky nasimulovat prvky přijímače jako jsou cívky a kondenzátory pomocí konfiguračního souboru nahraného do logického obvodu. To přináší výhodu ve flexibilitě zařízení, kdy například pro nový standard postačí jen aktualizovat firmware SDR [8].

1.1.1 Obecné schéma softwarově definovaného rádia

Každé SDR obsahuje AD převodník (ty které umějí i vysílat musejí mít DA převodník) Aby mohlo SDR pracovat i s frekvencemi vyššími než dovolují osazené převodníky, využívá se analogové down konverze. Existují dvě cesty jak přesunout signál do převodníkem podporovaných pásem nazývané homodyn a heterodyn. Homodyn směšuje signál do základního pásma a pak ho rovnou směšuje, zatímco heterodyn provádí konverzi do základního pásma až po digitalizaci, tedy až v číslicové oblasti. V obou případech se signály ve směšovači sloučí se signálem generovaným lokálním řízeným oscilátorem a výstupem je součtový a rozdílový signál se kterým je možno dále pracovat, neboť se nachází již na nižších frekvencích. Pro down konverzi se využívá rozdílových signálů [9], [10]. Obecný příklad schématu SDR je na Obr. 1.1.

1.1.2 Využití softwarově definovaného rádia

Díky zmíněné flexibilitě je využití SDR široké. Pouhou změnou firmwaru je tak možno s jedním hardwarem zachytávat komunikaci meteostanic a v jiném okamžiku přijí-



Obr. 1.1: Schéma softwarově definovaného rádia [11].

mat televizní signál. Tato výhoda je však na úkor náročnosti na výpočetní výkon jednotky zpracovávající surový signál generovaný softwarovým rádiem. To, a vyšší cena komponentů SDR, omezuje využití SDR v praktickém nasazení [6].

1.1.3 Omezení využívání bezdrátového spektra

Při využívání různých bezdrátových zařízení uživatel zpravidla nevěnuje pozornost omezením a pravidlům využívání rádiového spektra. Tato omezení aplikují již výrobci do svých zařízení a uživatel tak mnohdy nemá možnost zařízení využívat nepovoleným způsobem. Jiná situace však nastává u SDR. Vzhledem k tomu, že zařízení umí signály jak přijímat, tak i vysílat v širokém spektru frekvencí, musí uživatel vědět, v jakých pásmech smí vysílat a jaké to s sebou nese případné omezení. Informace o pravidlech využívání rádiového spektra jsou pro Českou Republiku vydávaná Českým Telekomunikačním Úřadem, který své směrnice harmonizuje s nařízením evropského parlamentu a rady.

1.1.4 Dostupná softwarově definovaná rádia

Při výběru SDR hraje roli mimo parametry jednotlivých hardwarových desek také komunita, která za nimi stojí. Tato komunita se mimo jiné stará o implementaci podpory různých softwarů a jejich aktuálnost a také o správnou funkci ovladačů. Například za projektem LimeSDR stojí silná komunita, přesto i po několika měsících od vydání GNUradia verze 3.8 není tato verze podporována obslužnými moduly. V Tab. 1.1 jsou parametry tří SDR, které jsou použity v této práci a pro srovnání je uvedeno i zařízení USRP, které je etalonem na poli SDR.

Tab. 1.1: Srovnávací tabulka softwarově definovaných rádií.

	LimeSDR mini	LimeSDR	bladeRF 2.0	USRP B210
Minimální frekvence	10 MHz	100 kHz	47 MHz	70 MHz
Maximální frekvence	3,5 GHz	3.8 GHz	6 GHz	6 GHz
Šířka pásma	30,72 MHz	61.44 MHz	56 MHz	56 MHz
Vzorkovací frekvence	30,72 MS/s	61,44 MS/s	61,44 MS/s	61,44 MS/s
Počet vstupů/výstupů	1x1 MIMO	2x2 MIMO	2x2 MIMO	2x2 MIMO

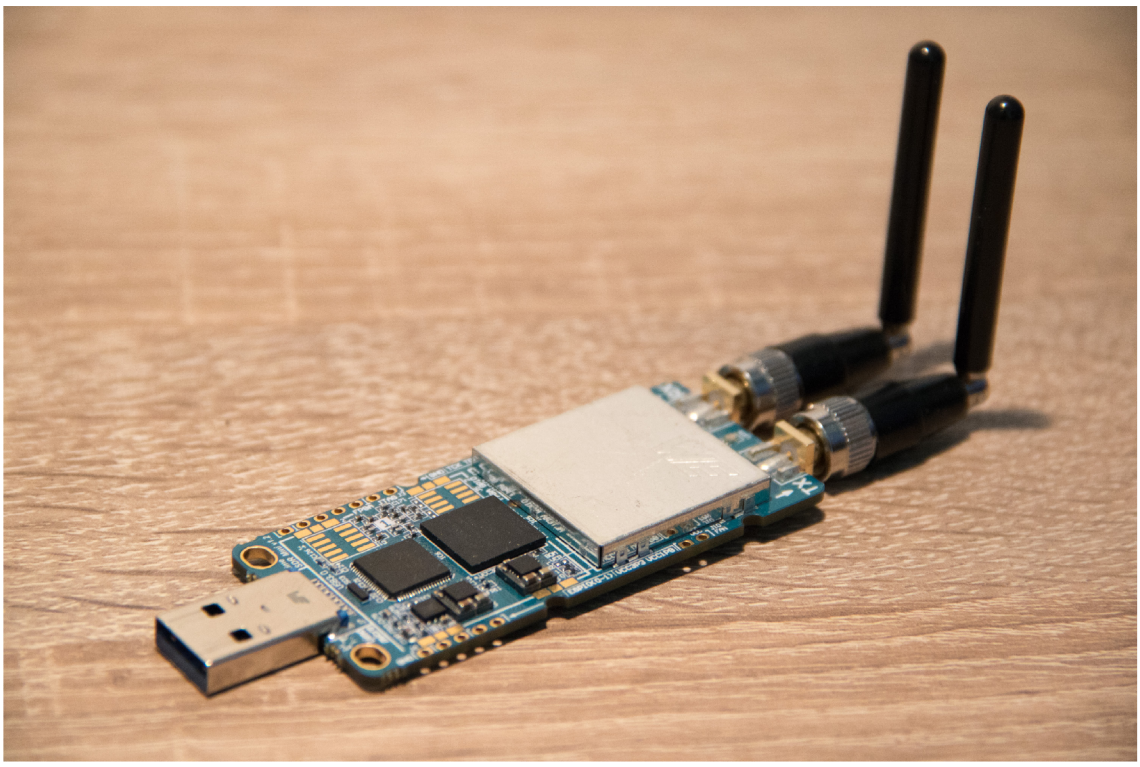
Universal Software Radio Peripheral

USRP (Universal Software Radio Peripheral) je podmnožina SDR. Ve spojení s výkoným softwarem jako je GNUradio je USRP schopno dosáhnout velmi širokého frekvenčního rozsahu 0 - 6 GHz. Tento frekvenční rozsah však závisí na typu subdesek. USRP se totiž skládá z jednoho FPGA obvodu, ke kterému může být připojeno více přijímacích, nebo vysílacích "subdesek". S pomocí USRP je také možno využívat technik vícenásobného vstupu a vícenásobného výstupu (MIMO). To je umožněno instalací propojovacího kabelu mezi dvěma zařízeními USRP [12], [13].

LimeSDR mini

LimeSDR mini je menší, cenově dostupnější verze původní LimeSDR a jako ona je osazena stejným transcieverem LMS7002M MIMO FPRF od Lime Microsystems, který je vybaven 12 bitovými DA/AD převodníky pro zpracování signálu. Samotný čip by měl pokrývat frekvenční rozsah od 100 kHz do 3,8 GHz, který je však dalšími obvody omezen na 10 MHz až 3,5 GHz, i šířka pásma byla omezena z 61,44 MHz na 30,72 MHz. Toto omezení vývojáři zvolili, aby docílili lepších výsledků v celém provozním rozsahu. LimeSDR Mini může vysílat i přijímat signály, jelikož na výstupu je k dispozici až 10 dBm vysílacího výkonu. V době psaní této práce se cena jedné desky pohybovala kolem 160 USD. LimrSDR mini má místo čtyř kanálů kanály dva

a dva SMA konektory pro připojení antén. Dále je vybaven MAX 10 FPGA od společnosti Intel, který je umístěn mezi USB 3.0 kontrolerem a trancieverem. Pomocí nástroje Intel Quartus lze vygenerovat instrukce pro FPGA a pomocí příslušného nástroje jej poté importovat do obvodu. Na desce je také přítomen teplotou řízený krystalový kondenzátor Rakon 40 MHz VCTCXO, kvůli kterému se doporučuje zajistit zařízení dostatečné chlazení, neboť se zmíněný oscilátor může odchýlit od nastavené frekvence. Na desce jsou však k dispozici i UF.L konektory pro připojení externího zdroje referenčního signálu [14].



Obr. 1.2: LimeSDR mini.

LimeSDR

LimeSDR je větší a výkonnější sourozenec LimeSDR mini, avšak oba používají stejný transceiver LMS7002M. Na rozdíl od mini disponuje LimeSDR pokročilými hradlovými poli Altera MAX 10 FPGA společnosti Intel. Zásadním rozdílem je také USB kontroler Cypress FX3 Super Speed USB třetí generace. Zařízení se dodává s anténami naladěnými na nejpoužívanější pásma 800–960 MHz / 1710–2170 MHz / 2400–2700 MHz. Deska disponuje jedenácti U.FL konektory. Šest z nich je pro přijímací část, čtyři pro vysílání a jeden pro externí generátor času. Dvě LED diody se starají o indikaci stavu zařízení. Napájení je zajišťováno buď z USB 3.0, nebo pro náročnější aplikace deska disponuje konektorem pro externí napájení s napětím

6 až 12 voltů. Vzhledem k velkému přehřívání zařízení je zde i konektor pro 3,3 V větráček. Výkon vysílací části dosahuje až 10 dBm v závislosti na dané frekvenci. Toto zařízení se dodává buď jen jako základní deska, nebo v akrylátovém obalu, nebo v hliníkové skříni, která navíc odvádí teplo. LimeSDR je plně open source projekt a navíc podporuje Snappy Ubuntu Core, což je platforma, která poskytuje prostředí pro aplikace vývojářů. Přináší jednoduchost instalace aplikací z mobilních telefonů do Linuxového prostředí Ubuntu, neboli technologie transakční instalace obrazů systému a aplikací.

Obr. 1.3: Základní deska LimeSDR.

BladeRF

Blade je další zástupce SDR od společnosti Nuand. Nová generace bladeRF 2.0 micro xA4 je SDR nabízející frekvenční rozsah 47 MHz až 6 GHz, vzorkovací frekvenci 61,44 MHz a 2×2 MIMO streamování. Díky libbladeRF je bladeRF 2.0 micro kompatibilní s GNURadio, GQRX, SDR-Radio, SDR #, gr-fosphor a SoapySDR. Všechny SMA RF porty jsou schopny poskytovat napájení pro širokopásmové zesilovače a předzesilovače. Napájení periferií je plně softwarově ovladatelné a poskytuje maximální provozní flexibilitu. Jádrem bladeRF 2.0 micro je nejnovější generace Cyclone V FPGA od společnosti Intel. Pokročilá taktovací architektura umožňuje tomuto

zařízení přijímat a vysílat hodiny z vysoce přesného a stabilního oscilátoru do a z jiných zařízení. Instalovaný DAC nastaví kmitočet oscilátoru na továrně kalibrovanou hodnotu. Distribuce napájení jednotlivých částí na desce je propracovaná a komplexní. Je tak možno napájet z USB, zatímco injektory je možno přepnout na napájení z externího stejnosměrného napájení pomocí lineárních regulátorů výkonu. To slouží k zajištění maximálního lineárního výkonu periferií trpících na zkreslení. To je docíleno blokovacími obvody pro optimalizaci odebírání energie mezi USB sběrnicí a externím stejnosměrným napájením. Další výhodou je, že může běžet i bez nutnosti připojení k PC, nebo SBC. Flash paměť je dostatečně velká, aby pojala obraz FPGA libovolné velikosti [15].

Obr. 1.4: Základní deska bladeRF.

1.2 Standard IEEE 802.11

Standard s označením IEEE 802.11 vydaný mezinárodním standardizačním institutem IEEE (Institute of Electrical and Electronics Engineers) popisuje strukturu bezdrátové komunikace v ISM (Industrial, Scientific, Medical) pásmech 2,4 GHz a 5 GHz. Institut pro elektrotechnické a elektronické inženýrství je organizace sídlící ve státě New Jersey a jejím cílem je vyvíjet a standardizovat nové technologie v oblasti radiokomunikací. Zkratka IEEE 802.11 se často zaměňuje za zkratku Wi-Fi.

Tato substituce však není na místě. Jedná se totiž o známku kompatibility, kterou vystavuje sdružení Wi-Fi Alliance. Wi-Fi Alliance vlastní ochrannou známku Wi-Fi, a tak každý výrobek toužící po tomto označení, musí projít testováním Wi-Fi Alliance, která jej může certifikovat. Znamená to tedy, že ne každý výrobek komunikující standardem IEEE 802.11 splňuje požadavky Wi-Fi Alliance a nemusí tak být kompatibilní. Avšak to, že zařízení nemá danou známku také neznamená, že s Wi-Fi zařízeními nemůže komunikovat. Potřeba této instituce vznikla v začátcích protokolu IEEE 802.11, kdy mezi sebou nebylo možné propojit zařízení různých výrobců z důvodu nekompatibility [16].

1.2.1 Frekvence využívané protokolem IEEE 802.11

Standard podporuje 39 kanálů v rozmezí od 2,312 GHz - 2,732 GHz a 237 kanálů v rozmezí 4,92 GHz - 6,1 GHz, avšak vzhledem k tomu, že bezlicenční pásmo má užší rozsahy, je ve skutečnosti používáno jen 13 kanálů ve frekvenčním rozmezí 2,4 GHz - 2,4835 GHz a 50 kanálů v oblasti 5,170 GHz - 5,825 GHz, a to díky omezením plynoucím z norem a národních kmitočtových tabulek. V České republice se při využívání těchto ISM frekvencí musí nastavení řídit harmonizovanou normou ČSN ETSI EN 300 440 upravující podmínky pro zařízení krátkého dosahu. Rádiová zařízení používaná v kmitočtovém rozsahu 1 GHz až 40 GHz, dále normou ČSN ETSI EN 300 328, která předepisuje chování zařízení pro přenos dat pracující v pásmu ISM 2,4 GHz a používající techniky širokopásmové modulace a pro 5 GHz pásmo normou ČSN ETSI EN 301 893 pro širokopásmové rádiové přístupové sítě a vysokovýkonné rádio LAN v 5 GHz pásmu. Tyto normy definují výkonové parametry, jakými je možno v těchto frekvencích komunikovat. Tyto hodnoty se liší podle lokálních norem daných geografických oblastí. Například pro Českou republiku, která své normy harmonizuje dle Směrnice 2014/53/EU Evropského parlamentu a rady ze dne 16. dubna 2014, platí omezení uvedené v Tab. 1.2. Český telekomunikační úřad vydává všeobecná oprávnění VO-R/12/09.2010-12 a VO-R/10/01.2019-1, ve kterých se definuje využívání pásem. Bohužel jsou však čísla kanálů lehce zavádějící, neboť jsou od sebe ve 2,4 GHz pásmu vzdáleny 5 MHz a šířka potřebná pro přenos s rozprostřeným spektrem je 20 MHz. To znamená, že ve 2,4 GHz pásmu zbývají jen tři nepřekrývající se kanály a v 5 GHz je jich pro Evropu 24.

Navíc jsou k jednotlivým omezením stanoveny další podmínky. Pro omezení je zde rozdíl v povolené spektrální hustotě podle druhu použité modulace. Pro modulaci DSSS/OFDM je maximální hodnota spektrální hustoty 10 mW/1 MHz a pro modulaci FSSS až 100 mW/1 MHz. Omezení pro skupiny b a c je použití pouze uvnitř jedné budovy [16], [17], [18].

Tab. 1.2: Tabulka omezení užívaných frekvenčních pásem.

Ozn.	Kmitočtové pásmo	Vyzářený výkon	Max. spektrální hustota
a	2400 - 2483,5 MHz	100 mW e.i.r.p.	10 mW/1 MHz
a	2400 - 2483,5 MHz	100 mW e.i.r.p.	100 mW/1 MHz
b	5150–5250 MHz	200 mW střední e.i.r.p.	10 mW/MHz
c	5250–5350 MHz	200 mW střední e.i.r.p.	10 mW/MHz
d	5470–5725 MHz	1 W střední e.i.r.p.	50 mW/MHz

1.2.2 Metoda přístupu k přenosovému médiu

V bezdrátových sítích standardu IEEE 802.11 se využívá CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) technika přístupu k médiu. To znamená, že stanice před odesláním rámce chvíli naslouchá, zdali je daný kanál volný. V případě, že v daném pásmu již někdo komunikuje, vyčká stanice dokud se médium neuvolní a následně zahájí proces exponenciálního čekání, kdy čeká náhodně dlouho a když je i poté kanál obsazen zdvojnásobuje svou čekací dobu. Díky tomu se vzrůstajícím počtem klientů v síti klesá reálná propustnost. CSMA/CA je u IEEE 802.11 využívána zejména kvůli takzvanému poloduplexnímu režimu spojení. To znamená, že stanice buď naslouchá, nebo vysílá na tomtéž kanálu, nikoliv obojí naráz. Největší problém tohoto přístupu je však takzvaný problém skrytého uzlu. Ten nastává v situaci, kdy přístupový bod je mezi dvěma stanicemi, které se vzájemně "neslyší"(jsou od sebe vzdálené natolik, že nedokáží přijmout signály mezi sebou navzájem). V tomto případě stanice začnou vysílat data do přístupového bodu paralelně a přístupový bod nedokáže rozeznat ani jeden datový tok. Tento problém řeší v protokolu IEEE 802.11 mechanizmus RTS/CTS, který definuje zprávy Request To Send a Clear To Send, kterými se stanice táže přístupového bodu, zdali může vysílat po stanovenou dobu. Přístupový bod odpovídá zprávou, že stanice může zahájit vysílání. Tuto zprávu obdrží i všechny ostatní stanice v síti a tak žádná z nich nezačne vysílání v intervalu vyhrazeném pro stanici, která si zažádala první. V praxi je tento mechanizmus aktivován od předem definované velikosti paketu, neboť pro mnoho malých paketů je tento přístup neefektivní [19].

1.2.3 Dodatky IEEE 802.11

Standard IEEE 802.11 má již řadu dodatků, které mění oproti původnímu standardu parametry přenosu a to jak zvolenou modulací, tak i jinými atributy, které mají vliv na výslednou rychlost. Původní standard vyšel v roce 1997 a od té doby bylo vydáno mnoho dodatků, které posouvají bezdrátovou komunikaci na vyšší rychlosti a lepší parametry. Vybrané dodatky jsou dále stručně popsány.

IEEE 802.11a

IEEE 802.11a byl vydán v roce 1999 a využívá 5 GHz pásmo a OFDM (Orthogonal Frequency Division Multiplexing) modulaci popsanou v kapitole 1.2.4. Od BPSK (Binary-Phase Shift Keying) s rychlostí 6 Mb/s až po 64-QAM s rychlostí 54 Mb/s. Využití 5 GHz pásma dává tomuto standardu velkou výhodu v zarušených prostředích, kde je obvykle 2,4 GHz pásmo zahlcené. Konflikty totiž mohou způsobovat časté přerušení připojení a zhoršení služeb. Vyšší frekvence však přináší i nevýhodu v podobě dosahu. Oproti IEEE 802.11b/g má IEEE 802.11a menší dosah zejména uvnitř budov. Signály standardu IEEE 802.11a nemohou pronikat tak hluboko, protože jsou snáze absorbovány stěnami a jinými pevnými předměty v jejich cestě a také díky tomu, že útlum volného prostoru je úměrný druhé mocnině signálové frekvence. Naopak propagační výhodou IEEE 802.11a je OFDM modulace, která je výhodou v prostředí, kde se signály šíří více cestami, například uvnitř budov. Vyšší frekvence navíc umožňují použití menších antén s vyšším ziskem.

IEEE 802.11b

IEEE 802.11b byl stejně jako IEEE 802.11a vydán v roce 1999, ale tento pracuje na frekvenci 2,4 GHz jako jeho předchůdce, avšak na rozdíl od něj používá modulační techniku CCK, neboli komplementární kódování klíčů, což je jen upravená metoda CDMA (Code Division Multiple Access), která jako základ používá základní techniku přímého rozprostřeného spektra DSSS (Direct Sequence Spread Spectrum) popsanou v kapitole 1.2.4. Každý paket IEEE 802.11b má záhlaví, které je přenášeno v režimech 1 Mb/s nebo 2 Mb/s pomocí DSSS. Záhlaví je složeno ze 192 bitů, z nichž 128 bitů je PN sekvence používaná pro identifikaci kanálu a školení ekvalizéru v přijímači. Dalších 64 bitů poskytuje informaci o typu modulace, délce paketu a jiné parametry. Těchto 192 bitů hlavičky se šíří s 11 bitovou Barkerovou sekvencí a moduluje se BPSK. Datová část rámce může být přenášena 1 Mb/s, 2 Mb/s režimy, které i nadále používají čistou techniku DSSS s Barkerovým kódováním, a nebo posledními dvěma režimy 5,5 Mb/s, 11 Mb/s, které používají CCK modulaci [20]. Vzhledem k tomu, že původní specifikace IEEE 802.11 používala čistou CDMA/DSSS techniku, bylo nasazení tohoto standardu rychlé, neboť stačilo jen lehce upravit stávající čipovou sadu. Touto úpravou se zvýšila odolnost proti rušení a i teoretická rychlost z 2 Mb/s na až 11 Mb/s. Jiné, neoficiální označení tohoto standardu je Wi-Fi 1, což je takzvaný retronym, neboli nový název pro starou věc [21].

IEEE 802.11g

IEEE 802.11g je standard rozšiřující předchozí IEEE 802.11b vydaný v roce 2003 Využívá stejnou frekvenci, ale využívá navíc OFDM modulaci, čímž se při jeho po-

užití posouvá teoretická propustnost na fyzické vrstvě až na 54 Mb/s. Retronymní označení je pro tuto generaci Wi-Fi 3. Standard je schopen používat jen DSSS modulaci, nebo OFDM modulaci, nebo jejich kombinace, proto jsou zde definovány čtyři fyzické vrstvy. Tyto vrstvy jsou pojmenovány jako extended rate physicals (ERPs). První dvě jsou povinné a zbylé dvě jsou volitelné. Komunikující zařízení se dohodnou, kterou vrstvu budou pro svou komunikaci používat.

- ERP-DSSS/CCK: Stará fyzická vrstva používaná standardem IEEE 802.11b. Technologie DSSS se používá s modulací CCK. Tato vrstva je zde kvůli zpětné kompatibilitě se standardem IEEE 802.11b a poskytuje tak i stejné přenosové rychlosti.
- ERP-OFDM: Nová fyzická vrstva, zavedená ve standardu IEEE 802.11g. Využívá OFDM modulaci k dosažení maximálních datových rychlostí IEEE 802.11a v pásmu 2,4 GHz.
- ERP-DSSS/PBCC: Tato fyzická vrstva byla zavedena v IEEE 802.11b a poskytuje stejné datové rychlosti jako fyzická vrstva DSSS/CCK a navíc je rozšiřuje o sadu přenosových rychlostí 22 Mb/s a 33 Mb/s. Toho bylo dosaženo využitém technologie DSSS s kódovacím algoritmem PBCC (packet binary convolutional coding).
- ERP-DSSS-OFDM: Nová fyzická vrstva, která používá hybridní kombinaci DSSS a OFDM. Fyzická hlavička paketu je přenášena pomocí DSSS, zatímco payload (užitečná data) paketu jsou přenášena pomocí OFDM.

Pro snížení režie a zvýšení výkonu sítě je zavedena povinná podpora krátké preambule. Režie fyzické vrstvy IEEE 802.11 sestává ze dvou částí: preambule protokolu fyzické vrstvy (PLCP) použitého pro synchronizaci a záhlaví PLCP, které obsahuje informace o paketech vztahující se k fyzické vrstvě. Krátká preambule je bezmála poloviční oproti dlouhé verzi. Standard IEEE 802.11g zahrnuje dynamické přizpůsobení časového okna pro jednu stanici. Podporují-li všechny stanice v sítí ERP-OFDM, aktivuje se ERP atribut. Vzhledem k široké škále možností parametrů komunikace a kvůli zpětné kompatibilitě zařízení můžou nastat komplikace, například když jedna stanice komunikuje pomocí nové EPS-OFDM fyzické vrstvy a jiná tuto vrstvu nepodporuje, a tak daný signál neslyší a začne tak vysílat svá data. Aby tento problém nenastal, jsou zavedeny dvě opatření, kdy se hlavičky přenášejí pomocí DSSS modulace, nebo je aktivován CTS-to-Self mechanismus, což je režijně méně náročná alternativa k RTS/CTS mechanismu [22].

IEEE 802.11n

IEEE 802.11n má oproti svým předchůdcům upravenou podvrstvu přístupu k médiu takovým způsobem, že maximální rychlost komunikace na fyzické vrstvě dosahuje

600 Mb/s. Těchto rychlostí je dosaženo zejména díky technice vícenásobného šíření signálu mezi komunikujícími stranami, označovaného jako MIMO (multiple input multiple output). Nejvyšších rychlostí je dosahováno v konfiguraci 4x4 MIMO, neboli 4 vstupy, 4 výstupy. Ovšem nejčastěji je v zařízeních použito 2x2 MIMO, neboť pro každý vstup musí být použita vlastní anténa a vyšší počet antén je z hlediska kompaktnosti zařízení mnohdy nemožný. K navýšení teoretické přenosové rychlosti přispěla i podpora 40 MHz šířky pásma, to vyplývá i z Shannonovy rovnice 1.1, kde C je kapacita kanálu, B je šířka pásma a SNR je odstup signálu od šumu.

$$C = B \log_2(1 + SNR) \tag{1.1}$$

Stejně jako v předchozích protokolech jsou některé inovace jen volitelné a v případě, že je jedna stanice v síti nepodporuje, klesá teoretická propustnost celé sítě. Dalším vylepšením je takzvaný Beamforming, neboli tvarování paprsku. To je technika kdy při využití MIMO může přístupový bod i přes vše-směrovost antény směrovat výkon paprsku [24].

1.2.4 Fyzická vrstva

Fyzická vrstva zajišťuje samotný přenos informace daným prostředím. V případě standardu IEEE 802.11 se jedná o vzduch, tedy o bezdrátové prostředí.

FHSS modulace

Frequency Hopping Spread Spectrum je název modulace, která je využívána například technologií Bluetooth, nebo původním standardem IEEE 802.11. Využívá se desítek kanálů s šířkou pásma 1 MHz, mezi kterými vysílač pseudonáhodně přeskakuje. Tato modulace poměrně dobře odolává rušení, neboť při neúspěšném přenosu na jedné nosné se jednoduše pošle daná informace znova na jiné frekvenci. Tento způsob modulace je však velmi limitující z hlediska přenosové rychlosti [19].

DSSS modulace

Direct Sequence Spread Spectrum je modulace s rozprostřeným spektrem jež byla využívána standardem IEEE 802.11b a umožnila tak přenášet větší objem dat za jednotku času. Princip spočívá v nahrazení přenášeného bit pseudonáhodnou sekvencí bitů rozprostřenou ve spektru. Tento princip je odolný vůči úzkopásmovému rušení. Bez znalosti kódovací sekvence je pro přijímač pozorovatelný pouze šum. To je prvním krokem k zabezpečení WiFi signálu [19].

OFDM modulace

Předchozí dvě modulační techniky však brzy nahradil ortogonální multiplex s frekvenčním dělením neboli OFDM. OFDM je taktéž širokopásmová modulace, která využívá ortogonálních frekvencí, které skládá velmi blízko sebe ve využívaném kanálu. Díky ortogonalitě nedochází mezi sousedními frekvencemi k přeslechům. Na samotném začátku modulátoru se posloupnost bitů převádí demultiplexorem rozdělí na n posloupností, kde n je počet subnosných pro data. Standard IEEE 802.11a/g/n/ac využívá dohromady 64 subnosných, ale ne všechny jsou použity pro přenos dat. Pro IEEE 802.11a/g je pro data vyčleněno 48 subnosných a pro standard IEEE 802.11n/ac jich je 52. Těchto n řetězců se moduluje každý zvlášť příslušnou modulací, například BPSK, nebo QAM na komplexní symboly. Tyto jsou dále v bloku inverzní rychlé furierovy transformace převedeny z frekvenční oblasti do časové. Pro omezení intersymbolové interference se nakonec vkládá mezi symboly ochranný interval, čímž se modulace stává odolnější proti přeslechům způsobeným například způsobeným vícecestným šířením. Na výstupu modulátoru je pak digitálně-analogový převodník a upkonvertor [32].

Struktura zpráv na fyzické vrstvě

Fyzické vrstvy se liší dle jednotlivých standardů IEEE 802.11X, všechny však mají fyzickou vrstvu rozdělenu do dvou podvrstev.

- První vrstva zvaná PLCP (Physical Layer Convergence Procedure) přidává k datovým rámcům informace o použitém přenosovém mechanismu a modulaci. Pro vyšší vrstvy je tak nepodstatné jaké přenosové médium je využíváno. Vyšší vrstvě kromě samotných dat předává tato podvrstva i informace o dostupnosti přenosového média.
- Druhou vrstvou je PMD (Physical Medium Dependent), což je podvrstva, která má na starost samotná přenos dat mezi vysílači. Využity jsou k tomu data o modulaci a přenosovém mechanizmu z předcházející podvrstvy PLCP.

1.2.5 Zabezpečení

Kvůli nedostatkům v původním zabezpečení WPA byla založena skupina IEEE 802.11i, která měla za úkol vytvořit nové zabezpečení pro bezdrátové sítě. Vzniklý protokol IEEE 802.11i známý jako WPA2 je nejčastější způsob zabezpečení. Využívá místo kryptografického algoritmu RC4 standardní šifrovací standard AES (Advanced Encryption Standard). Velkým bezpečnostním rizikem je volitelná funkce, která je stále u mnohých sítí aktivována, a to funkce WPS (Wi-Fi Protected Setup). WPS není

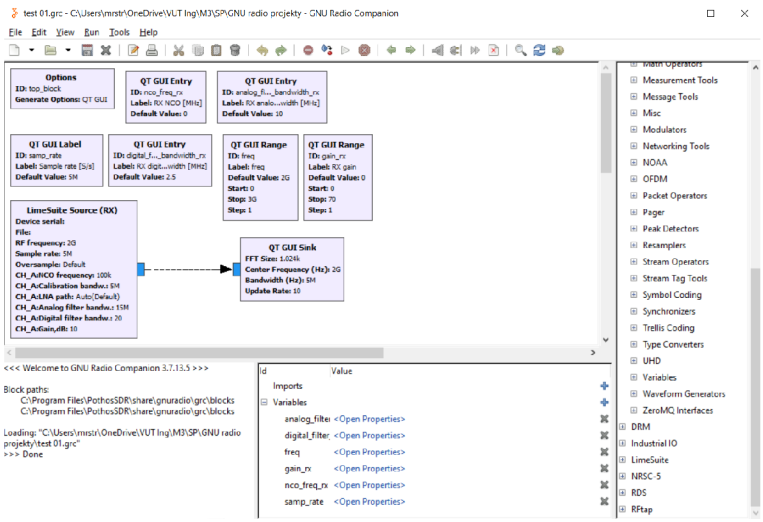
součástí protokolu IEEE 802.11 a umožňuje útočníkovi obnovit kód WPS a tím i heslo routeru během několika hodin [23].

1.3 Popis softwaru GNUradio

GNU Radio je open-source nástroj pro implementaci SDR, který poskytuje framework a nástroje pro tvorbu a spouštění SDR a navazujících aplikací. Projekty se v GNU Radiu nazývají flow grafy, které jsou složeny z vzájemně propojených bloků zpracování signálu. Tyto bloky mohou být napsány v jazyce C++ nebo Python. Jádro aplikace je napsáno v jazyce C++. GNU Radio lze provozovat jako nástroj pro ovládání SDR, nebo jen k simulování signálových toků. Lze si zcela virtuálně vytvořit různé signály se kterými lze pracovat a následně třeba odeslat do SDR a vysílat je do rádiového prostředí. Tento nástroj je využíván jak v akademické tak i v komerční sféře, nebo také v zájmové oblasti.

1.3.1 GNU Radio Companion

GNU Radio Companion je grafický nástroj pro vytváření Flow grafů (projektů) a následné generování zdrojového kódu podle vytvořeného schéma. Na Obr. 1.5 je snímek uživatelského rozhraní GNU Radio Companion s vytvořeným projektem pro základní zobrazení spektra a nastavení parametrů pomocí posuvníku v běhu programu bez nutnosti manuální rekonfigurace Flow grafu. V pravé části se nachází "strom"prvků, do kterého je před připojením SDR nutné přidat instalací položky pro ovládání konkrétní rodiny SDR pomocí instalace daného modulu.



Obr. 1.5: Uživatelské rozhraní GNU Radia s vytvořeným Flow grafem.

2 Zachycení komunikace IEEE 802.11

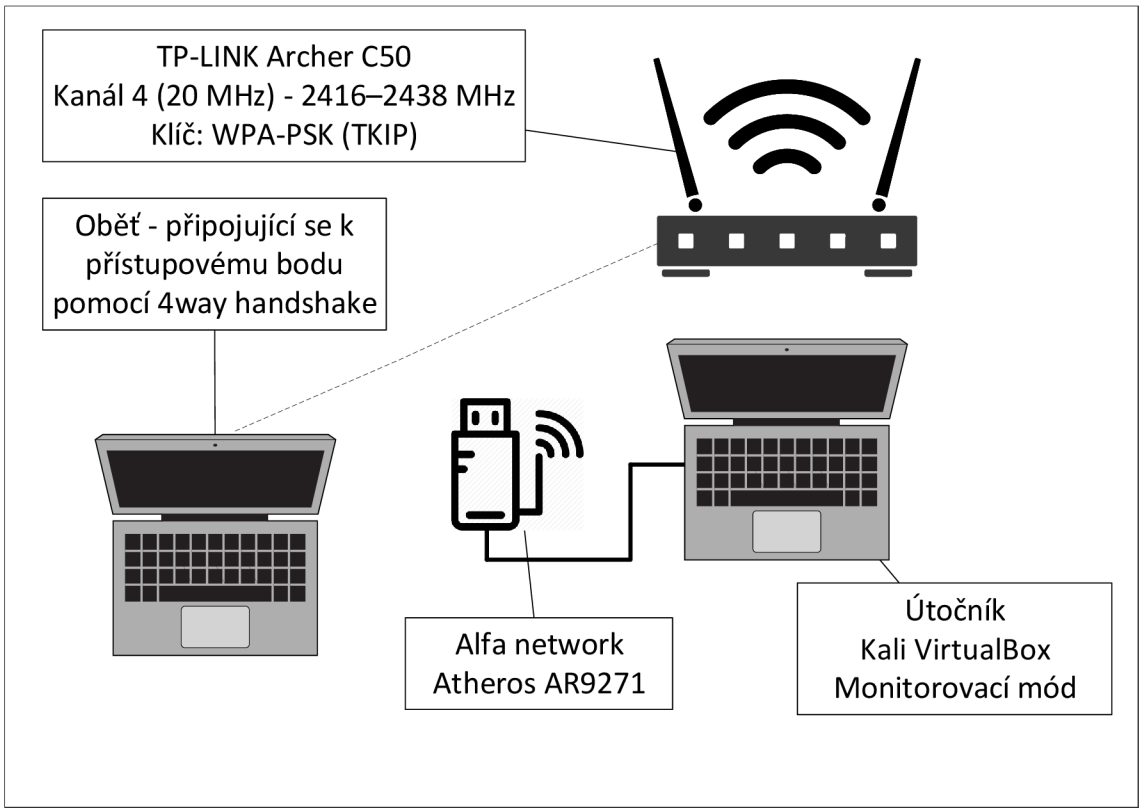
Cílem této kapitoly stejně jako cílem diplomové práce je zachytit bezdrátovou komunikaci splňující požadavky standardu IEEE 802.11. Bude popsán postup instalace potřebných nástrojů, jejich konfigurace a následné zprovoznění odposlechu komunikace pomocí USB bezdrátové síťové karty, která bude následně postupně nahrazena softwarově definovanými rádii LimeSDR mini, LimeSDR a bladeRF.

2.1 Zachycení pomocí bezdrátové síťové karty

Prvním krokem pro seznámení se s problematikou odposlechu bezdrátové komunikace bylo zachytávání pomocí bezdrátové síťové karty.

2.1.1 Sestavení topologie

Předpokladem k zachycení komunikace využívající protokol IEEE 802.11 bylo sestavení sítě viz Obr. 2.1.



Obr. 2.1: Topologie odposlechu bezdrátové komunikace.

Topologie sestává z routeru TP-LINK Archer C50 s bezdrátovým přístupovým rozhraním, umožňujícím komunikovat standardem IEEE 802.11b, k němu připojitelnému zařízení a počítačem s potřebnými nástroji pro odposlech bezdrátových sítí a bezdrátovou síťovou kartu umožnující monitoring.

Konfigurace routeru

Po zapojení routeru a jeho konfiguraci připojení k internetu byly zvoleny parametry podle následující tabulky Tab. 2.1.

Tab. 2.1: Parametry přístupového bodu.

Parametr	**Hodnota**
Standard:	IEEE 802.11b
SSID:	TP-LINK
Kanál:	4
Frekvence:	2416–2438 MHz
Šířka pásma:	20 MHz
Typ zabezpečení:	WPA-PSK
Typ šifrování:	TKIP

Typ šifrování TKIP byl zvolen z toho důvodu, že se šifrováním druhého možného způsobu, tedy ASK, nebylo následně možno dekódovat obsah rámce.

Konfigurace monitorovací stanice

Pro zachycení bezdrátové komunikace byla využita síťová karta od společnosti Alfa Network s chipsetem Atheros AR9271, umožňujícím provozovat monitorování veškeré komunikace na daném kanálu. Na rozdíl od promiskuitního módu lze v monitorovacím módu sledovat veškerou komunikaci na daném kanálu a monitorovací zařízení nemusí být připojeno k přístupovému bodu jako tomu je u promiskuitního módu. Tato možnost je nezbytná pro zachycení úvodní komunikace připojujícího se zařízení. Dalším krokem konfigurace bylo nastavit samotný počítač. Jako nejvhodnější operační systém byl zvolen Kali Linux verze 2019.4, který je hojně využívaný pro forenzní analýzu a penetrační testování. Tato distribuce je odvozena od Debianu a obsahuje mnoho nástrojů pro práci v síťovém prostředí. Instalace systému byla provedena na virtuální stanici a připojená síťová karta byla přemostěna a následně přepnuta do monitorovacího módu pomocí následující sekvence příkazů: Výpis všech dostupných bezdrátových rozhraní.

```
sudo airmon-ng
```

Přepnutí módu síťové karty.

```
sudo airmon-ng start wlan0
```

Tímto příkazem bylo vytvořeno nové rozhraní wlan0mon, které je již v monitorovacím módu. Nakonec je nutné ukončit ostatní procesy využívající dané rozhraní.

```
sudo airmon-ng check kill
```

Generování zachyceného provozu

Jako zdroj odposlouchávaného provozu bude sloužit počítač využívající program Scapy. Scapy je program umožňující vytvářet, posílat a falšovat pakety. Je to program psaný v jazyce python a lze jej importovat do Python scriptu. Pro názornost a snadné rozeznání při následné analýze datové komunikace byl vytvořen příkaz vytvářející deset ICMP paketů o velikosti 1 kB. Tento příkaz byl spuštěn 5 krát. Příkaz pro generování paketů v programu Scapy:

```
send(IP(dst="169.254.96.148")/
ICMP()Raw(RandString(size=1000)),count=5)
```

Tato sekvence pěti pingů byla odeslána na IP adresu routeru šest krát s rozestupem přibližně pět sekund.

2.1.2 Analýza zachyceného signálu

Po spuštění zachytávání provozu programem Wireshark je možno vidět všechny rámce vysílané různými zařízeními v daném kanálu. Tuto situaci zobrazuje Obr. 2.2. Zjistit MAC adresu síťové karty klientské stanice lze pomocí příkazu

```
ipconfig /all
```

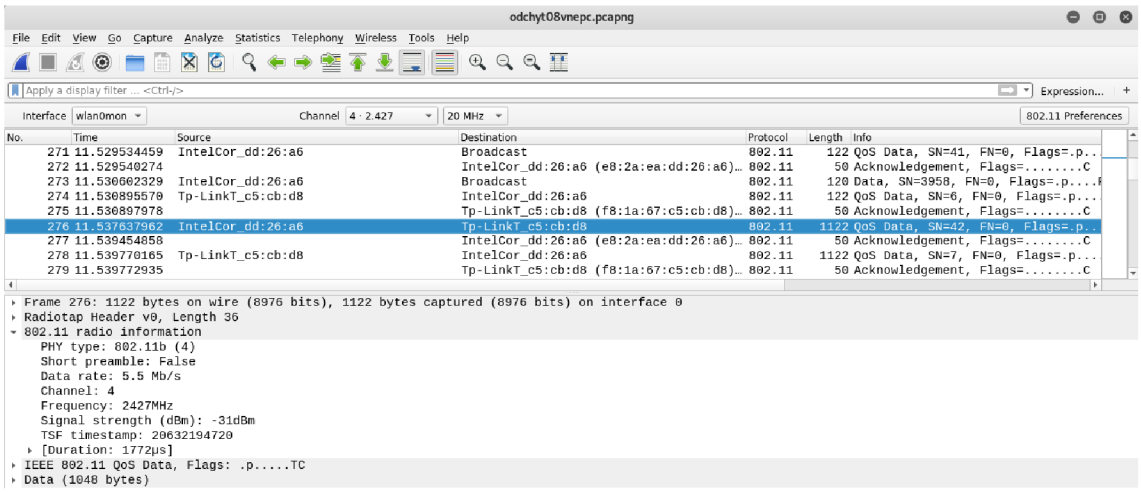
v příkazovém řádku systému Windows.

Odfiltrovat komunikaci patřící pouze klientské síťové kartě lze pomocí filtru:

```
wlan.sa == e8:2a:ea:dd:26:a6
```

2.1.3 Dešifrování IEEE 802.11 komunikace

Aby bylo možné dešifrovat komunikaci mezi zařízeními, je nutné znát zabezpečovací klíč a následně zachytit přihlašování stanice k přístupovému bodu. Po nalezení požadované stanice aktivním nebo pasivním skenováním klientské zařízení vyšle stanici (přístupovému bodu) žádost o autentizaci (Authentication request) na kterou stanice odpovídá buď kladně nebo zamítavě autentizační odpovědí (Authentication response). Po dokončení autentizace následuje asociační proces, který začíná stejně



Obr. 2.2: První zachycená, zabezpečená komunikace.

jako u autentizace klientská stanice vysláním rámce asociační žádosti (Association Request).

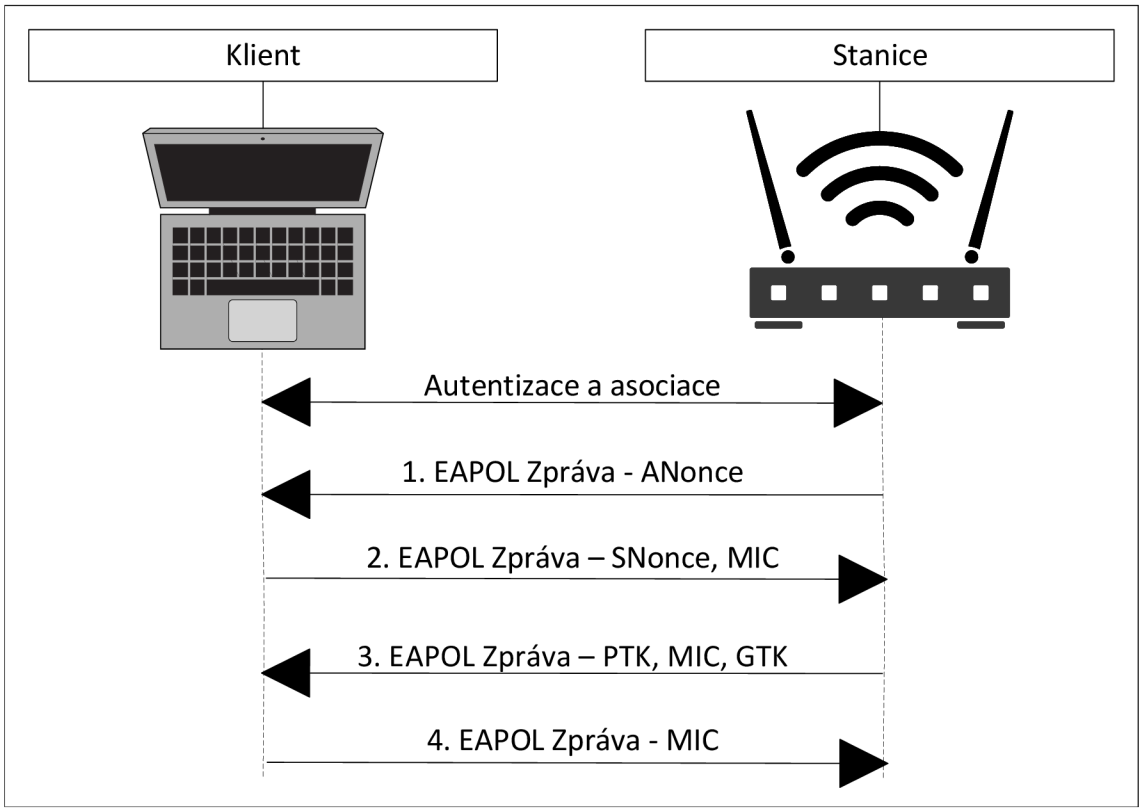
Dalším krokem v připojování stanice je vytvoření klíčů, pomocí kterých bude následný provoz zašifrován. Tento proces vytváření zabezpečovacích klíčů probíhá ve čtyřech zprávách, proto je nazýván čtyřcestný handshake (4-Way handshake) a probíhá ihned po dokončení autentizace a autorizace stanice v síti pomocí zpráv EAPOL (Extensible authentication protocol over LAN). Průběh těchto zpráv je znázorněn na Obr. 2.3.

V první zprávě přístupový bod pošle klientovi EAPOL zprávu, obsahující ANonce (náhodně vygenerované číslo) a další informace o typu šifrování (TKIP/AES). Klient následně vytváří PTK (Pairwise Transient Key) z ANonce, SNonce, své MAC adresy, z MAC adresy stranice a z PMK (Pairwise master key). PMK je klíč generovaný z klíče master relace (MSK). V případě WPA2/PSK, se PSK při autentizaci zařízení stává PMK.

Použité SNonce pro vytvoření PTK z minulého bodu posílá klient stanici ve druhé zprávě. Druhá zpráva obsahuje také kontrolu integrity zprávy pomocí MIC (message integrity check).

Třetí zpráva jdoucí od stanice ke klientovi obsahuje GTK (Group Temporal Key), který se využívá k šifrování veškerého přenosu směřujícímu od přístupového bodu k více klientským stanicím. GTK je klíč, který je sdílen mezi všemi klientskými zařízeními spojenými s 1 přístupovým bodem. Mimo GTK třetí zpráva obsahuje jako v předchozích zprávách ANonce, RSN Element a MIC.

Zpráva 4 je odeslána klientem. Je to poslední ze zpráv 4-Way Handshake. Tato závěrečná zpráva informuje přístupový bod o tom, zda byly časové klíče nainstalovány úspěšně nebo ne [23].



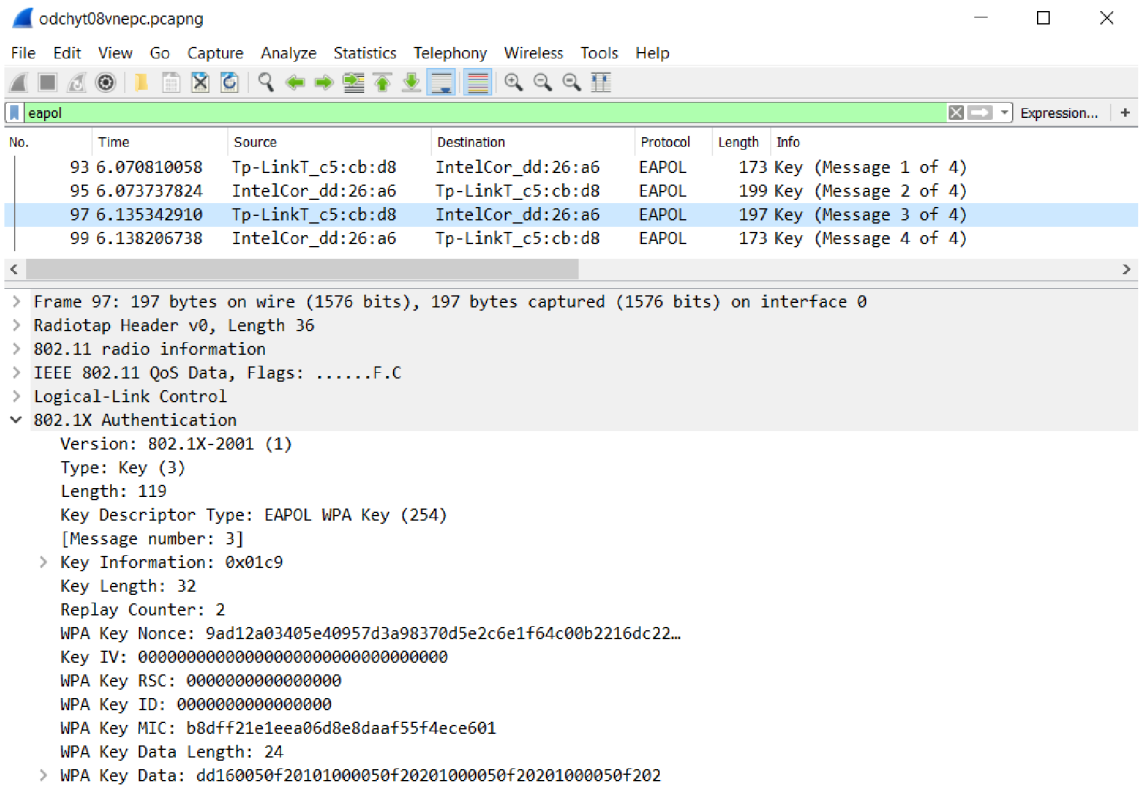
Obr. 2.3: 4-Way handshake.

Čtyřcestný handshake je zachycen na Obr. 2.4. Pro zobrazení autentizačních a autorizačních zpráv slouží ve Wiresharku filtr eapol.

2.1.4 Srovnání komunikace vně a uvnitř sítě

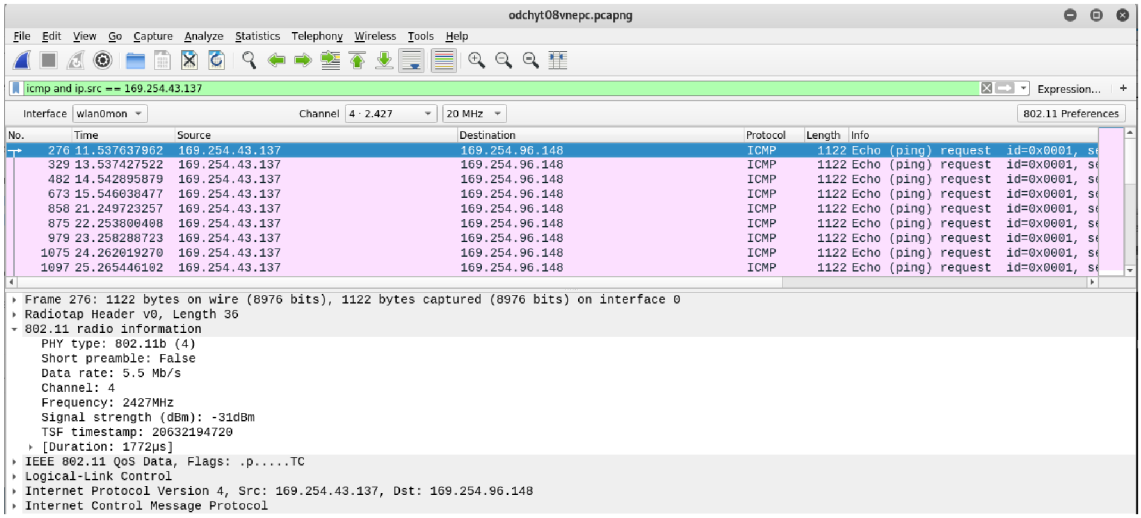
Po rozšifrování zpráv Wiresharkem se zobrazí komunikace na síťové úrovni (Obr. 2.5), která je srovnatelná s komunikací zachycenou na klientském počítači (Obr. 2.6). Hlavním rozdílem je, že v komunikaci pocházející z odposlouchávající strany je více rámců, které patří jiným zařízením v síti nebo pocházejí z jiných sítí. Lze si povšimnout, že ICMP pakety mají odlišnou velikost. To je způsobeno hlavičkou protokolu IEEE 802.11b, která je dlouhá 48 bitů a hlavičkou radiotap, což je prakticky kontejner pro doplňující data. Tyto data poskytují doplňující informace o zachycených paketech. Nejedná se o součást IEEE 802.11 standardu. Obě komunikace jsou uloženy v souborech a jsou k dispozici v adresáři "Zachycená komunikace/Kapitola 1"pod názvem uvnitr_site.pcap a vne_site.pcap.

Na Obr. 2.7 a Obr. 2.8 jsou grafy závislosti přenesených dat na čase vně a uvnitř sítě. Na Obr. 2.7 je znázorněn graf objemu veškeré komunikace ve čtvrtém kanálu. Přestože byl zvolen neobsazený kanál lze pozorovat, že se zde vyskytuje nejenom

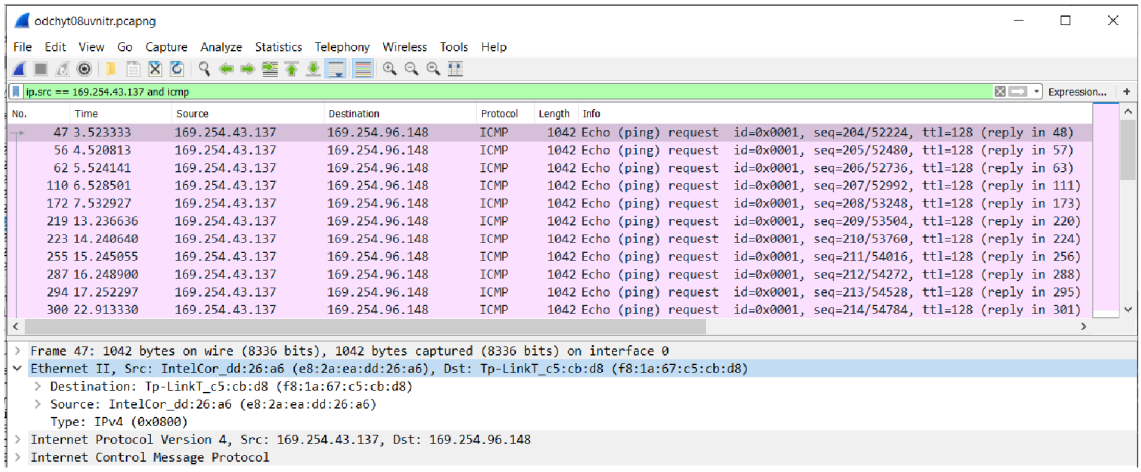


Obr. 2.4: 4-Way handshake zachycen ve Wiresharku.

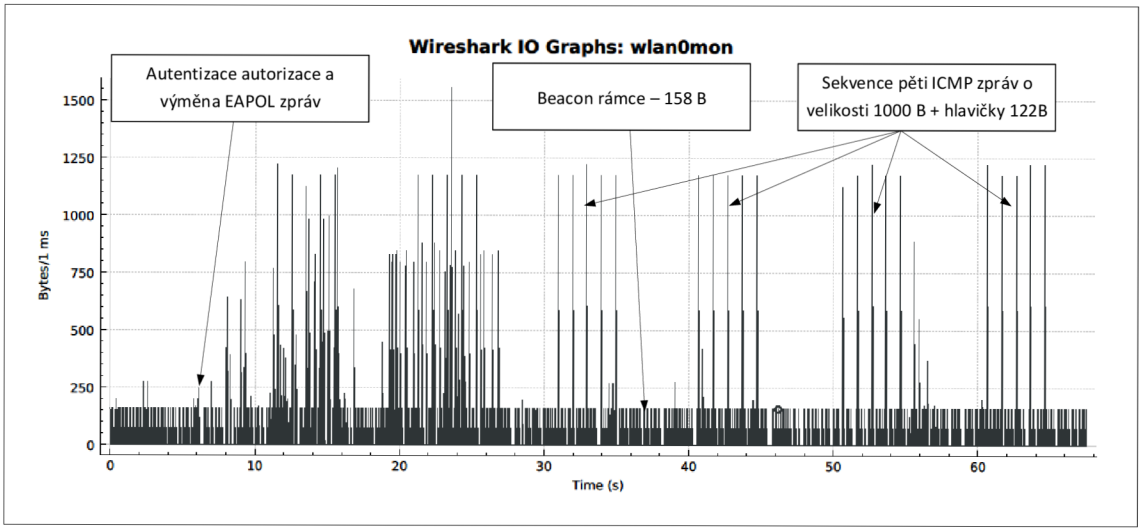
vygenerovaná komunikace klientskou stanicí, ale i rámce z jiných zařízení, nebo například všesměrová data. Největší zastoupení mají rámce beacon frame o velikosti 158 B. Rámce beacon frame jsou pravidelně vysílány přístupovým bodem a obsahují informace o síti. V grafu na Obr. 2.7 se nacházejí ve spodní části. Časové osy ve zmíněných grafech jsou odlišné, neboť Wireshark začíná počítat čas prvním zachyceným rámcem, což v případě rozhraní uvnitř sítě bylo o pár sekund později kvůli prodlevám při spouštění bezdrátového adaptéru a podobně.



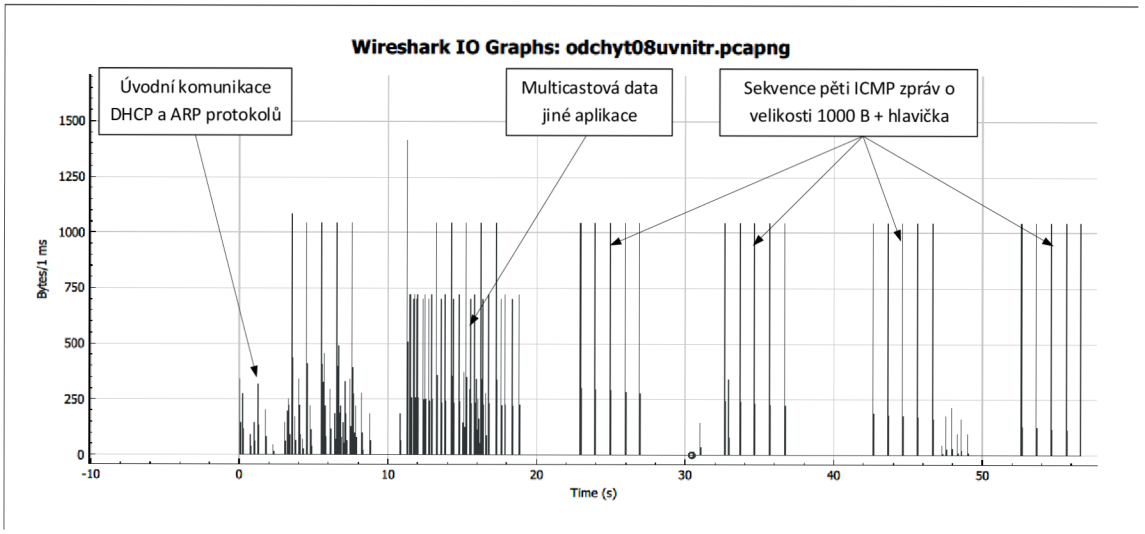
Obr. 2.5: Dešifrovaná komunikace zachycená monitorovací stanicí.



Obr. 2.6: Vyfiltrovaná komunikace zachycená klientskou stanicí.



Obr. 2.7: Graf závislosti objemu přenesených dat na čase pomocí zařízení vně sítě.

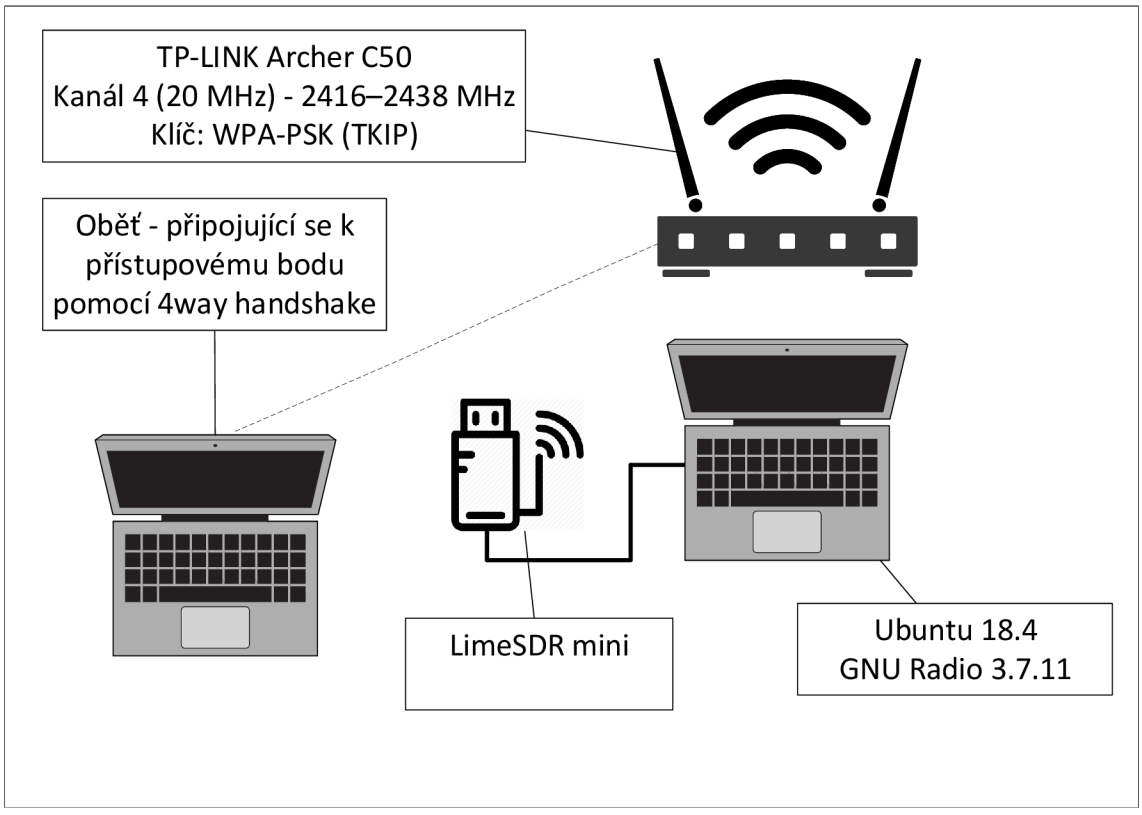


Obr. 2.8: Graf závislosti objemu přenesených dat na čase pomocí rozhraní uvnitř sítě.

2.2 Zachycení s pomocí LimeSDR mini

V této kapitole je opakován postup z předchozí kapitoly se záměnou bezdrátové karty za softwarově definované rádio LimeSDR mini. Bezdrátová karta byla nahrazena softwarově definovaným rádiem vzhledem k jejím limitům v přizpůsobitelnosti přijímaného signálu. Operace, které se vstupním signálem bezdrátová karta provádí jsou vykonávány převážně hardwarovými obvody a jejich modifikace je bez zásahu do jejich struktury neuskutečnitelná. SDR obsahuje programovatelná hradlová pole. Ty je možno patřičným softwarem jednoduše nastavit a přijímat tak jakýkoliv signál z podporovaného frekvenčního rozsahu SDR. S tímto signálem pak lze pracovat již na softwarové úrovni. Zpracování signálu probíhá s využitím výpočetního výkonu počítače. Tím poskytuje SDR široké možnosti k úpravě parametrů samotné komunikace, kdežto bezdrátová síťová karta je zde limitována na přednastavené hodnoty. SDR by mělo být teoreticky schopné přijímat více kanálů zároveň, nebo pro přenos využívat větší šířku pásma, či implementovat jinou modulační techniku.

2.2.1 Sestavení topologie



Obr. 2.9: Topologie odposlechu bezdrátové komunikace pomocí LimeSDR mini.

Topologie, jejíž schéma je na Obr. 2.9, byla oproti předchozí kapitole 2.1.1 upravena záměnou bezdrátové síťové karty za softwarově definované rádio. Druhým rozdílem je operační systém stanice zachytávající provoz. Důvody k výběru operačního systému budou vysvětleny dále v kapitole 2.2.3.

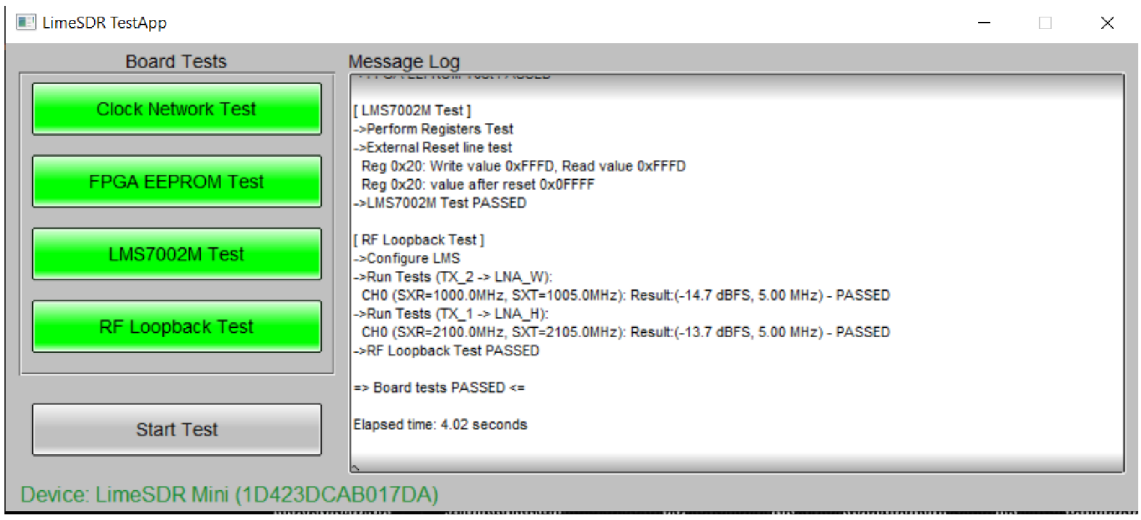
2.2.2 Instalace ovladačů a ověření funkčnosti ve Windows

Pro Windows 10 jsou poskytovány ovladače FTDI FT601 USB3.0. Ne vždy se však nainstalují automatiky a je nutné je manuálně nainstalovat. Při instalaci může nastat problém, kdy Windows považuje aktuální ovladač za optimálnější než instalovaný a tak ho jednoduše nenainstaluje. K tomu složí nástroj Zading, který zamění konkrétní ovladač za výchozí a je tak možné nainstalovat chtěný ovladač FTDI.

Před instalací virtuálního obrazu operačního systému je vhodné ověřit funkčnost zařízení a nainstalovaných ovladačů pomocí Pothos SDR dev enviroment balíku, který obsahuje základní software pro SDR:

- GNUradio
- GQRX
- CubicSDR
- LimeSuite

a pluginy potřebné ke komunikaci s LimeSDR. Většina programů však byla primárně vytvořena pro systém Linux a s jejich využití se počítá primárně v něm.



Obr. 2.10: LimeSDR aplikace testující funkčnost desky.

Prvním krokem bývá doporučováno ověření funkčnosti desky pomocí aplikace LimeQuickTest. Pozitivní výsledek lze zachycuje Obr. 2.10.

2.2.3 Příprava operačního systému Linux

Vzhledem ke složitosti instalace a potřebných nástrojů a programů na které je software GNUradio závislý je výhodné zvolit jako operační systém Linux. Při výběru distribuce byla zvažována distribuce Kali, která je určena pro penetrační testy a byla by tak vhodná pro s WiFi rámci. Bohužel však není podporovaná vývojáři SDR. Pro práci s SDR je nejpoužívanější distribucí Ubuntu. Vývojáři ovladačů a nástrojů SDR vydávají nové verze svého software pomaleji než vycházejí nové verze operačních systémů. To vytváří problémy s kompatibilitou. Následně bude uveden konkrétní soubor použitých programů.

Linux Ubuntu 18.4.4

Po zkušenostech s různými verzemi Ubuntu je verze 18.4.4 nejstabilnější a podporována všemi závislými programy z následující podkapitoly. Pro snadnější práci tak byl vytvořen virtuální obraz operačního systému za pomocí programu VirtualBox. S následujícími parametry:

Parametr	**Hodnota**
Operační paměť	4096 MB
Velikost disku	20 GB
Počet přidělených jader	4
Video paměť	128 MB
Akcelerace	3D
USB controller	xHCI

Tab. 2.2: Parametry virtuálního operačního systému Linux Ubuntu.

Pro pohodlnou práci je vhodné doinstalovat VirtualBox Guest Additions. Jedná se o sbírku ovladačů zařízení a systémových aplikací. Pomáhá zvyšovat výkon a použitelnost systému. Umožňuje sdílení složek, přetahování souborů a sdílení schránky mezi hostitelským a hostujícím operačním systémem a automaticky přizpůsobuje rozlišení virtuální obrazovky velikosti okna.

2.2.4 Instalace nástrojů

Před instalací programů a nástrojů z následujících podkapitol je nutné nainstalovat dlouhý seznam prerekvizitních nástrojů, které nejsou součástí systému Kali Linux. Těmito nástroji jsou například programy make a cmake, které vytvářejí spustitelné programů ze zdrojového kódu. Jednou z důležitých komponent je také knihovna Python, která musí být stažena.

LimeSuite

Lime Suite je soubor softwaru, podporující hardware vybraných SDR, ovladačů pro LIC7002M transceiver RFIC a dalších nástrojů pro vývoj pomocí hardwaru založeného na LMS7 [25].

USRP Hardware Driver

Aby bylo možné využívat některé knihovny a bloky GNUradia je potřebné doinstalovat rozhraní zvané USRP Hardware Driver (UHD). To podporuje všechny USRP a nabízí tak společné univerzální softwarové rozhraní, které je pro použití v SDR velkou výhodou. Není pak potřeba pro každý kus hardware psát nové algoritmy. Je tedy podporováno řadou vývojových prostředí jako RFNoC, GNU Radio, LabVIEW a Matlab/Simulink [26].

PyBOMBS

GNU Radio má díky složitosti instalace všech závislostí svého „manažera balíčků“ s názvem PyBOMBS. Je to nástroj, který pomáhá při instalaci GNU Radia, modulů a dalších softwarových balíčků V ideálním případě by nástroj jako PyBOMBS nebyl potřeba, ale každý operační systém a distribuce má jinou hierarchii a strukturu, jiné verze balíčků, kompilačního software a nástroj PyBOMBS by měl umět řešit většinu problémů za uživatele. Bohužel i tento nástroj ještě zdaleka není bezproblémový a uživatelky přívětivý. Tento projekt funguje teprve rok a brzy má přijít nová verze, která by mohla instalaci GNU radia usnadnit [27].

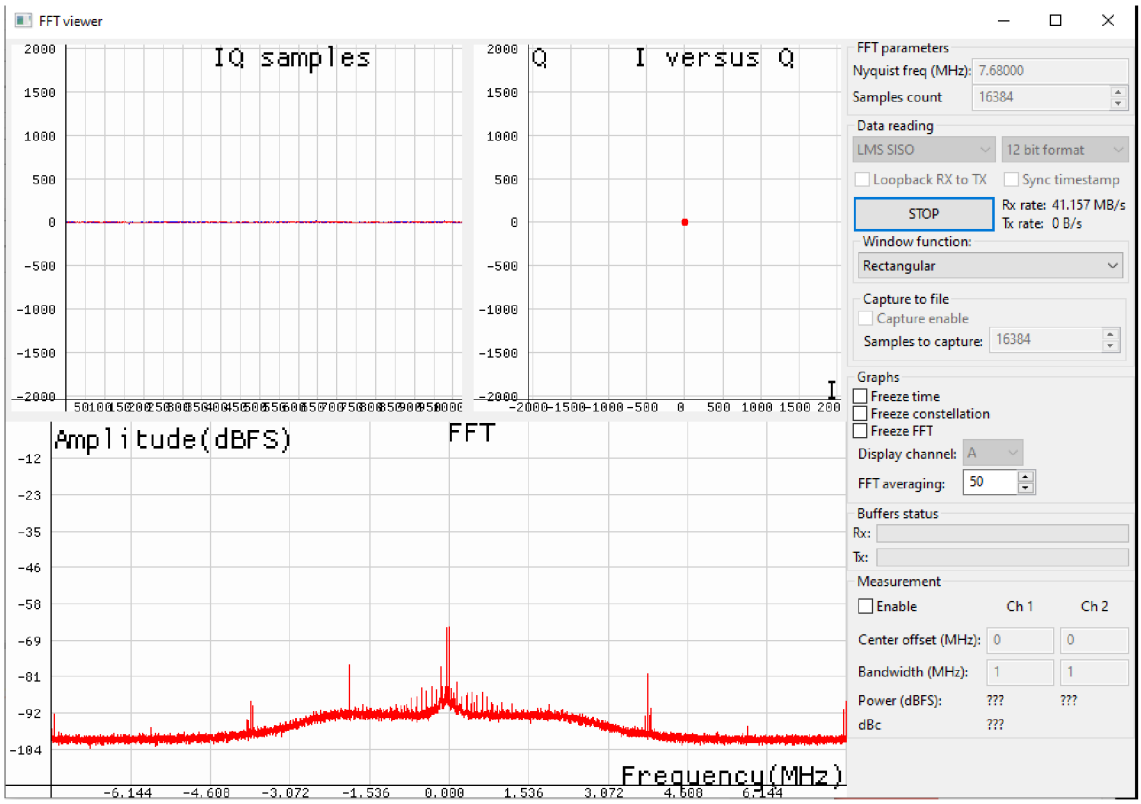
2.2.5 Testování funkcí v systému Windows

Tato kapitola bude shrnovat problematiku spojenou se zprovozněním konkrétního zařízení LimeSDR mini.

LimeSuite GUI

Základním nástrojem z balíčku Lime Suite je Lime Suite QUI. Po spuštění je v menu Options - ConnectionSettings možno zvolit kterou připojenou desku má program obsluhovat, jak se znázorněno na Obr. A.1.

Po zvolení připojeného zařízení lze tímto programem pro konfiguraci a ladění parametrů desky, načíst její aktuální stav, nebo ověřit její základní funkčnost, dále umožňuje prohlížet, upravovat, ukládat a načítat stav registrů LMS7002M, provádět aktualizace firmwaru deskového mikroprocesoru a FPGA. Další funkcí je generace signálu WCDMA a následné zobrazení prostřednictvím zpětné vazby a modulu FFT viewer. Zde se objevil první problém.



Obr. 2.11: Lime Suite GUI FFT viewer.

Jak lze vidět na Obr. 2.11, zpětnovazební test funkčnosti nezobrazuje žádný signál. Pouze šum na úrovni -90 dB.

Další funkcí Lime Suite GUI je automatická kalibrace desky, která bohužel v tomto případě končila pokaždé následující chybou.

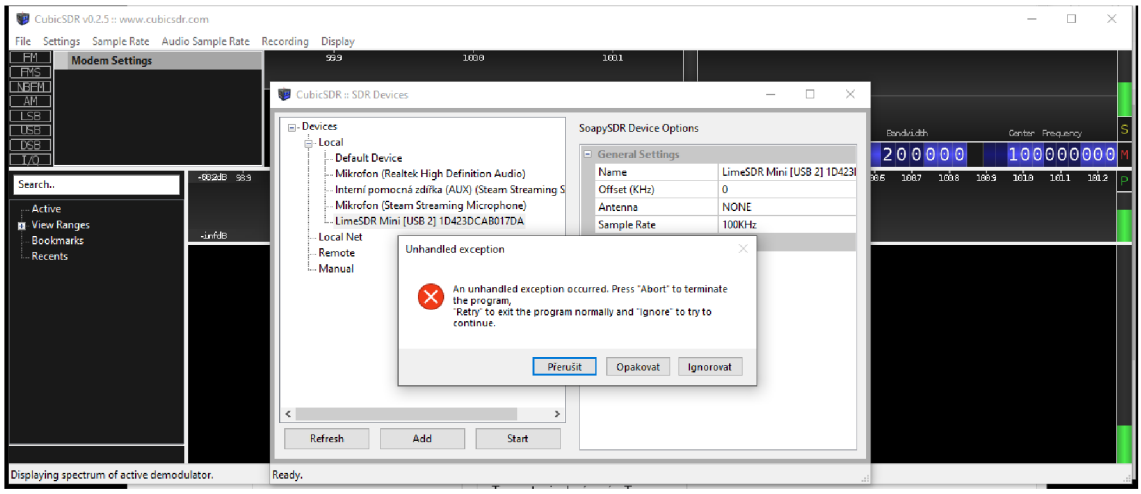
```
MCU error 4 (SXTtune failed)
```

PothosFlow

Dalším programem z balíčku Lime Suite je PothosFlow. Tento program má GUI umožňující uživatelům pomocí funkčních bloků graficky navrhovat schémata toku dat a následně je vykreslovat v implementovaných grafických widgetech. Na Obr. A.2 je však vidět chyba při pokusu o připojení k desce.

CubicSDR

CubicSDR je multiplatformní aplikace pro SDR, která umožňuje zobrazit rádiové spektrum a demodulovat různé signály. V současné době zahrnuje několik běžných analogových nemodulačních schémat, jako například AM a FM.



Obr. 2.12: Chybová hláška aplikace CubicSDR.

Naneštěstí ani tato aplikace nekomunikovala s využitým SDR. Po spuštění aplikace se zařízení LimeSDR mini načetlo do seznamu dostupných zařízení, nicméně po jeho zvolení se aplikace ukončila chybou viz Obr. 2.12.

GQRX

Posledním nástrojem využívaným pro prohlížení rádiového spektra pomocí SDR je program GQRX. Jako CubicSDR je multiplatformní a tudíž podporuje mnoho dostupných SDR.

Před spuštěním samotné aplikace se objeví dialogové okno pro nastavení parametrů připojeného zařízení, kterou je potřeba nastavit dle následující Tab. 2.3.

Parametr	**Hodnota**
Řetězec zařízení	driver=lime,index=0,media='USB 2',module=FT601, name='LimeSDR Mini',serial=1D423DCAB017DA,soapy=4
Vzorkovací frekvence	5 000 000 Hz
Decimační faktor	Žádný
Šířka pásma	2 500 000 Hz
Frekvence oscilátoru	0 Hz

Tab. 2.3: Parametry nastavení aplikace GQRX.

- Řetězec zařízení je řetězec parametrů pro ovladač sloužící jako identifikátor konkrétního hardwaru. Po vybrání LimeSDR mini z vybídky výše se toto pole předvyplní následujícím řetězcem.

  `driver=lime,index=0,media='USB␣2',module=FT601,`

```
name='LimeSDR Mini',serial=1D423DCAB017DA,soapy=4
```

- Vzorkovací frekvence definuje počet vzorků za jednotku času (obvykle za 1 sekundu) načítaných ze spojitého analogového signálu při jeho přeměně na diskrétní signál.
- Decimační faktor je jednoduše poměr vstupní rychlosti k výstupní rychlosti. Volně řečeno je decimace proces snižování vzorkovací frekvence. V praxi to obvykle znamená filtrování signálu s nízkou propustností a následné vyhození některých jeho vzorků. Operace je tedy podobná downsamplingu, který se týká pouze procesu vyhazování vzorků bez operace filtrování dolních frekvencí.
- Šířka pásma je rozmezí, ve kterém může SDR monitorovat rádiové spektrum. Jde o rozdíl mezi nejvyšší a nejnižší frekvencí kterou může zařízení v jeden okamžik pozorovat.
- Parametr frekvence lokálního oscilátoru (LNB LO) se využívá při zapojení down nebo up převodníku vřazeným před samotným zařízením. V opačném případě se hodnota nastavuje na 0 MHz.

Bohužel i tento program po zadání správných hodnot zamrzne a po chvíli se ukončí.

2.2.6 Testování funkcí v systému Ubuntu Linux

Jak již bylo řečeno SDR jsou nejčastěji používány se systémem Linux a od toho se také odvíjí softwarová podpora. Proto bylo další testování funkčnosti prováděno ve virtuálním systému Ubuntu Linux.

LimeQuickTest

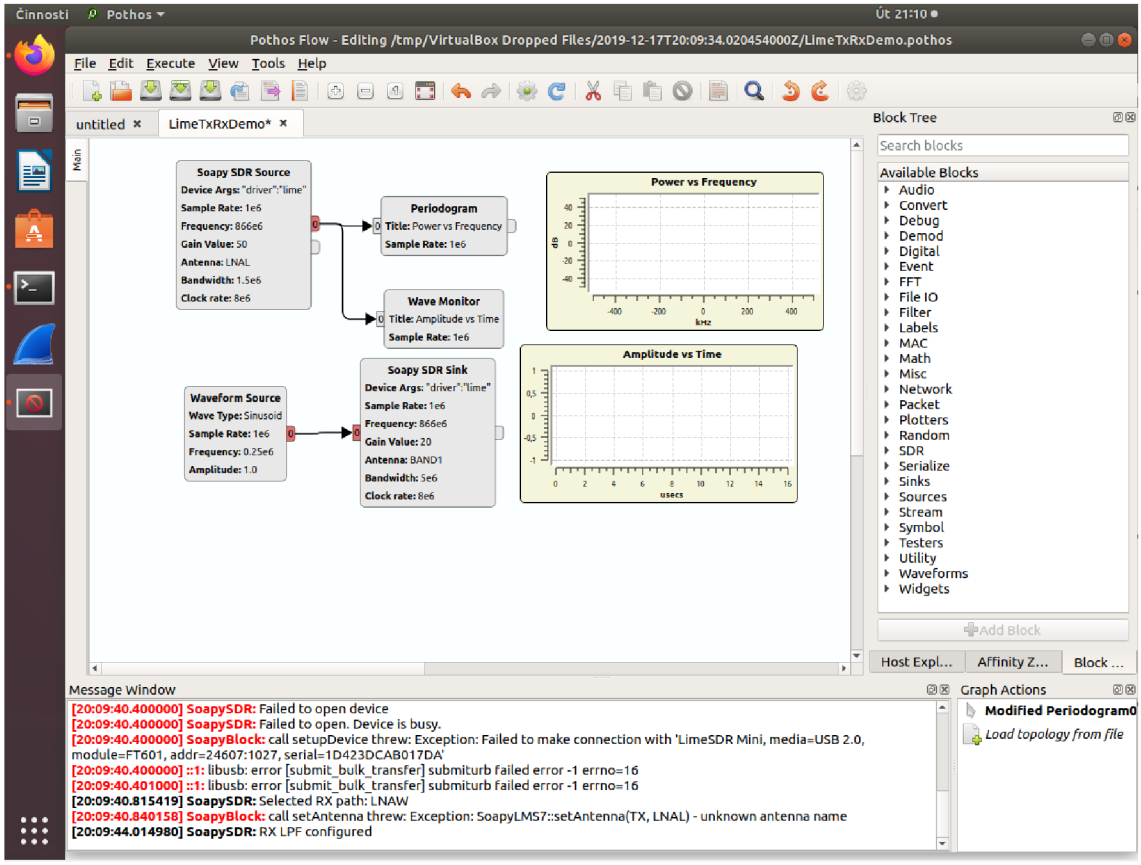
Jako první v testování bylo stejně jako ve Windows sekci spuštěno kontrolování funkčnosti desky programem LimeQuickTest. Výsledek v podobě textového výstupu lze vidět na Obr. B.1. Kontrola hardwaru proběhla v pořádku, avšak při pokusu o zpětnovazební smyčku nastala chyba. Znamená to tedy, že signál který se vysílá jednou anténou SDR, není zachycen druhou z antén.

Lime Suite GUI

Po prvním neúspěšném zpětnovazebném testu z programu LimeQuickTest se očekávatelně test smyčky v Programu Lime Suite GUI nepodařil. Jak lze vidět na Obr. B.2 nevidíme ani šum, který bylo možno pozorovat ve Windows aplikaci. Nejspíš se tedy jedná o problém přijímací části.

PothosFlow

Na Obr. 2.13 lze vidět stejný výsledek jako ve Windows prostředí na Obr. A.2. Chybová hláška oznamuje, že zařízení je zaneprázdněno a nelze k němu přistupovat, přestože v daném okamžiku zařízení není využíváno žádnou jinou aplikací.



Obr. 2.13: Error v logu aplikace PothosFlow.

CubicSDR

Program CubicSDR ve virtuálním operačním systému po svém spuštění a načtení dostupných zařízení vyvolal chybu končící pádem celého systému Linux. Chybová hláška popisovala vždy problém některé Instrukce, která odkazovala na neplatnou část paměti. Na Obr. 2.12 je zachycen screenshot před pádem virtuálního systému.

GQRX

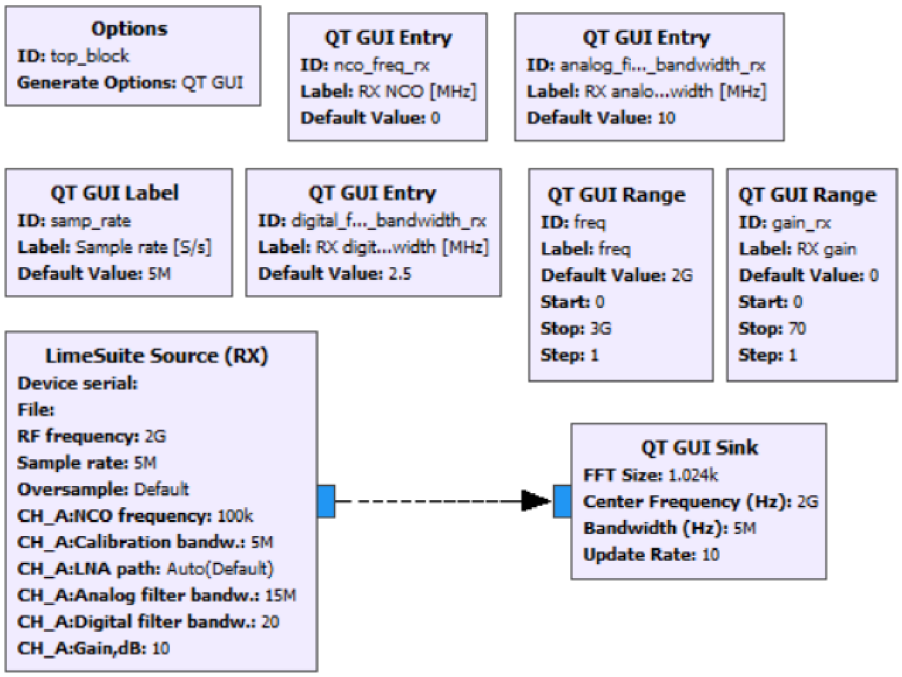
Stejně jako předchozí aplikace, tak i aplikace GQRX v Linuxovém prostředí byla neúspěšná při pokusech o připojení k desce SDR. Podle webového návodu [28] byly nastaveny parametry programu na hodnoty v Obr. B.4.

2.2.7 GNU Radio

Přestože se nepodařilo plně zprovoznit funkci SDR, byl sestaven projekt pro primární zobrazení signálu v daném úseku spektra.

První projekt GNU Radia

Pro základní ověření funkčnosti v programu GNU radio byl vytvořen jednoduchý projekt pro grafické zobrazení obsahu frekvenčního rozsahu. Parametry upravující zobrazené spektrum je možno upravovat pomocí sliderů za běhu programu. Na Obr. 2.14 je schéma vytvořeného projektu.

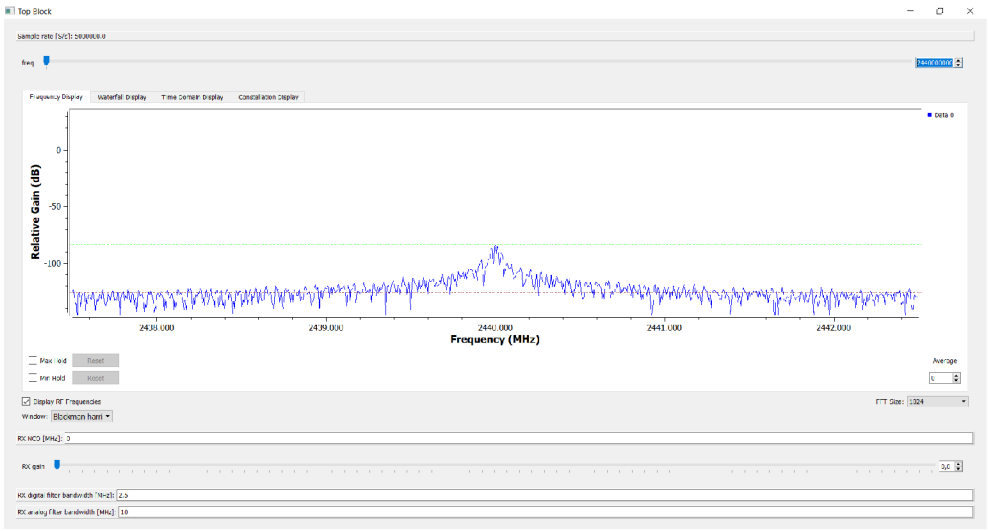


Obr. 2.14: Prvotní testovací projekt v GNUrádiu pro zobrazení spektra.

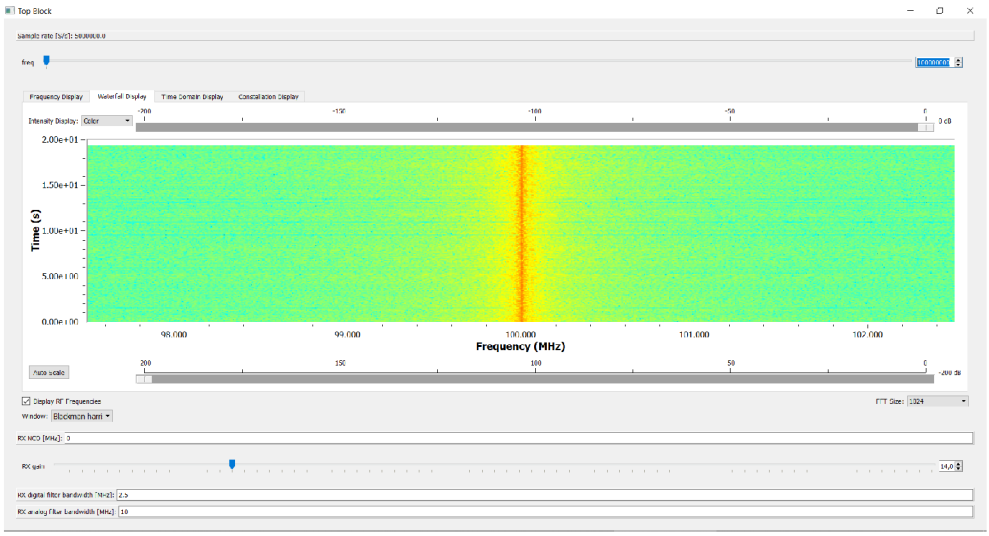
Na Obr. 2.15 a Obr. 2.16 lze pozorovat výstup ze SDR naladěného v prvním případě (Obr. 2.15) na frekvenci 2440 MHz, kde by měl být viditelný signál vysílaný bezdrátovým přístupovým bodem TP-LINK, avšak žádný signál zde pozorovatelný není. U Obr. 2.16 je situace obdobná jen pro frekvence v okolí 100 MHz, kde by se měly zobrazovat jednotlivé rádiové stanice, nicméně jak je zde patrné, SDR nepřijímá žádný signál.

Modul gr-rftap

GNU Radio disponuje blokem Wireshark connector, který dokáže transformovat vstupní řetězec zpráv do formátu .pcap se kterou umí pracovat nástroj Wireshark.



Obr. 2.15: Zachycený šum ze zařízení LimeSDR.



Obr. 2.16: Waterfall diagram vytvořen v GNUradiu.

Tento postup ukládá data do souboru, který lze po ukončení běhu programu spustit. Mnohem praktičtější však je zachytávat pakety v reálném čase. Proto je nutné doinstalovat do GNU Radia modul s názvem gr-rftap. Tento modul přidá do GNU Rádiového stromu dva bloky jež umožňují vytvořené pakety zasílat na definovanou IP adresu. Pro jednoduchost lze nastavit loopback adresa 127.0.0.1. Následně otevřít Wireshark se zachytáváním toho rozhraní. V Linuxu je pro přístup k těmto prostředkům nutné spustit Wireshark s právy root uživatele.

Modul gr-limesdr

Modul gr-Limesdr slouží ke konfiguraci a komunikaci se samotným SDR. Modul obsahuje dva bloky. Jeden pro příjem a druhý pro vysílání signálu. Blok LimeSuite Source je zdrojem dat pro GNU Radio, jedná se tedy o přijímač signálu z bezdrátového spektra. Zajišťuje konfiguraci přijímacích parametrů jako kmitočet, zisk a jiné parametry. Na výstupu tohoto bloku je řetězec datového typu 32 bitový komplexní float. Druhým modulem je LimeSuite Sink, který naopak dovoluje signál vysílat. Jeho parametry jsou podobné těm u vysílacího bloku.

Modul gr-IEEE802.11

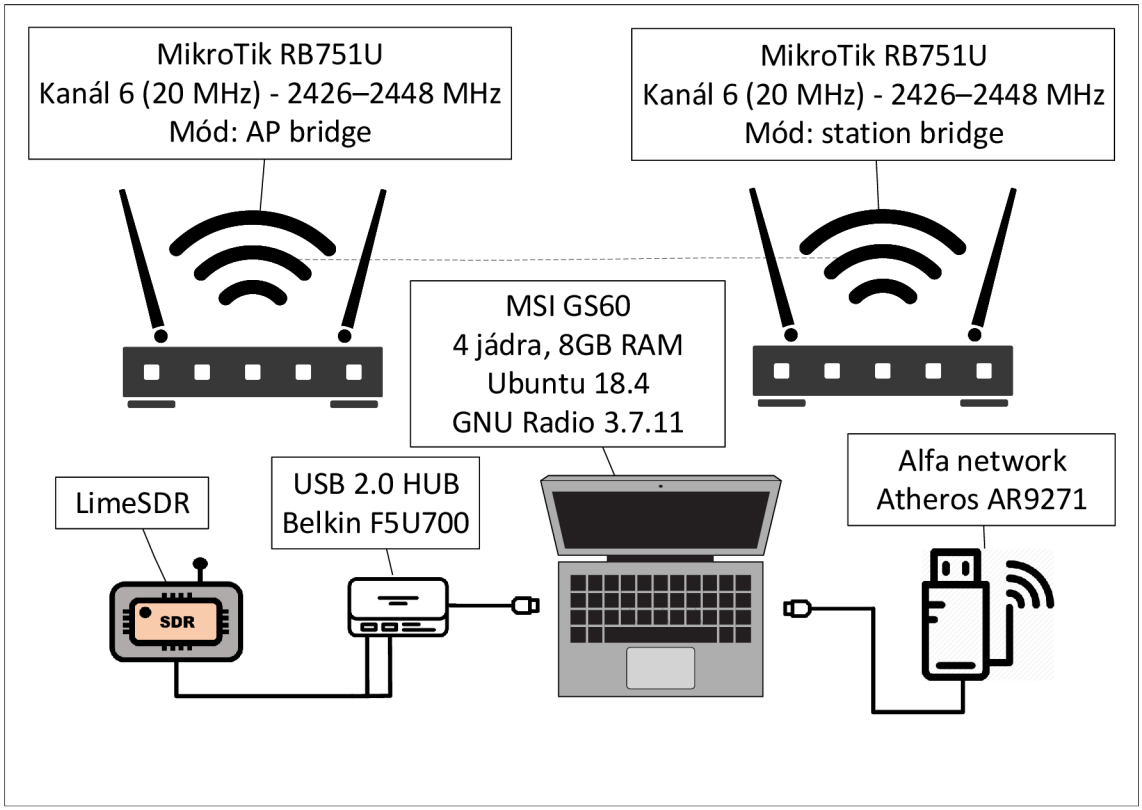
Využít GNU Radio za účelem zachytávání bezdrátové komunikace IEEE 802.11 lze pomocí modulu gr-802.11, který je možné nainstalovat pomocí instalace ze zdrojových souborů. Všechny soubory k tomu potřebné jsou uloženy na webových stránkách Githubu. Projekt je pojmenován IEEE 802.11 a/g/p Transceiver. Projekt vytvořil německý výzkumník Dr. Bastian Bloessl. Před prvním spuštěním tohoto projektu je nutné nejprve spustit projekt wifi_phy_hier.grc. Dalším krokem k ověření instalace je projekt wifi_loopback.grc, ten po spuštění vytváří řetězec definovaných zpráv, které jsou převedeny na signál a následně zpět dekódovány. Nevýhodou tohoto projektu je omezení pouze na doplňkové standardy IEEE 802.11a/g/p. Pro funkci tohoto modulu je také zapotřebí nainstalovat modul gr-foo, který obsahuje některé bloky potřebné v projektu. Instalace probíhá stejným způsobem jako u předchozích, tedy ze zdrojových souborů.

2.3 Zachycení s pomocí LimeSDR

Kvůli komplikacím se zařízením LimeSDR mini z minulé kapitoly se přešlo k analýze bezdrátové komunikace pomocí SDR s označením LimeSDR-USB, které by mělo plně podporovat USB 3.0 a mělo by tedy fungovat bezproblémově.

2.3.1 Sestavení topologie

Se změnou zachytávajícího zařízení se musela upravit i předchozí topologie. Jako zdroj komunikace byly tentokrát vybrány dva MikroTik routery s označením RB751U, vybaveny bezdrátovými síťovými kartami Atheros AR9283. Bezdrátová síťová karta byla zaměněna za LimeSDR. Topologii znázorňují Obr. 2.17 a Obr. 2.18.



Obr. 2.17: Topologie odposlechu bezdrátové komunikace s LimeSDR.

Další změnou oproti topologii v kapitole 2.2 je přidání USB 2.0 aktivního rozbočovače Belkin F5U700. Tento byl do topologie vřazen kvůli problémům se stabilitou programu ve virtuálním Ubuntu a také z důvodu vyššího proudového odběru SDR. Právě díky vyšším nárokům na odběr se LimeSDR dodává s Y-rozdělovacím kabelem pomocí kterého lze sloučit výkon dvou USB portů do jednoho. Použití USB rozbočovače je ostatně doporučeno i na stránkách výrobce [29]. Z předchozí topologie

v kapitole 2.1.1 zůstala monitorovací bezdrátová síťová karta Alfa network s kartou Atheros AR9271 sloužící ke srovnání zachycených paketů, jako v minulém scénáři.

Obr. 2.18: Reaálná topologie odposlechu bezdrátové komunikace s LimeSDR.

Konfigurace routeru

Routery MikroTik byly vybrány díky pokročilým možnostem nastavení parametrů bezdrátové komunikace. Pro jednoduchost se upustilo od zabezpečení komunikace a nastavení zabezpečení bylo ponecháno otevřené. Konkrétní parametry viz Tab 2.4. Následně byl mezi routery spuštěn nekonečný ICMP ping s jednosekundovým intervalem a velikosti 1000 B.

Konfigurace stanice

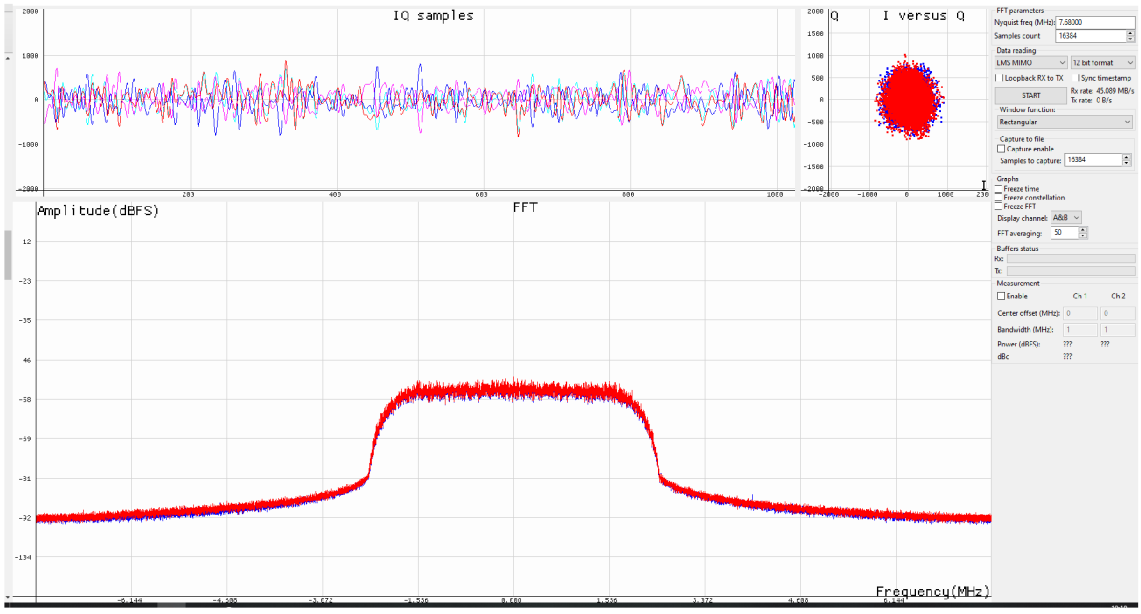
Zde byl použit přenosný počítač MSI s označením GS60 osazený čtyř-jádrovým procesorem i7-4710HQ s taktovací frekvencí 2,5 GHz, 8 GB operační paměti RAM s přístupem DDR3 a harddiskem Samsung SSD 850 EVO. Nativním operačním systémem byl 64 bitový Windows 10 Pro. Na počítači byl nainstalován software VirtualBox 6.1.4, který v tomto případě umožňuje virtualizovat operační systém Linux Ubuntu 18.4.4.

Tab. 2.4: Parametry přístupového bodu.

Parametr	Hodnota
Standard:	IEEE 802.11g
SSID:	MikroTik-PODO
Kanál:	6
Frekvence	2426–2448 MHz
Šířka pásma:	20 MHz
Typ zabezpečení:	-
Typ šifrování:	-

2.3.2 Kalibrace zařízení

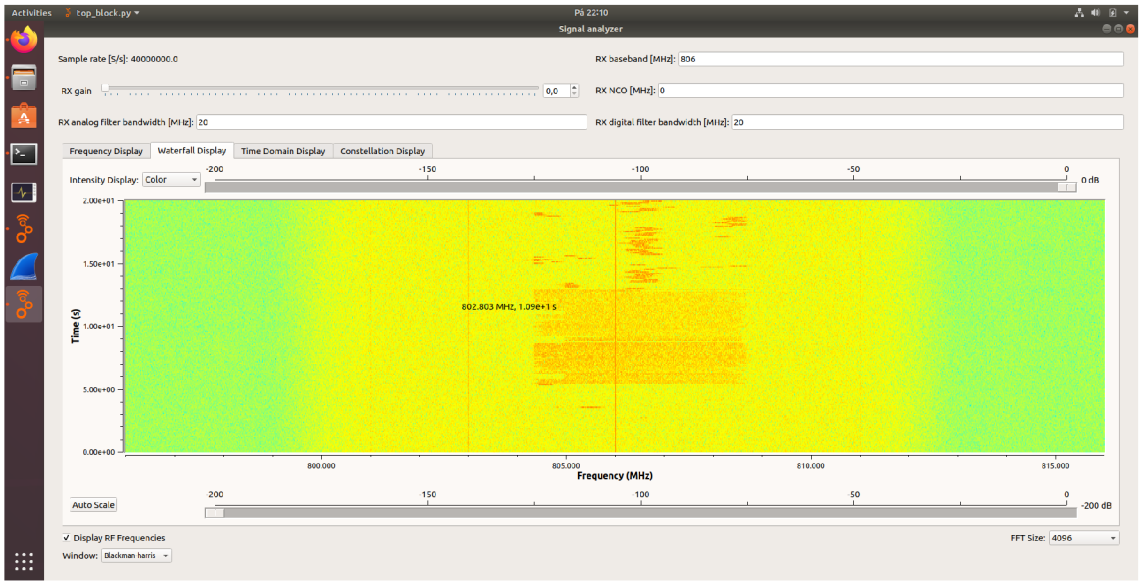
Po aktualizaci základní desky se před zahájením práce se SDR výrobcem doporučuje provést kalibraci desky s pomocí softwaru LimeSuite a následně provést jednoduchý loopback test vysíláním W-CDMA (širokopásmový vícenásobný přístup s kódovým dělením) signálu TX větví a jeho současného příjímání RX větví zařízení. Na Obr. 2.19 je výsledek tohoto testu. Výsledný, přijatý signál se shoduje s vyslaným, a je tak ověřena funkčnost, nastavení a kalibrace desky LimeSDR [29].



Obr. 2.19: Výsledek loopback testu ve spektrálním zobrazení.

2.3.3 Ověření funkčnosti GNU Radia s ostatními komponenty

Aby bylo potvrzeno správné propojení s hardwarovým zařízením a ověřena funkčnost všech modulů, byl vytvořen projekt obsahující pouze zdroj signálu a jeho GUI zobrazovač. Prakticky se jedná o digitální spektrální analyzátor, s jeho pomocí lze sledovat signály z různých částí rádiového spektra. Například při znalosti RF Channel Number (číslo kanálu) buňky e-NodeB (základnové stanice systému LTE) ke které je připojen mobilní telefon, lze snadno dohledat které frekvence tomuto kanálu odpovídají a zaměřit se pomocí SDR ne ně.



Obr. 2.20: LTE signál zachycen na waterfall grafu pomocí LimeSDR.

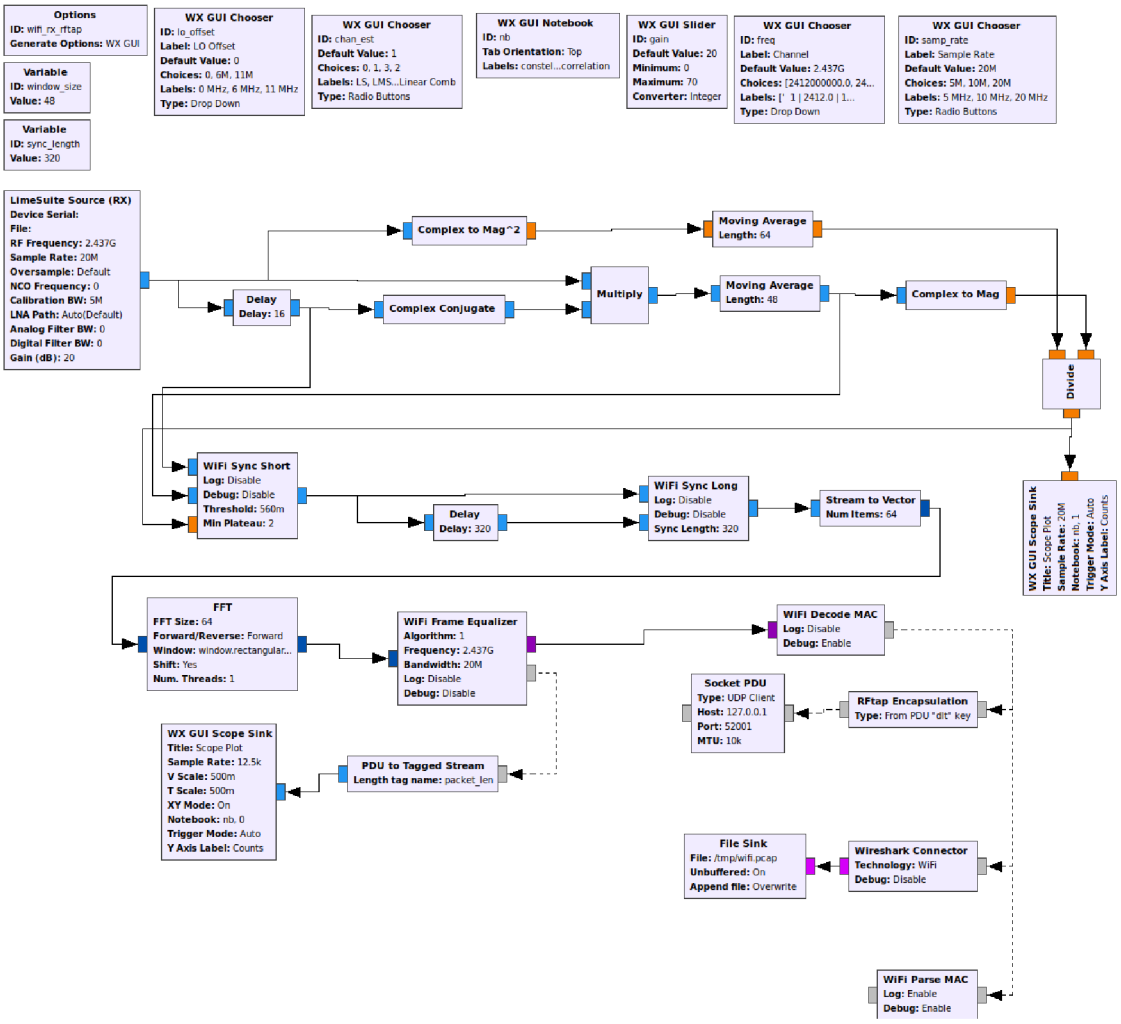
Na Obr. 2.20 je zachycen LTE signál. Tento průběh byl docílen spuštěním testu rychlosti připojení. V první části je LTE download s využitím modulace OFDMA (ortogonální multiplex s frekvenčním dělením) a následně LTE upload s modulací SC-FDMA (frekvenčně dělený vícenásobný přístup na jedné nosné).

Dále byl pro demonstraci možností programu GNU Radio spuštěn příkladový projekt přijímače RDS a FM rozhlasového rádia. Tento projekt po vyladění zisku a frekvence fungoval a z reproduktorů hrálo místní rozhlasové rádio.

Pro ujištění, že SDR pracuje v potřebném rozsahu, tedy 2,4 GHz, byl tento základní testovací projekt nastaven na konkrétní frekvenci kanálu, na kterém vysílá router z připravené topologie na Obr. 2.17. Při jeho vytížení bylo pozorovatelné, jak OFDM modulace využívá celé 20 MHz pásmo.

2.3.4 Spuštění projektu pro zachytávání komunikace IEEE802.11

Po ověření funkčnosti příjmu signálu v kýženém frekvenčním rozsahu byl otevřen projekt pro příjem komunikace standardem IEEE 802.11 jehož flowgraph (blokové schéma) je na Obr. 2.21.



Obr. 2.21: Projekt GNU Radia z balíčku gr-802.11

Jedinou změnou oproti původnímu projektu je zdrojový blok. Výchozím zdrojovým blokem byl totiž USRP blok pro zařízení od společnosti Ettus Research. Po prvním rozběhnutí program bohužel do stavového okna vypisoval pouze hlášku

```
LONG: frame start at 320
```

která znamená, že diagram nerozpoznává žádné rámce. Následovalo dlouhé nastavování dostupných parametrů, jako zisk, obnovovací frekvence, algoritmus pro odhad kanálu, offset a po jejich vyladění podle konstalačního diagramu se podařilo zachytit ACK rámce délky 84 bajtů se zdrojovou MAC adresou MikroTiku. Příjem ACK paketu je doporvázan konzolovým výpisem:

Výpis 2.1: Část konzolového výpisu při zahazování rámce

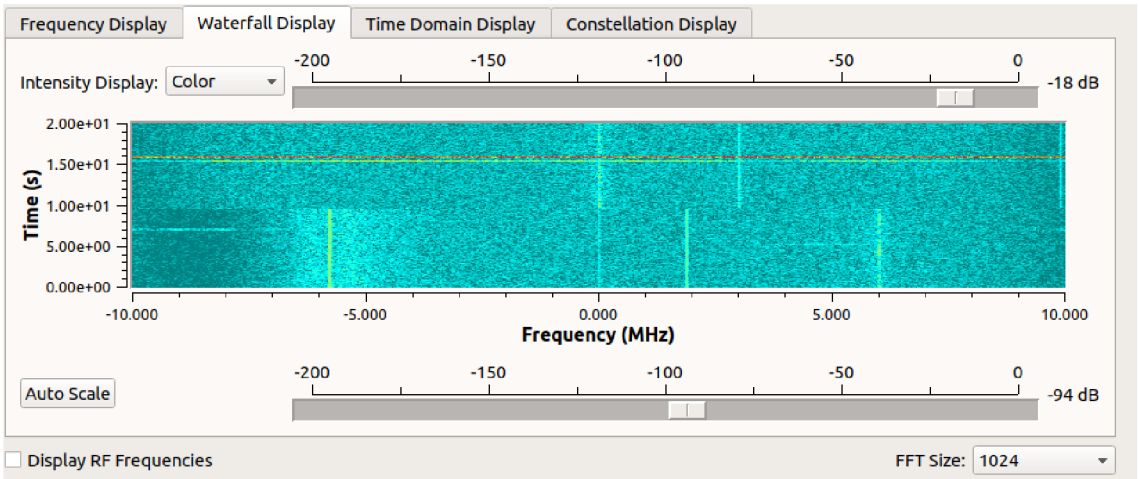
```
new mac frame  (length 10)
========================================
frame too short to parse (<20)
encoding: 2- length-14 symbols:3
length:10
```

Výsledky jsou uloženy v souborech na přiloženém médiu v adresáři "/Zachycená komunikace/LimeSDR/2.3.4"pod názvem SDR.pcap a karta.pcapng. Přiložen je i konzolový výpis v souboru log.txt.

Kompenzace stejnosměrné složky

Projekt disponuje volbou lo_offset, která nabízí volbu jedné z hodnot 0 MHz, 6 MHz a 11 MHz. Tato možnost je zde pro odstranění, nebo lépe přesunutí, stejnosměrné špičky uprostřed sledovaného okna. Tento jev je u SDR zcela normální. Je způsoben nenulovým napětím mezi tunerem a ADC na základní desce SDR. Většina softwaru pro ovládání SDR má možnost kompenzovat DC složku softwarově, to ale v GNU Radiu implementováno není.

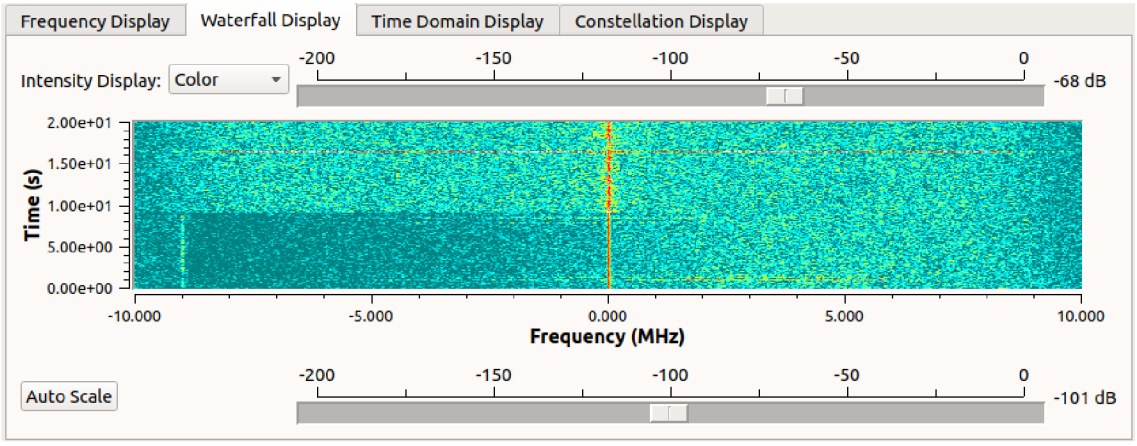
Na Obr. 2.22 je na waterfall grafu znázorněno jak v čase 10 sekund byla přepnuta hodnota z 0 MHz na hodnotu 6 MHz, čímž se DC offset přesunul z oblasti centrální frekvence. Stupnice na ose x v Obr. 2.22 je zavádějící, rozsah okna je samozřejmě nastaven na frekvence, kde komunikují použitá zařízení, zde konkrétně 2427 MHz až 2447 MHz.



Obr. 2.22: Spektrum signálu v požadované oblasti 2,4 GHz s posunutou centrální frekvence o 6 MHz.

I přes tuto úpravu však konzolové okno vypisovalo stejnou hlášku a žádné pakety

nebyly detekovány. Výsledky jsou uloženy v souborech na přiloženém médiu v adresáři "/Zachycená komunikace/LimeSDR/2.3.4"pod názvem SDR_offset_6MHz.pcap a karta_offset_6MHz.pcapng. Přiložen je i konzolový výpis v log_offset_6MHz.txt.

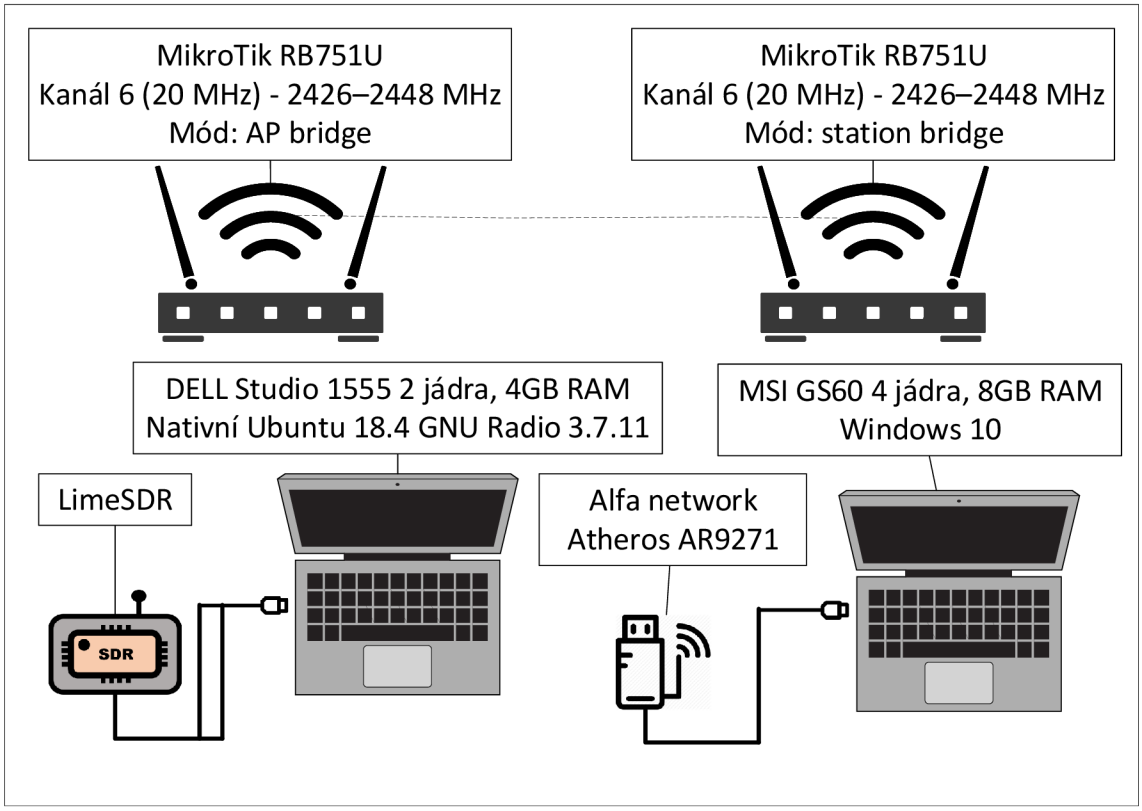


Obr. 2.23: Spektrum signálu v požadované oblasti 2,4 GHz s posunutou centrální frekvence o 11 MHz.

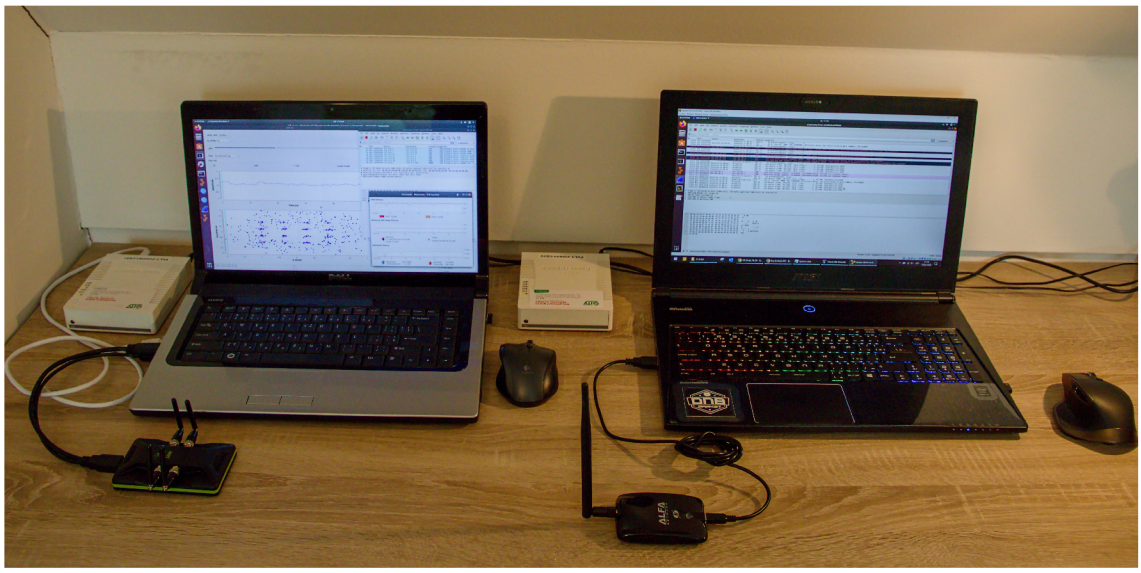
Stejná situace nastala při spuštění zachytávání s offsetem nastaveným na hodnotu 11 MHz přestože byla stejnosměrná špička posunuta mimo rozsah zájmu, který sahá 10 MHz nad a pod centrální frekvenci, jak je patrné z Obr. 2.23. Výsledky jsou uloženy v souborech na přiloženém médiu v adresáři "/Zachycená komunikace/LimeSDR/2.3.4"pod názvem SDR_offset_11MHz.pcap a karta_offset_11MHz.pcapng. Přiložen je i konzolový výpis v souboru log_offset_11MHz.txt.

2.3.5 Nativní Linux 18.04

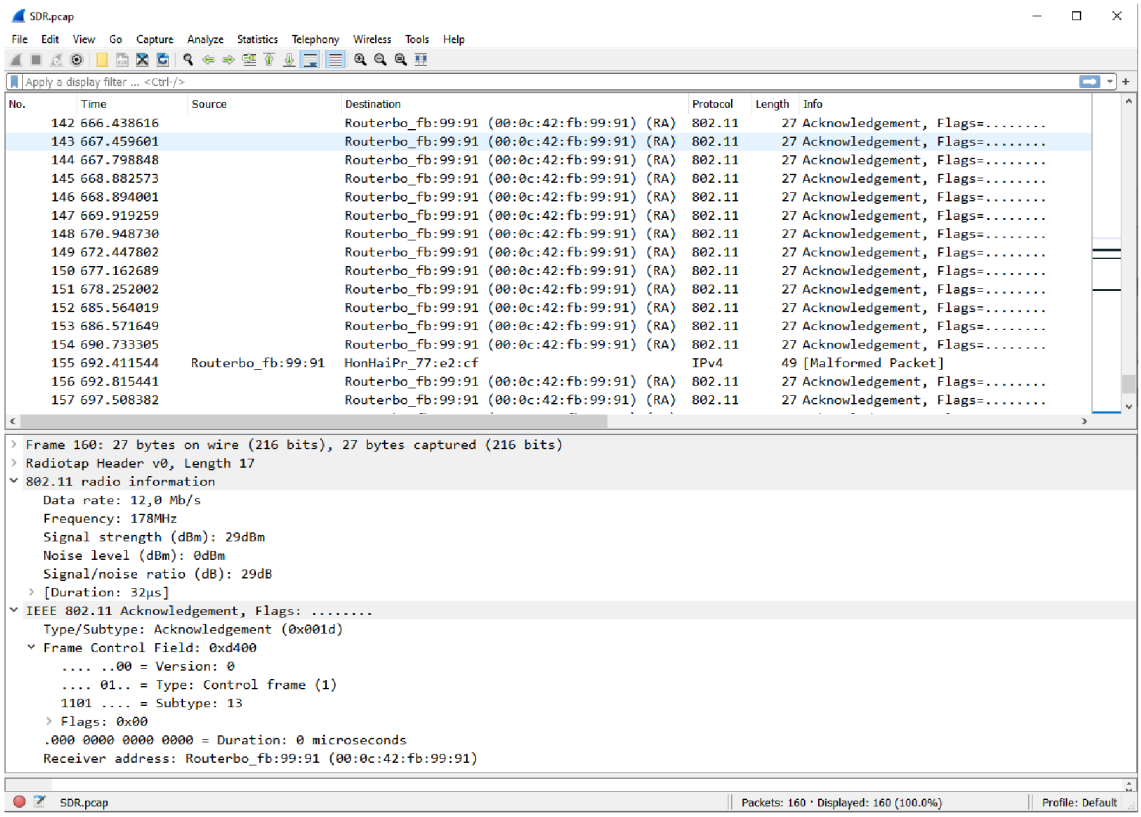
Jedním z důvodů, který by mohl způsobovat potíže s příjmem vyslaných paketů je použití virtualizovaného operačního systému. Byl tedy vybrán náhradní notebook, na který byl po vzoru virtuálního systému nainstalován systém nativní se všemi moduly. Jednalo se o notebook DELL Studio 1555 s dvou-jádrovým procesorem Core2Duo a 4 GB operační paměti. Tyto parametry jsou však pro účely tohoto projektu hrubě nedostačující. Výsledky však byly srovnatelné s těmi z předešlého pokusu s virtuálním Linuxem. Zatímco bezdrátová síťová karta Alfa network zachytila 36000 paketů, LimeSDR jich zachytilo pouze 160. Navíc se jednalo pouze o pakety ACK. Na Obr. 2.26 je snímek obrazovky programu Wireshark, zobrazující zachycené pakety.
Již při pohledu na měřítka grafu (Obr. 2.27) lze konstatovat řádový rozdíl objemu zachycených paketů a to po celou dobu zachytávání. Výsledky jsou uloženy v souborech na přiloženém médiu v adresáři "/Zachycená komunikace/LimeSDR/2.3.5"pod názvem SDR.pcap a karta.pcapng. Přiložen je i konzolový výpis v souboru log.txt.



Obr. 2.24: Topologie odposlechu bezdrátové komunikace s použitím jiného počítače.



Obr. 2.25: Reálná topologie s počítačem DELL.



Obr. 2.26: Wireshark zobrazující výsledky z GNU Radia.

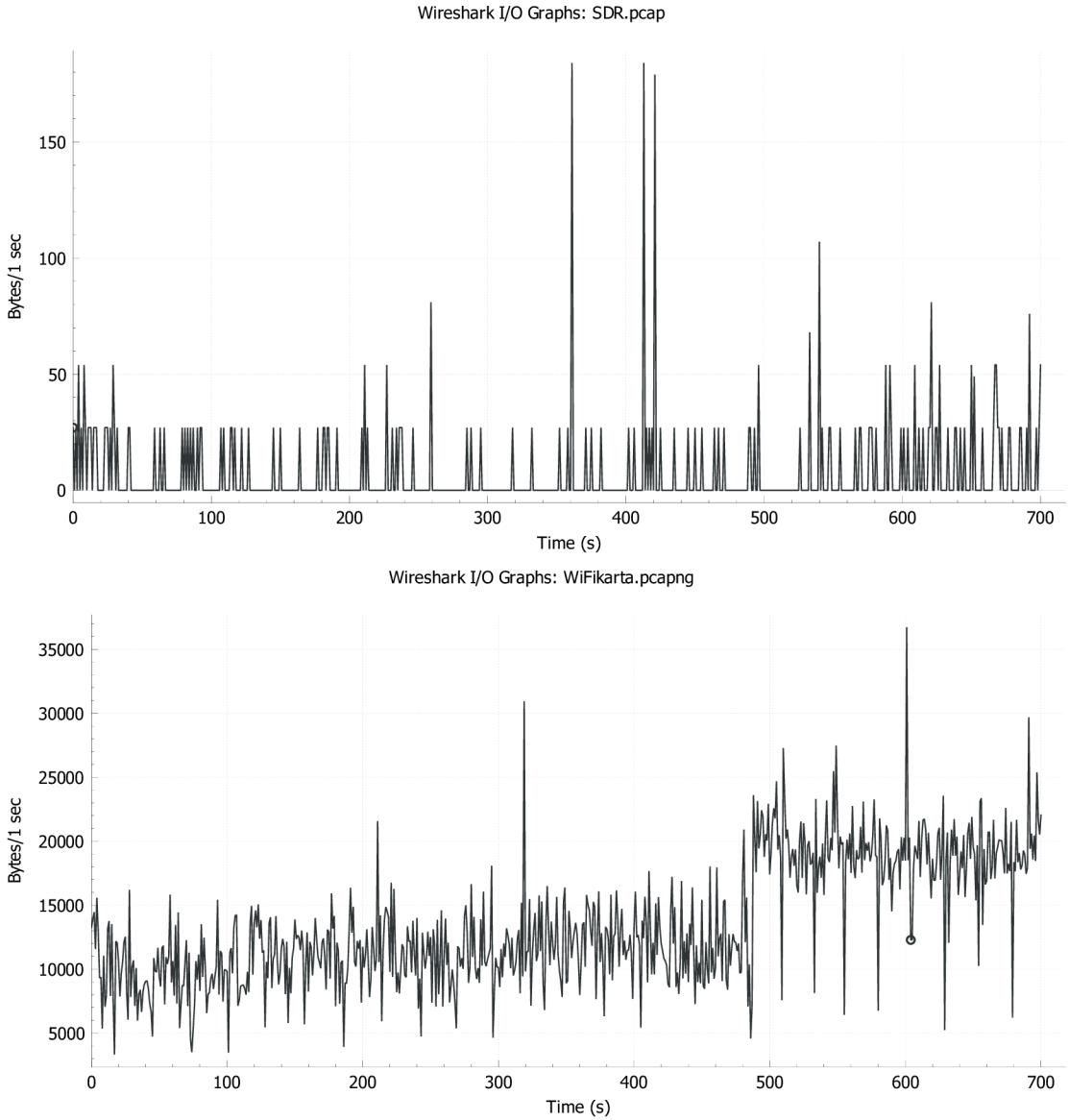
2.3.6 GNU Radio Live SDR Environment

Zmíněné problémy může způsobovat použití virtuálního operačního systému. Pro tyto případy existuje připravený "živý"systém Linux GNU Radio Live SDR Environment. Tento živý obraz Ubuntu verze 16.04.2 lze s pomocí vhodného programu nainstalovat na flash disk a následně z něj bootovat systém. Po spuštění lze ihned spustit GNU Radio s množstvím předinstalovaných modulů, včetně gr-IEEE802.11. Bylo potřeba doinstalovat jen gr-limesdr modul. Nicméně i v tomto případě tento postup problém nevyřešil a výsledky byly znova nedostačující. Vytížení procesoru nepřekračovalo hranici 80% a nebylo nutné použít USB rozbočovač.

2.3.7 Ukládání datového toku do souboru

Dalším tipem pro zmírnění zátěže počítače bylo datový tok ze zařízení nejprve ukládat do souboru a následně z něj tok streamovat do dekódovacího projektu. V GNU Radiu jsou k ukládání a čtení ze souboru určeny bloky File Sink a File Source. Během necelé minuty nahrávání se vytvořil bezmála tří-gigabajtový soubor. Bohužel ani tak se při dekódování nevyřešil problém s výkonem. Vytížení procesoru bylo přibližně stejné jako v předchozím případě a zachyceno bylo pouze 6 rámců

ze 2000. Celý postup byl zaznamenán při nahrávání obrazovky a umístěn k výsledným souborům na přiložené médium do adresáře "/Zachycená komunikace/LimeSDR/2.3.6"pod názvem záznam.mp4. Obsahem adresáře je dále zachycená komunikace v souboru SDR.pcap, konzolový výpis v souboru log.txt i soubor filesink, který obsahuje zdrojový signál.



Obr. 2.27: Srovnání objemu zachycených dat. Nahoře LimeSDR a dole síťová karta Alfa network.

2.3.8 Úprava projektu v GNU Radiu

Aby bylo možné detekovat, kde nastává chyba při příjmu paketů, bylo v projektu nastaveno detailnější vypisování logování do konzole.

Výpis 2.2: Část konzolového výpisu příjmu jednoho rámce.

```
Decode MAC: frame start -- len 127  symbols 44  encoding 0
copy one symbol, copied 0 out of 44
...
copy one symbol, copied 43 out of 44
received complete frame - decoding
psdu size127
80 00 00 00 ff ff ff ff ff ff 00 0c 42 fb
99 91 00 0c ea fb 99 91 50 c0 80 71 f8 8d 0e 00
90 00 64 00 21 04 00 0d 4d 69 6b 72 6f 54 69 6b
2d 50 4f 44 4f 61 46 52 75 21 30 8c 12 18 24 03
01 06 05 04 00 01 00 00 2a 01 00 32 04 30 48 60
6c dd 2a 00 0c 42 00 00 00 01 1e 00 10 00 00 02
66 27 36 bf fb 31 30 30 43 34 52 70 42 39 39 39
31 00 00 00 00 00 00 78 6c 5b 38 da 73 52 22 d3
87
............B.........P..q......d.!...MikroTik-PODOaFRu!0
............*..2.0H‘l.*..B..........f’6..100C4RpB9991....
..xl[8.sR"..
checksum␣wrong␣--␣dropping
```

Na posledním řádku se objevuje hláška "checksum wrong - dropping", což v překladu znamená, že kontrolní součet vyšel špatně a z toho důvodu je rámec zahozen. Zahazování paketu způsobuje část kódu bloku decode_mac.cc.

Výpis 2.3: Úryvek kódu z bloku decode_mac.cc

```
  boost::crc_32_type result;
  result.process_bytes(out_bytes + 2, d_frame.psdu_size);
  if(result.checksum() != 558161692) {
    dout << "checksum␣wrong␣--␣dropping" << std::endl;
    return;
      }
```

Tato část kódu s magickou podmínkou, že kontrolní součet se musí rovnat hodnotě 558161692 byla zakomentována. Jedná se o návratovou hodnotu funkce checksum a znamená, že pokud se výsledek rovná právě této hodnotě, kontrolní součet je správný. [30]. Tato část kódu byla zakomentována a projekt gr-IEEE802.11 znovu zkompilován a nainstalován. Výsledkem bylo mnohem více zachycených paketů, avšak stále pouhý zlomek toho co dokázala zachytit bezdrátová karta. Konkrétně jich během jedné minuty SDR zachytilo 226 a bezdrátová karta 4525. Navíc část z oněch 226 paketů byla poškozena a nedávala smysl. To dokládá Tab. 2.5 a Tab. 2.6,

Tab. 2.5: Statistika zachycených dat ze SDR.

Adresa A	Adresa B	Bajty	Paketů z A do B	Paketů z B do A
39.133.36.192	192.104.190.132	107	0	1
54.106.20.183	116.168.168.16	107	0	1
64.6.127.100	192.168.88.250	107	0	1
64.118.162.25	249.154.241.96	1055	0	1
74.172.247.203	192.40.43.11	107	0	1
87.135.17.124	117.235.89.30	107	0	1
92.237.166.215	117.112.10.14	107	1	0
192.168.88.1	192.168.88.2	2110	2	0
192.168.88.2	192.168.88.250	1995	0	13
192.168.88.194	192.168.88.250	107	0	1
192.168.176.103	205.139.1.91	107	1	0

Tab. 2.6: Statistika zachycených dat z bezdrátové karty.

Adresa A	Adresa B	Bajty	Paketů z A do B	Paketů z B do A
192.168.10.1	255.255.255.255	230	1	0
192.168.88.1	192.168.88.2	151998	64	77
192.168.88.1	255.255.255.255	208	1	0
192.168.88.2	192.168.88.250	1108470	898	738
192.168.88.2	255.255.255.255	642	3	0

které obsahují statistiky komunikace mezi jednotlivými adresami. V tabulce pro SDR (Tab. 2.5) je mnoho nesmyslných adres. Tyto adresy jsou nesmyslné a v testované síti se nenachází, to znamená, že SDR chybným příjmem zaměnilo za správné adresy, které se nacházejí v Tab. 2.6.

Výsledky jsou uloženy v souborech na přiloženém médiu v adresáři "/Zachycená komunikace/LimeSDR/2.3.8"pod názvem SDR.pcap a karta.pcapng. Přiložen je i konzolový výpis v souboru log.txt.

2.3.9 Zahazování nepotřebných paketů

Pakety/rámce je možno rozdělit do tří základních skupin dle jejich účelu.

- Kontrolní rovina
- Managmentová rovina
- Datová rovina

Kontrolní pakety jsou označovány například pakety směrovacích protokolů a podobně. Managmentové pakety slouží k monitorování a administrativě sítě. Spadá sem

například ICMP ping. Datové pakety přenášejí ostatní užitečný provoz. Aby se ulehčilo výpočetnímu výkonu byl znova upraven kód projektu. Nyní změna spočívala v zahazování datových a kontrolních paketů. Tato změna však nepřinesla téměř žádné zlepšení. Zjištění o jaký paket se jedná totiž nastává až na samotném konci dekódovacího procesu a nároky na výkon jsou tak prakticky shodné. Výsledky jsou uloženy v souborech na přiloženém médiu v adresáři "/Zachycená komunikace/LimeSDR/2.3.9"pod názvem SDR.pcap a karta.pcapng. Přiložen je i konzolový výpis v souboru log.txt a záznam postupu nahrán zaznamenáváním obrazovky a umístěn k výsledným souborům pod názvem záznam.mp4.

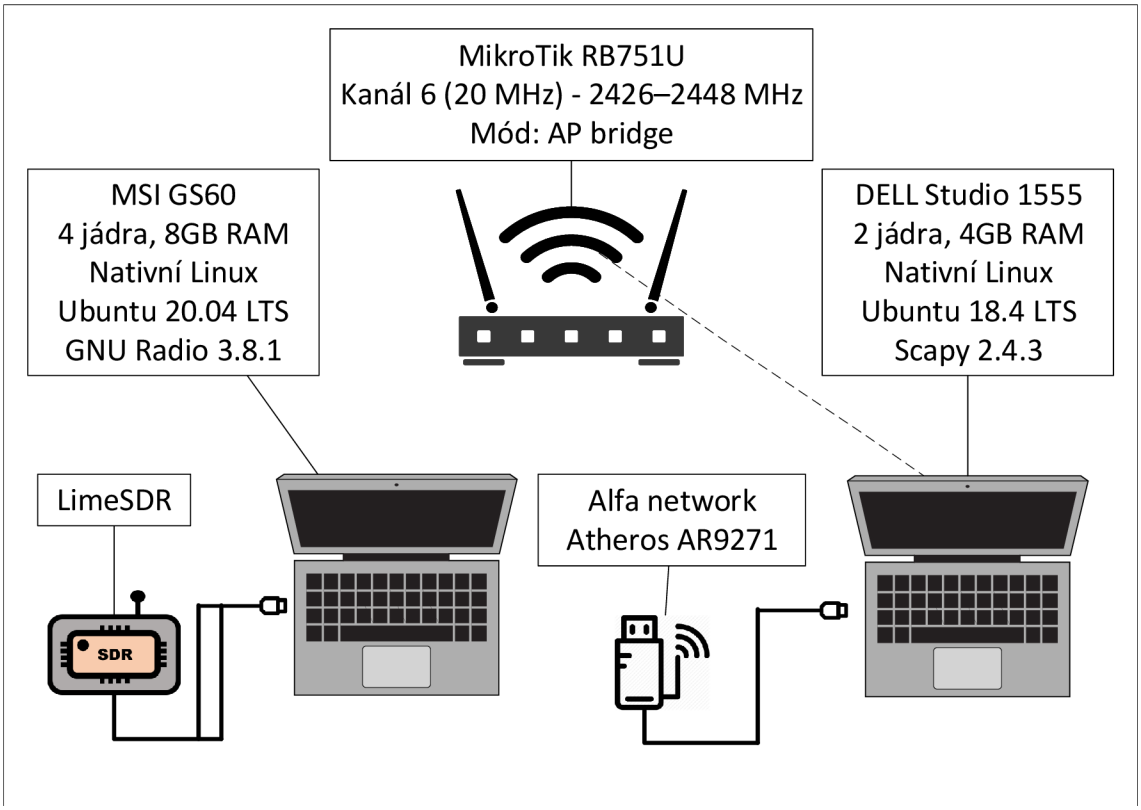
2.3.10 Nativní Linux Ubuntu 20.04

Ohledně problému se zprovozněním projektu gr-802.11 (popsaném v podkapitole 2.2.7) a s tím spojeným zachytáváním bezdrátové komunikace IEEE 802.11 byl kontaktován i samotný tvůrce projektu.

Nejprve byl v emailové komunikaci tázán zda by bylo možné jeho projekt rozšířit o implementaci standardu IEEE 802.11n, neboť stávají projekt podporuje pouze IEEE 802.11 a/g/p. Dr. Bastian Bloessl odpověděl, že on sám se do rozšíření projektu tímto způsobem nechystá, ale již ho ohledně této záležitosti kontaktovali někteří lidé, avšak nikomu z nich se nepodařilo podporu standardu IEEE 802.11n implementovat. Nedostatečný výkon a neurčitost propojení USB zařízení s virtuálním operačním systémem si vyžádali přestoupení k dalšímu testu. Tentokrát byl systém nainstalován přímo na pevný disk výkonnějšího počítače MSI GS60. Pro tento pokus byla zvolena verze Focal Fossa 20.04 LTS operačního systému systému Linux Ubuntu. Po zprovoznění systému byl nainstalován software Lime Suite pro ovládání hardware SDR následně bylo nainstalováno nejnovější GNU Radio 3.8.1 a doinstalovány požadované moduly, konkrétně gr-IEEE802.11, gr-limesdr. Ještě však před instalací GNU Radia bylo nutné nainstalovat seznam všech prerekvizit, jako jsou programy CMake, git, python a celou řadu knihoven. Při instalaci se vyskytly problémy. Software Lime Suite se nepodařilo nainstalovat tradičním způsobem pomocí PPA (Personal Package Archives), bylo tak nutné jej zkompilovat a nainstalovat ze zdrojových souborů. Instalaci GNU Radia předchází instalace VOLK (Vector-Optimized Library of Kernels) knihovny pro tvorbu nejlepší architektury SIMD (Single Instruction, Multiple Data). Instalace samotného GNU Radia byla také doprovázena chybami. Při kompilaci se ukázalo, že nová verze potřebuje navíc balíčky swig, které byly doinstalovány. Následně bylo kvůli další sérii chyb potřebné upravit cestu k python knihovnám. Nakonec byly doinstalovány potřebné moduly gr-limesdr, gr-foo a gr-IEEE802.11, všechny tři ze zdrojových souborů. Kalibrace základní desky byla provedena tradičně programem Lime Suite. Program GNU Radio spuštěn pomocí

terminálu, kvůli přehlednějšímu zobrazení konzolového výpisu. Předinstalovaný příkladový projekt byl upraven záměnou zdrojového bloku (původní projekt obsahuje USRP blok, který je určen pro jiný druh SDR) za nainstalovaný blok LimeSDR Source. Dále byly aktivovány bloky pro ukládání zachycených dat do souboru. GNU Radio při kompilaci stále hlásilo chyby v datových typech proměnných. Bylo nutné nahradit grafické posuvníky statickými proměnnými. Tento problém by mohl být přisouzen úpravám v grafickém balíku gr-qtgui, které byly provedeny v nové verzi GNU Radia 3.8.1 [31]. Nakonec byl nainstalován Wireshark pro zobrazení obsahu výsledného souboru formátu .pcap a spuštěn optimalizační příkaz run_volk.

Výslednou topologii vykresluje Obr. 2.28 a reálný obraz zapojení je zachycen na Obr. 2.29.



Obr. 2.28: Topologie při testování nativního Linuxu Ubuntu 20.04 LTS.

Oproti předchozím scénářům vytvářel komunikaci počítač DELL Studio 1555 softwarem pro tvorbu definovaných paketů Scapy 2.4.3, který byl využíván již dříve. Příkazem:

```
send(IP(dst="192.168.88.1")/ICMP()/"televize123456televize
123456televize123456televize123456televize123456televize
123456televize123456televize123456televize123456televize
123456", count=10)
```

Obr. 2.29: Reálná topologie s nativním Linuxem Ubuntu 20.04 LTS.

byla desetkrát odeslána odeslána dávka deseti ICMP zpráv obsahujících 10 za sebou jdoucích výrazů "televize123456". V předcházejících případech byl obsahem ICMP zpráv náhodný řetězec. To ztěžovalo identifikaci vyslaných paketů v konzoli GNU Radia. Referenční zachytávání paketů bezdrátovou síťovou kartou tentokrát obstarával také počítač DELL.

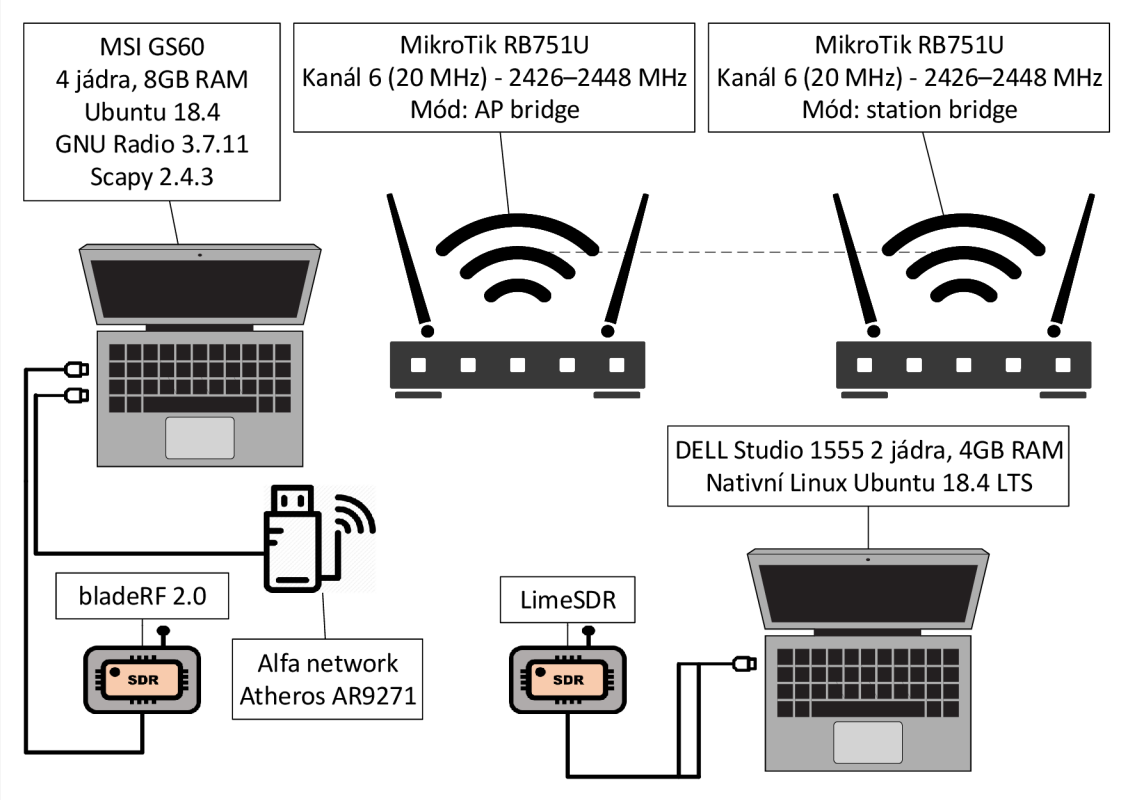
Bohužel ani v nativním Linuxu s novou verzí GNU Radia se nedostavily požadované výsledky. Počet zachycených paketů byl víceméně stejný jako v případě zachytávání ve virtuálním Linuxu. Při analyzování konzolového výpisu se vyslaný výraz "televize123456"vyskytl pouze jednou. Avšak vysláno bylo během jedné minuty dohromady jeden tisíc těchto výrazů. Výsledky jsou uloženy v souborech na přiloženém médiu v adresáři "/Zachycená komunikace/LimeSDR/2.3.10"pod názvem SDR.pcap. Přiložen je i konzolový výpis v souboru log.txt a záznam postupu nahrán zaznamenáváním obrazovky a umístěn k výsledným souborům pod názvem záznam.mkv.

2.4 Zachycení s pomocí bladeRF 2.0

Poslední SDR, které bylo vyzkoušeno bylo bladeRF verze 2.0.

2.4.1 Sestavení topologie

Topologie se od předchozí příliš nezměnila. Zdrojem komunikace byl bezdrátový přístupový bod. Na rozdíl od LimeSDR neměl bladeRF 2.0 problém se stabilitou ve virtuálním operačním systému s přímým zapojením do počítače. Nebylo tak nutné použít rozbočovač. Topologii graficky znázorňuje Obr. 2.30.



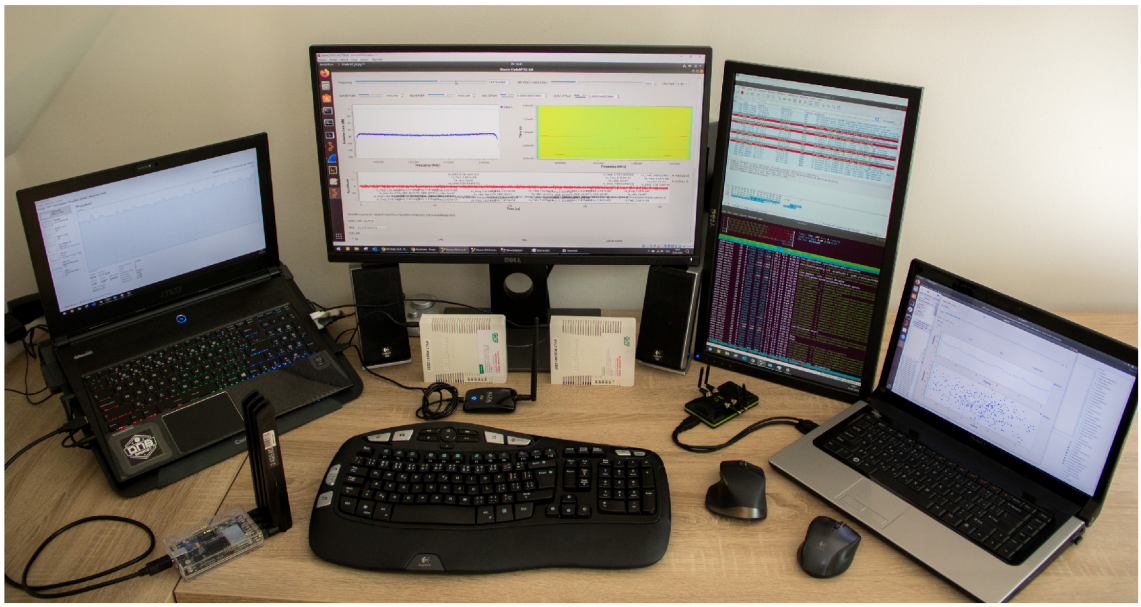
Obr. 2.30: Topologie odposlechu bezdrátové komunikace pomocí bladeRF.

Konfigurace bezdrátových směrovačů

Na routerech MikroTik byl spuštěn ICMP ping o velikosti 1000 B, každých 1000 ms. Zabezpečení bylo ponecháno otevřené. Parametry přístupového bodu se nezměnily od Tab. 2.4.

Konfigurace stanice

Jako v minulých případech byl použit přenosný počítač MSI s označením GS60 osazený čtyř-jádrovým procesorem i7-4710HQ s taktovací frekvencí 2,5 GHz, 8 GB operační paměti RAM s přístupem DDR3 a harddiskem Samsung SSD 850 EVO. Nativním operačním systémem byl 64 bitový Windows 10 Pro. Na počítači byl nainstalován software VirtualBox 6.1.4, který v tomto případě umožňuje virtualizovat operační systém Linux Ubuntu 18.4.4. Ze stránek výrobce byl stažen soubor obsahující všechny potřebné nástroje pro správné rozpoznání a ovládání bladeRF. Instalátor nabízí na výběr mezi ovladačem LibUSB a Cypress CyUSB3. Podle doporučení byl vybrán ovladač LibUSB.



Obr. 2.31: Reálná topologie se zařízením bladeRF 2.0.

OsmoSDR

OsmoSDR je balík softwaru který spravuje projekt Osmocom (Open source mobile communications). OsmoSDR podporuje širokou škálu hardwaru od USRP, přes LimeSDR po BladeRF.

gr-osmosdr

Tento modul GNU Radia obsahuje komunikační bloky pro ovládání SDR. Prerekvizitou funkce tohoto modulu je instalace balíčku OsmoSDR viz 2.4.1. Stejně jako gr-limesdr se gr-osmosdr modul GNU Radia instaluje ze zdrojových souborů uložených v distribuovaném systému správy verzí, Git.

Výsledek testu

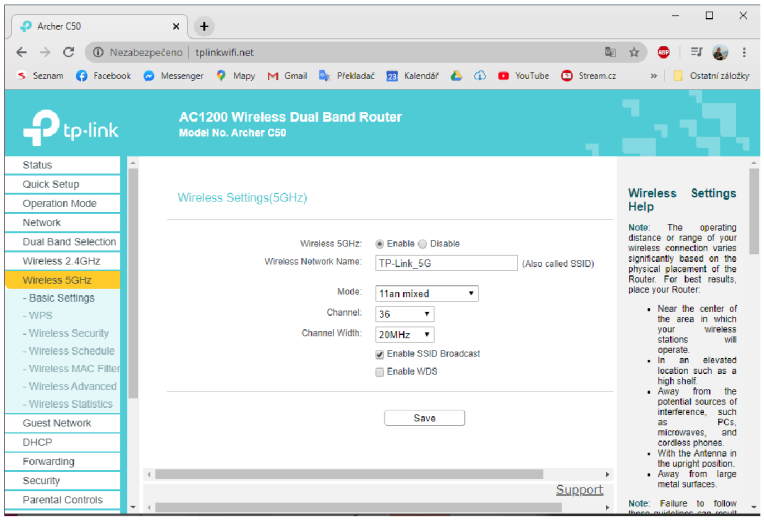
Při tomto pokusu se také nedostavily požadované výsledky. Navíc zde prokazatelně nedostačoval výkon počítače MSI, jehož procesor byl vytížen z 95%. To mělo pravděpodobně za následek zachycení pouze jednoho rámce. Pro porovnání bylo LimeSDR připojené ke druhému počítači a zachytávalo identickou komunikaci. Výsledkem bylo, že bladeRF zachytil jeden rámec a LimeSDR je podařilo zachytit 67 rámců z celkových 7226 rámců zachycených bezdrátovou síťovou kartou. Log i zachycené datové toky jsou uloženy na přiloženém médiu v adresáři: "/Zachycená komunikace/bladeRF/2.4.1".

2.4.2 Test v 5 GHz pásmu

BladeRF 2.0 disponuje frekvenčním rozsahem od 47 MHz po 6 GHz. To umožňuje práci se standardem IEEE 802.11 v pásmu 5 GHz. V tomto pásmu bohužel nepracují používané bezdrátové routery MikroTik ani bezdrátová síťová karta Alfa Network. Proto byly routery MikroTik nahrazeny routerem TP-LINK Archer C50, dovolující komunikaci na vyšších frekvencích. Referenční zachytávání paketů bude obstarávat síťová karta vestavěná v počítači MSI Intel Dual Band Wireless-AC 7260. S ohledem na protokoly podporované projektem v GNU Radiu byl zvolen standard IEEE 802.11a.

Konfigurace bezdrátového směrovače

Router TP-LINK Archer C50 nedovoluje nastavit ryze IEEE 802.11a mód komunikace, ale jen smíšený mód s IEEE 802.11n viz Obr. 2.32.



Obr. 2.32: Nastavení bezdrátového směrovače TP-LINK.

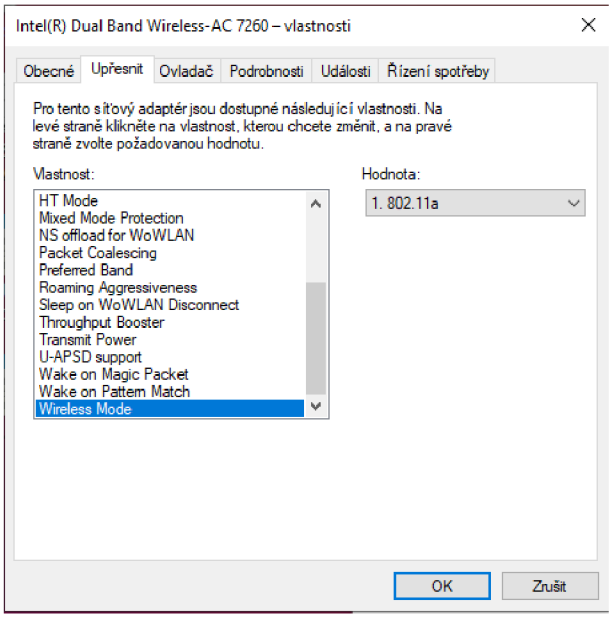
Konkrétní parametry byly nastaveny podle Tab. 2.7.

Tab. 2.7: Parametry přístupového bodu.

Parametr	**Hodnota**
Standard:	IEEE 802.11a
SSID:	TP-LINK_5G
Kanál:	36
Frekvence:	5170–5190 MHz
Šířka pásma:	20 MHz
Typ zabezpečení:	-
Typ šifrování:	-

Konfigurace stanice

Aby byl dodržen podporovaný mód komunikace IEEE 802.11a musela být síťová karta v počítači stanice nastavena do tohoto módu. V konfiguračním nastavení adaptéru je tato možnost pod záložkou Wireless Mode (Obr. 2.33).



Obr. 2.33: Nastavení módu komunikace bezdrátového adaptéru.

Iniciátorem odposlouchávané komunikace byl počítač MSI se svým bezdrátovým adaptérem Intel Dual Band Wireless-AC 7260 a softwarem pro tvorbu definovaných paketů Scapy 2.4.3 jenž vytvořil dávku deseti ICMP zpráv obsahujících 10 za sebou jdoucích výrazů "televize123456".

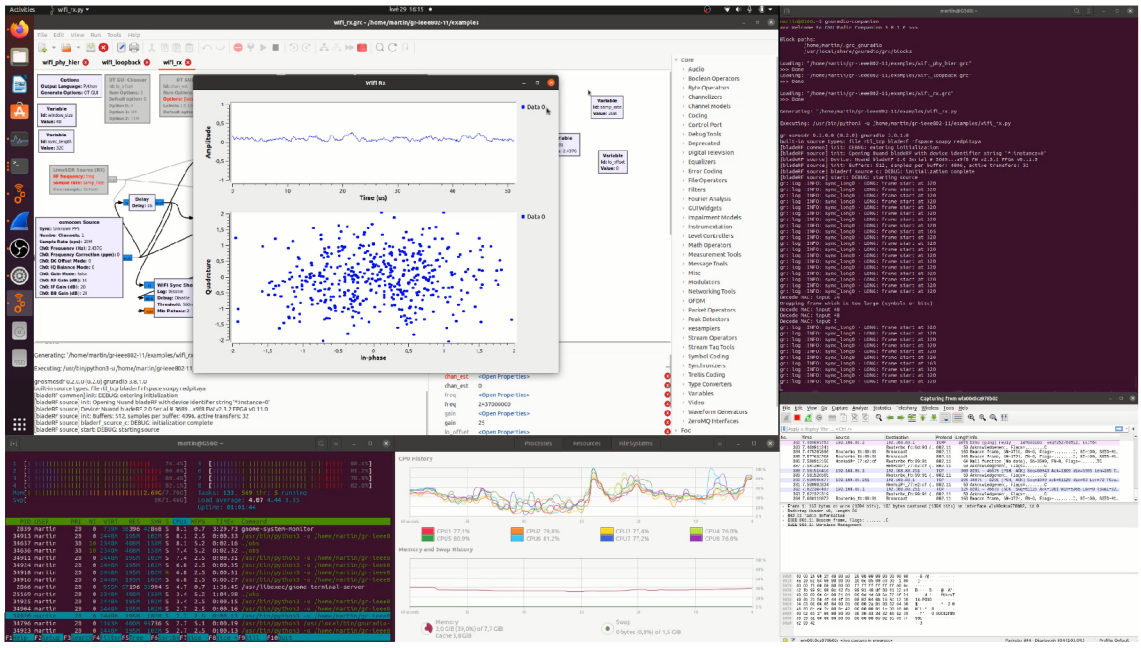
Výsledek zachytávání v 5 GHz pásmu

Výsledek zachytávání nebyl překvapivý v objemu zachycených rámců, kterých bylo jen 134, ale v jejich typu. Podařilo se totiž zachytit všechny Request-to-send a Clear-to-send pakety. Všechny zachycené rámce nepřesahují velikost 50 B.

Při zachytávání bylo vytížení procesoru velmi vysoké. Nástroj htop ve virtuálním prostředí Linux zobrazoval vytížení průměrně 95% všech čtyř jader. Konzolový výpis zkopírovaný do souboru log.txt ukazuje stejný problém jako v předchozích případech, tedy nesmyslnost zachycených dat a následné zahození rámce z důvodu nesprávného výsledku kontrolního součtu. Log i zachycené datové toky jsou uloženy na přiloženém médiu v adresáři: "/Zachycená komunikace/bladeRF/2.4.2".

Výsledek zachytávání v nativním Linuxu

Poslední varianta ověření funkčnosti v GNU Radiu spočívala ve využití nativního Linuxu z předchozí kapitoly, konkrétně podkapitoly 2.3.10. Provoz již tradičně vytvářely dva MikroTik routery na šestém kanálu. Zachytávání bylo spuštěno na 10 sekund. Během této doby se bohužel nezachytil žádný paket, jako v předchozích případech byly dle konzolového výpisu všechny zahozeny. Důvodem byl nevycházející kontrolní součet. Samotný proces dekódování běžel v pozadí ještě dalších 15 minut po ukončení zachytávání. Snímek obrazovky z nahrávání je na Obr. 2.34.

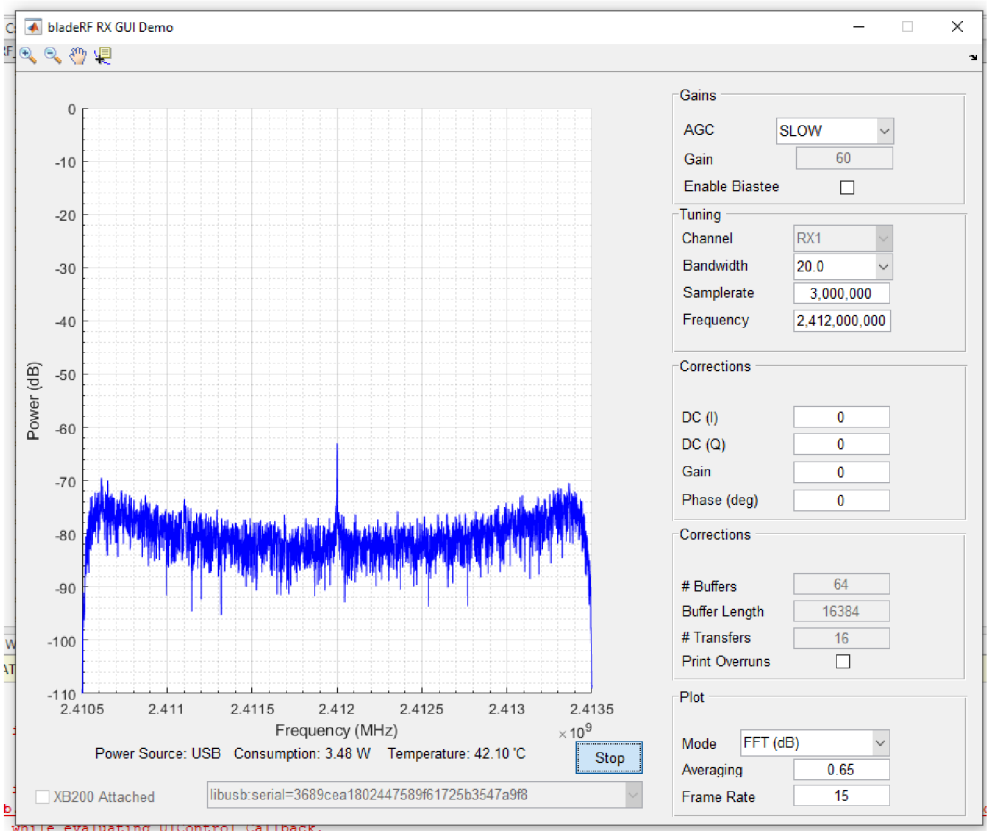


Obr. 2.34: Snímek obrazovek při zachytávání nativním Linuxu.

Celý průběh zachytávání byl nahrán programem OBS a i se všemi výslednými soubory vložen na přiložené CD do adresáře "/Zachycená komunikace/bladeRF/2.4.3".

2.4.3 MATLAB

Pro vytvoření bezdrátové sondy může být jako jedna z dalších variant využit software MATLAB. Tento program je alternativou k software GNU Radio. Disponuje obsáhlou databází uživatelských projektů, včetně pokusů o implementaci IEEE 802.11 dekodérů. Zařízení bladeRF tento program podporuje. Pro propojení SDR bladeRF s programem existuje balík zvaný "Communications Toolbox Support Package for BladeRF 2.0". Po jeho intuitivním nainstalování je v adresáři C:\Program Files\bladeRF\matlab připraven projekt bladeRF_rx_gui.m, který je po spuštění programu MATLAB a nastavení aktuální cesty do složky s tímto souborem spustitelný. Je li vše správně nainstalováno spustí se jednoduché okno s FFT grafem, kde je možné nastavit parametry zařízení s zobrazit tak požadované spektrum signálu. Pro demonstraci bylo zařízení nastaveno na frekvenci využívanou nedalekým bezdrátovým přístupovým bodem. Graf nedisponuje funkcní "waterfall"grafu, nicméně i přesto bylo patrné, že signál má charakteristickou podobu OFDM modulace. Znamená to tedy, že s pomocí tohoto programu by mělo být možné sestavit bezdrátovou sondu.



Obr. 2.35: Snímek obrazovky při testováni bladeRF s programem MATLAB.

Závěr

Cílem práce bylo vytvořit prototyp přijímače bezdrátové komunikace, který by umožňoval v reálném čase dekódovat pomocí SDR signál vytvořený podle standardu IEEE 802.11b/g/n. V porovnání s běžnou síťovou kartou má SDR několikanásobně větší šířku pásma a díky softwarově programovatelným obvodům a následné softwarové implementací demodulátoru také široké možnosti rozšiřitelnosti a přizpůsobitelnosti, které bezdrátová karta kvůli pevně daným hardwarovým parametrům nemůže nabídnout.

Nejprve byla bezdrátová komunikace zachycena pomocí bezdrátové síťové karty podporující monitorovací mód, ve kterém dovede karta přijímat i rámce, které jsou určeny jiným síťovým kartám. Výstupem jsou dva toky dat, kdy první obsahuje vygenerovanou komunikaci uvnitř sítě a ve druhém toku zachyceném monitorovací stanicí je po dešifrování pozorovatelná ta samá komunikace. Z těchto dat byly vytvořeny grafy zachycující komunikaci uvnitř a vně sítě, kde lze pozorovat kromě vygenerované komunikace i ostatní provoz, jako například Beacon rámce vysílané přístupovým bodem, nebo komunikaci během připojování stanice. Tyto data sloužily jako srovnávací podklad při práci s SDR, kdy srovnáním byl podroben zachycený datový tok SDR a bezdrátové karty.

V následujících sekcích byla síťová karta v topologii zaměněna za postupně tři SDR. První z nich bylo LimeSDR mini. To provázela řada problémů se zprovozněním, kdy přestože zařízení dle specifikace podporuje USB 3.0, v počítači bylo detekováno jen v USB 2.0 portech a výsledná úroveň signálu v celém rozsahu byla na úrovni šumu. Následující dvě SDR, LimeSDR a bladeRF, potíže s připojením neměly. Po instalaci ovladačů bylo možné sledovat běžné signály jako LTE, bluetooth, FM rádio, nebo signál z bezdrátového routeru.

Přistoupilo se tak k jádru práce, tedy k softwarové implementaci dekodéru komunikace. Po sestavení potřebné topologie byl vytvořen projekt inspirovaný podobným open-source projektem nesoucím název Wime Project. K tomu bylo nutné doinstalovat řadu modulů, jako OFDM demodulační blok, blok fyzické vrstvy, blok pro připojení do Wiresharku. Dále byl projekt vyladěn na optimální hodnoty parametrů přijímače, jako zesílení, modelování pásmové propusti, nastavení centrální frekvence a dalších významně příjem ovliňujících hodnot. Nicméně výsledek zachytávání byl neuspokojivý, neboť zachycen byl jen zlomek doopravdy vyslaných rámců. Následovalo mnoho pokusů o zlepšení výsledků, jako kalibrace zařízení, kompenzace SS složky, využití jiných počítačů, jiných operačních systémů, jiných frekvenčních pásem, zahazování části provozu a dalších úprav. Nicméně na výsledky zachytávání to nemělo téměř žádný vliv. Cíl práce byl tak naplněn pouze z části. Sonda pro zachytávání bezdrátové komunikace standartu IEEE 802.11a/g byla vytvořena, avšak

nejspíš kvůli nárokům na výpočetní výkon není zachycená komunikace kompletní. To je také jeden z důvodů, proč se nepokračovalo v rozšiřování projektu o podporu standardu IEEE 802.11n. Dalším důvodem byla podstatně větší složitost tohoto standardu. Standard využívá vícecestné multi-anténní šíření, jehož implementace by byla z časových důvodů neuskutečnitelná. Práce se většinu času zabývala zprovozněním zachycení komunikace standardu IEEE 802.11g. Zprovoznit sondu pro tento protokol bylo před pokračováním v implementaci dalších standardů klíčové. Bohužel plné funkčnosti kvůli vzniklým problémům nebylo dosaženo. Nepomohly ani pokusy o změny topologie, či nahrazení postupně všech použitých zařízení. Proto také nebyl standard 802.11b v práci uvažován. Využívá odlišnou modulační techniku a jeho implementace by byla časově náročná. Výsledek zachytávání by navíc patrně vedl stejným směrem jako u testovaného IEEE 802.11g.

Alternativní možností při pokračování v této problematice je místo GNU Radia použít software MATLAB, který byl v závěru práce otestován se zařízením bladeRF a je tedy pro základní práci s SDR připraven. Nicméně by bylo nutné naprogramovat projekt pro standard IEEE 802.11, který doposud nebyl vytvořen. Proto se tato cesta jeví jako vhodné rozšíření této práce, nicméně je potřeba počítat s poměrně velkou časovou náročností při řešení tohoto problému.

Literatura

[1] SMETANOVÁ, Lucie. *Internet věcí a možnosti jeho využití pro komerční účely.* Praha, 2016. Bakalářská práce. České vysoké učení technické v Praze. Vedoucí práce Ing. NÁPLAVA Pavel, Ph.D.

[2] ŠTRAJT, Martin. *Experimentální měření a simulace nízkoenergetické komunikační sítě VUT dlouhého dosahu.* Brno, 2018. Bakalářská práce. Vysoké učení technické v Brně. Vedoucí práce Ing. FUJDIAK Radek, Ph.D.

[3] POLITIS, Christos, Sina MALEKI, Juan Merlano DUNCAN, Jevgenij KRIVOCHIZA, Symeon CHATZINOTAS a Bjorn OTTESTEN. SDR Implementation of a Testbed for Real-Time Interference Detection With Signal Cancellation. *IEEE Access* [online]. 2018, 6, 20807-20821 [cit. 2020-05-29]. DOI: 10.1109/ACCESS.2018.2825885. ISSN 2169-3536. Dostupné z: https://ieeexplore.ieee.org/document/8340048/

[4] ZHANG, Yueying, Keju WANG a Hang LONG. SDR-Based ADS-B with Dual-Frequency for UAS: A Universal Design. In: *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing* [online]. IEEE, 2015, 2015, s. 59-63 [cit. 2020-05-29]. DOI: 10.1109/CIT/IUCC/DASC/PICOM.2015.12. ISBN 978-1-5090-0154-5. Dostupné z: http://ieeexplore.ieee.org/document/7363052/

[5] BANG, Saehee, Chiyoung AHN, Yong JIN, Seungwon CHOI, John GLOSSNER a Sungsoo AHN. Implementation of LTE system on an SDR platform using CUDA and UHD. *Analog Integrated Circuits and Signal Processing* [online]. 2014, 78(3), 599-610 [cit. 2020-05-29]. DOI: 10.1007/s10470-013-0229-1. ISSN 0925-1030. Dostupné z: http://link.springer.com/10.1007/s10470-013-0229-1

[6] KOCKS, Christian, Alexander VIESSMANN, Andreas WAADT, et al. A DVB-T2 receiver realization based on a software-defined radio concept. In: *2010 4th International Symposium on Communications, Control and Signal Processing (ISCCSP)* [online]. IEEE, 2010, 2010, s. 1-4 [cit. 2020-05-29]. DOI: 10.1109/ISCCSP.2010.5463488. ISBN 978-1-4244-6285-8. Dostupné z: http://ieeexplore.ieee.org/document/5463488/

[7] VELASCO, Cesar a Christian TIPANTUNA. Meteorological picture reception system using software defined radio (SDR). In: *2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM)* [online]. IEEE, 2017, 2017, s. 1-6 [cit.

2020-05-29]. DOI: 10.1109/ETCM.2017.8247551. ISBN 978-1-5386-3894-1. Dostupné z: http://ieeexplore.ieee.org/document/8247551/

[8] MARŠÁLEK, Roman. *Učebnice teorie rádiové komunikace* [online]. 2013. Brno, 2013 [cit. 2020-05-29]. Dostupné z: http://www.urel.feec.vutbr.cz/MTRK/

[9] UTTAMCHANDANI, Deepak. *Handbook of MEMS for wireless and mobile applications*. Elsevier, 2013. ISBN 978-0-85709-271-7.

[10] RYKACZEWSKI, P., D. PIENKOWSKI, R. CIRCA a B. STEINKE. Signal path optimization in software-defined radio systems. *IEEE Transactions on Microwave Theory and Techniques* [online]. 2005, 53(3), 1056-1064 [cit. 2020-05-29]. DOI: 10.1109/TMTT.2005.843510. ISSN 0018-9480. Dostupné z: http://ieeexplore.ieee.org/document/1406311/

[11] ABIDI, Asad A. The Path to the Software-Defined Radio Receiver. *IEEE Journal of Solid-State Circuits* [online]. 2007, **42**(5), 954-966 [cit. 2020-05-30]. DOI: 10.1109/JSSC.2007.894307. ISSN 0018-9200. Dostupné z: http://ieeexplore.ieee.org/document/4160058/

[12] TONG, Z., M. S. ARIFIANTO a C. F. LIAU. Wireless transmission using universal software radio peripheral. In: *2009 International Conference on Space Science and Communication* [online]. IEEE, 2009, 2009, s. 19-23 [cit. 2020-05-29]. DOI: 10.1109/ICONSPACE.2009.5352678. ISBN 978-1-4244-4956-9. Dostupné z: http://ieeexplore.ieee.org/document/5352678/

[13] WYGLINSKI, Alexander M., Don P. OROFINO, Matthew N. ETTUS a Thomas W. RONDEAU. Revolutionizing software defined radio: case studies in hardware, software, and education. *IEEE Communications Magazine* [online]. 2016, 54(1), 68-75 [cit. 2020-05-29]. DOI: 10.1109/MCOM.2016.7378428. ISSN 0163-6804. Dostupné z: http://ieeexplore.ieee.org/document/7378428/

[14] LimeSDR-Mini v1.2 hardware description. *MYRIAD.RF* [online]. [cit. 2020-05-29]. Dostupné z: https://wiki.myriadrf.org/LimeSDR-Mini_v1.2_hardware_description

[15] BladeRF 2.0 micro xA4. *Nuand* [online]. [cit. 2020-05-29]. Dostupné z: https://www.nuand.com/product/bladerf-xa4/

[16] MILAN, Klement. *Technologie bezdrátových sítí - základní principy a standardy* [online]. Křížkovského 8, 771 47 Olomouc: Univerzita Palackého v Olomouci, 2017 [cit. 2020-05-29]. DOI: 10.5507/pdf.17.24451565. ISBN 978-80-244-5156-5.

[17] GAST, Matthew. *802.11 wireless networks: the definitive guide*. Beijing: O'Reilly, c2002. ISBN 0-596-00183-5.

[18] Využívání vymezených rádiových kmitočtů. *ČTU* [online]. Praha: Český telekomunikační úřad, 2019 [cit. 2020-05-28]. Dostupné z: https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu

[19] XIAO, Yang a Yi PAN. *Emerging wireless LANs, wireless PANs, and wireless MANs: IEEE 802.11, IEEE 802.15, IEEE 802.16 wireless standard family*. Hoboken, N.J.: Wiley, 2009. Wiley series on parallel and distributed computing. ISBN 9780471720690.

[20] GHOSH, M. Joint equalization and decoding for complementary code keying (CCK) modulation. In: *2004 IEEE International Conference on Communications (IEEE Cat. No.04CH37577)* [online]. IEEE, 2004, 2004, 3465-3469 Vol.6 [cit. 2020-05-28]. DOI: 10.1109/ICC.2004.1313188. ISBN 0-7803-8533-0. Dostupné z: http://ieeexplore.ieee.org/document/1313188/

[21] Retronym. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-05-28]. Dostupné z: https://en.wikipedia.org/wiki/Retronym

[22] VASSIS, D., G. KORMENTZAS, A. ROUSKAS a I. MAGLOGIANNIS. The IEEE 802.11g standard for high data rate WLANs. *IEEE Network* [online]. 2005, **19**(3), 21-26 [cit. 2020-05-28]. DOI: 10.1109/MNET.2005.1453395. ISSN 0890-8044. Dostupné z: http://ieeexplore.ieee.org/document/1453395/

[23] JYH-CHENG CHEN, MING-CHIA JIANG a YI-WEN LIU. Wireless LAN security and IEEE 802.11i. *IEEE Wireless Communications* [online]. 2005, 12(1), 27-36 [cit. 2020-05-29]. DOI: 10.1109/MWC.2005.1404570. ISSN 1536-1284. Dostupné z: http://ieeexplore.ieee.org/document/1404570/

[24] SHRIVASTAVA, Vivek, Shravan RAYANCHU, Jongwoon YOONJ a Suman BANERJEE. 802.11n under the microscope. In: *Proceedings of the 8th ACM SIGCOMM conference on Internet measurement conference - IMC '08* [online]. New York, New York, USA: ACM Press, 2008, 2008, s. 105- [cit. 2020-05-28]. DOI: 10.1145/1452520.1452533. ISBN 9781605583341. Dostupné z: http://portal.acm.org/citation.cfm?doid=1452520.1452533

[25] BLUM, Josh. Lime Suite driver architecture. *MYRIAD.RF* [online]. 4.5.2016 [cit. 2020-05-28]. Dostupné z: https://myriadrf.org/news/limesuite-driver-architecture/

[26] UHD Introduction. *Ettus Research* [online]. 7.2.2020 [cit. 2020-05-28]. Dostupné z: https://kb.ettus.com/UHD

[27] BRAUN, Martin. PyBOMBS: The What, the How and the Why. *GNURadio* [online]. GNU Radio project, 2020 [cit. 2020-05-28]. Dostupné z: https://www.gnuradio.org/blog/2016-06-19-pybombs-the-what-the-how-and-the-why/

[28] MUSINGS, John. LimeSDR - Mini on Ubuntu with GQRX. *John's Musings: Blog* [online]. 2016 [cit. 2020-05-28]. Dostupné z: https://www.hagensieker.com/blog/page/?post_id=104title=limesdr—mini-on-ubuntu-with-gqrx

[29] LimeSDR Quick Start. *MYRIAD.RF* [online]. Lime Microsystems [cit. 2020-05-28]. Dostupné z: https://wiki.myriadrf.org/LimeSDR_Quick_Start

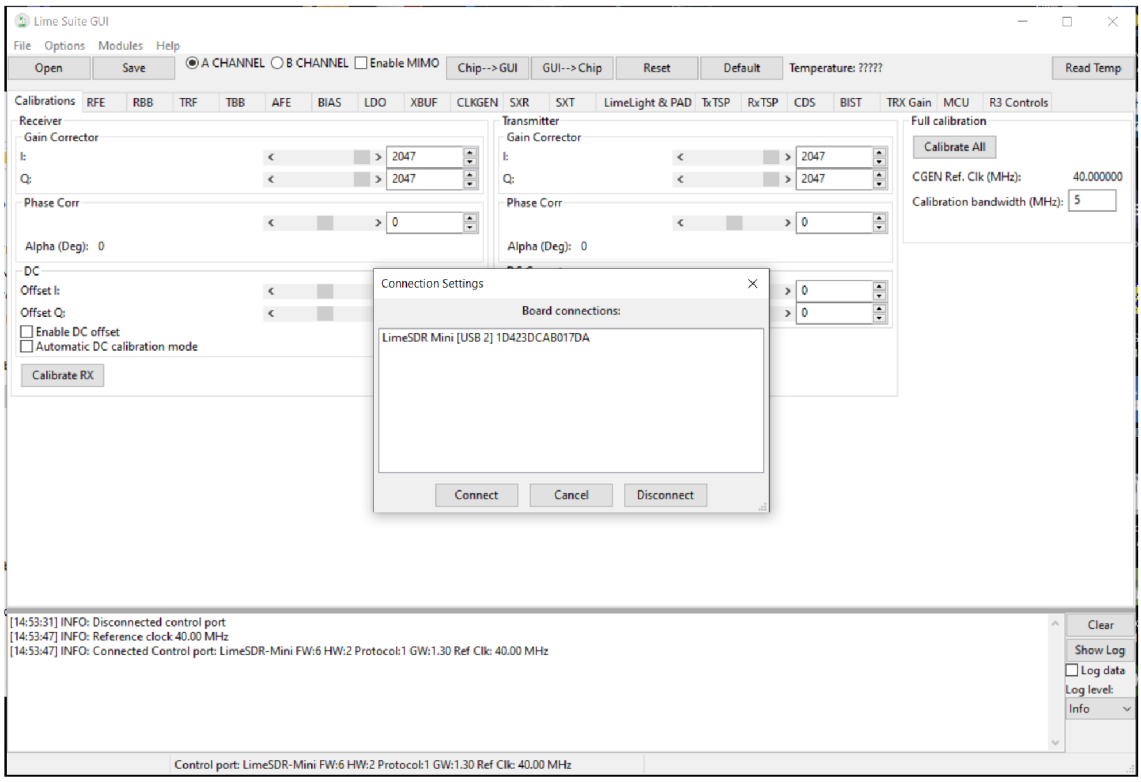
[30] Tp_crc32(): compute Zmodem-style CRC. *X-hacker* [online]. [cit. 2020-05-28]. Dostupné z: http://www.x-hacker.org/ng/telepath/ng3baf.html

[31] NAMÁRIË, Marcus. Release Candidate GNU Radio 3.8.1.0-rc1. *GNURadio* [online]. GNU Radio project, 2020 [cit. 2020-05-28]. Dostupné z: https://www.gnuradio.org/news/2020-02-16-gnu-radio-v3-8-1-0-rc1-release-candidate/

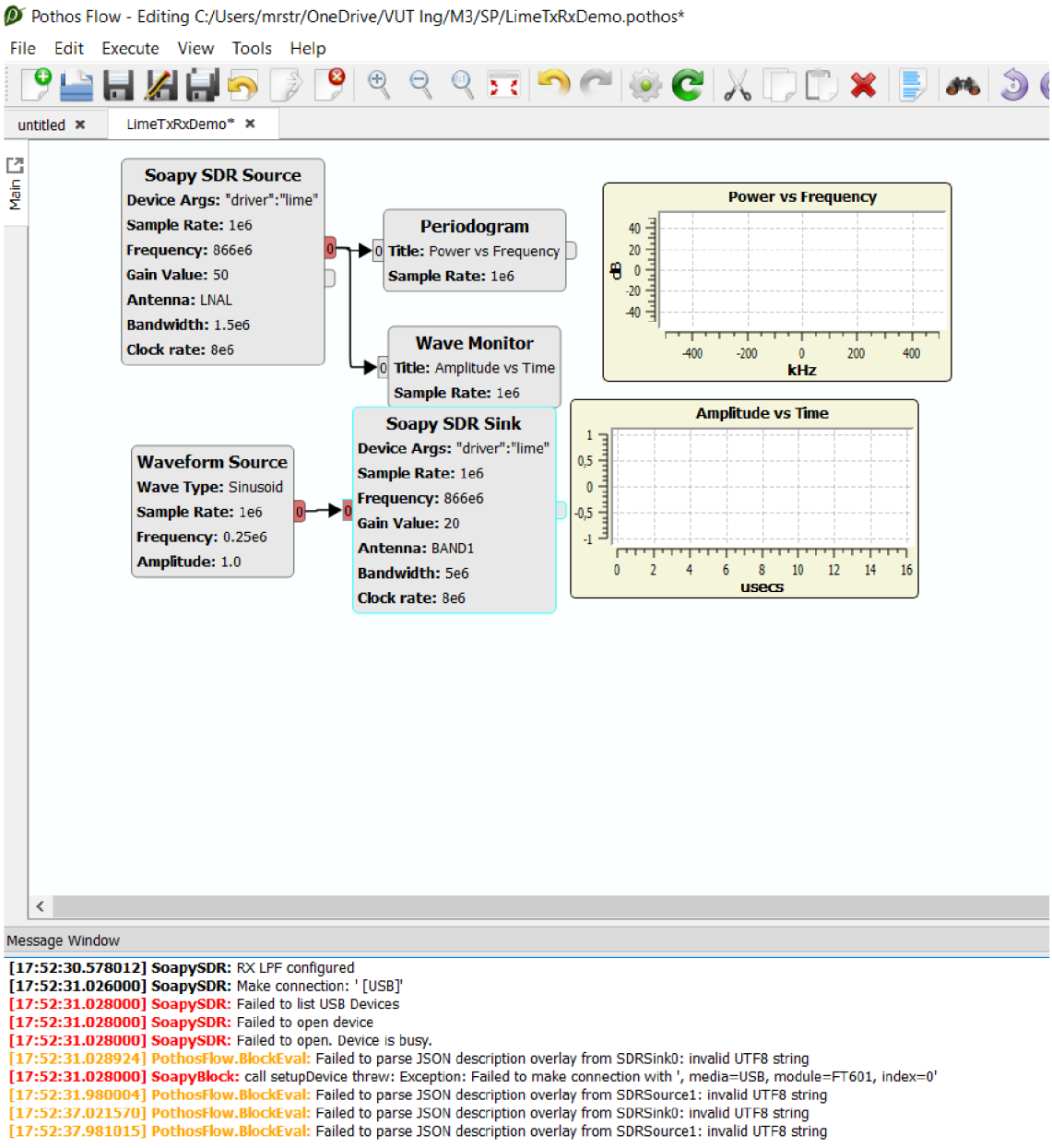
[32] BLOESSL, Bastian, Michele SEGATA, Christoph SOMMER a Falko DRESSLER. An IEEE 802.11a/g/p OFDM receiver for GNU radio. In: *Proceedings of the second workshop on Software radio implementation forum - SRIF '13* [online]. New York, New York, USA: ACM Press, 2013, 2013, s. 9- [cit. 2020-05-28]. DOI: 10.1145/2491246.2491248. ISBN 9781450321815. Dostupné z: http://dl.acm.org/citation.cfm?doid=2491246.2491248

Seznam příloh

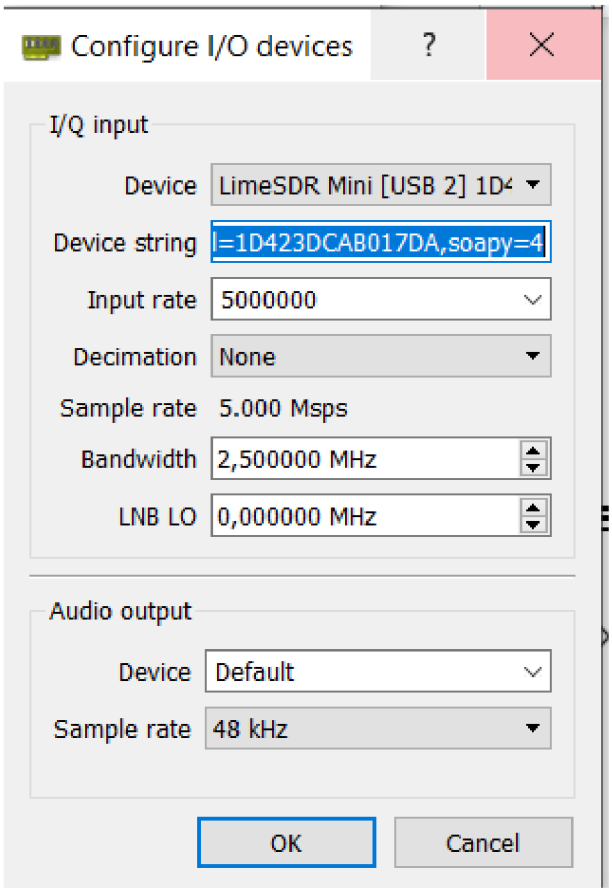
A Chybové hlášky použitých aplikací z prostředí Windows



Obr. A.1: Připojení LimeSDR mini k Lime Suite GUI.



Obr. A.2: Errory v logu aplikace PothosFlow.

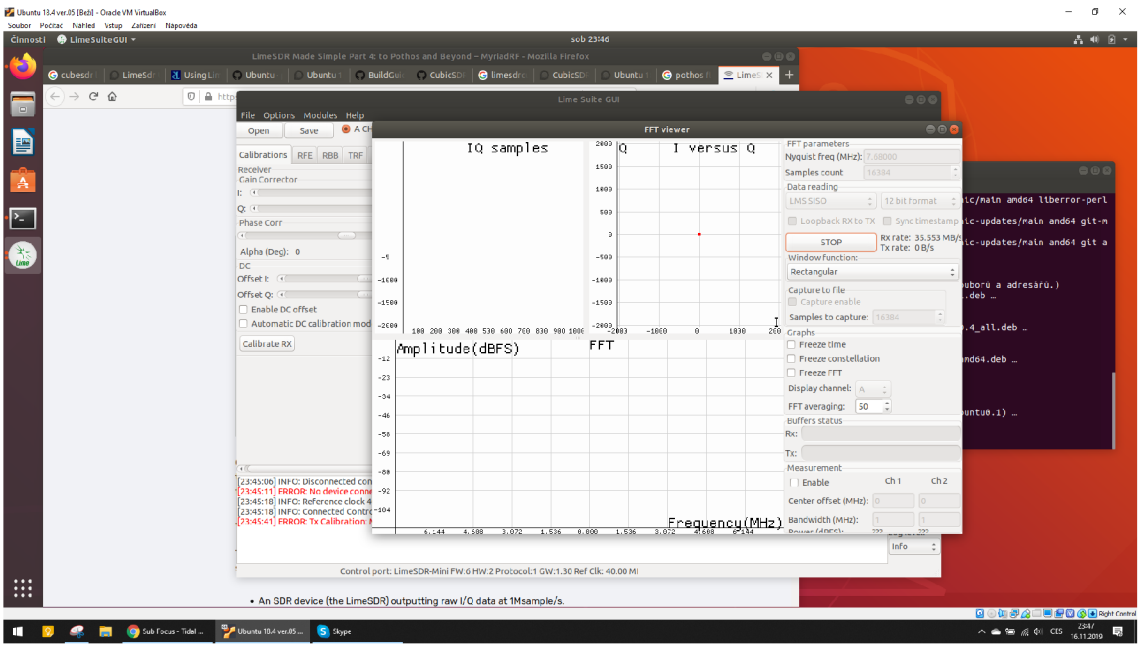


Obr. A.3: Nastavení parametrů před spuštěním GQRX.

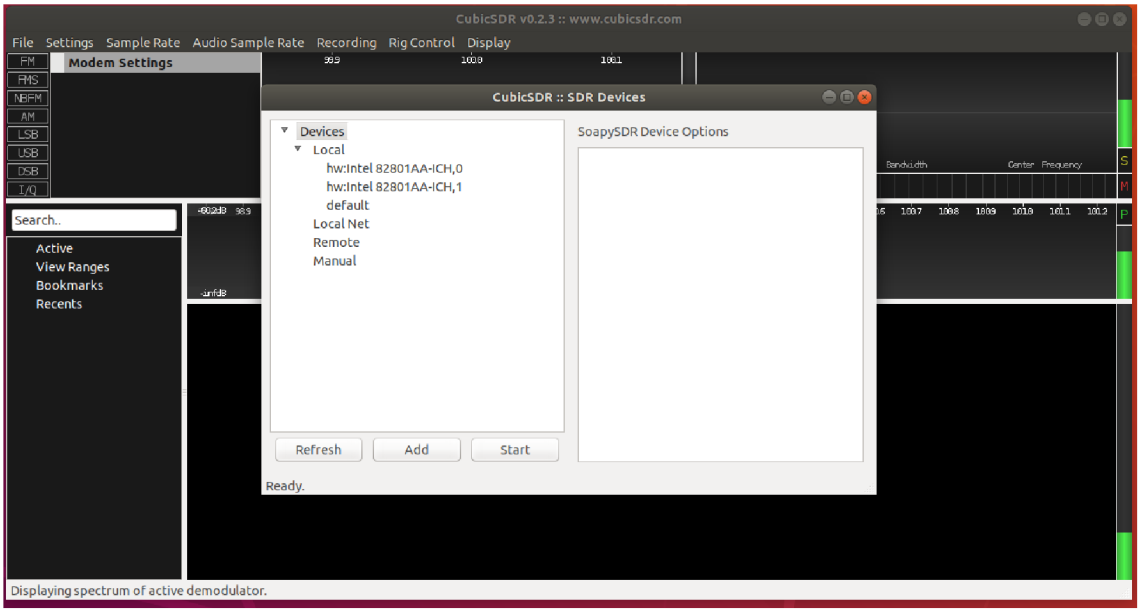
B Chybové hlášky použitých aplikací z prostředí Linux Ubuntu

```
martin@martin-VirtualBox:~$ LimeQuickTest --no-gui
[ TESTING STARTED ]
->Start time: Mon Nov 18 12:51:15 2019

->Device: LimeSDR Mini, media=USB 2.0, module=FT601, addr=24607:1027, serial=1D423DCAB017DA
Warning: USB3 not available
  Serial Number: 1D423DCAB017DA

[ Clock Network Test ]
->REF clock test
  Test results: 32611; 45808; 59005 - PASSED
->VCTCXO test
  Results : 6711088 (min); 6711243 (max) - PASSED
->Clock Network Test PASSED

[ FPGA EEPROM Test ]
->Read EEPROM
->Read data: 12 07 19 12 07 19 02
->FPGA EEPROM Test PASSED

[ LMS7002M Test ]
->Perform Registers Test
->External Reset line test
  Reg 0x20: Write value 0xFFFD, Read value 0xFFFD
  Reg 0x20: value after reset 0x0FFFF
->LMS7002M Test PASSED

[ RF Loopback Test ]
->Configure LMS
->Run Tests (TX_2 -> LNA_W):
  CH0 (SXR=1000.0MHz, SXT=1005.0MHz): Result:(-57.9 dBFS, -2.10 MHz) - FAILED
->Run Tests (TX_1 -> LNA_H):
  CH0 (SXR=2100.0MHz, SXT=2105.0MHz): Result:(-14.0 dBFS, 5.00 MHz) - PASSED
->RF Loopback Test FAILED

=> Board tests FAILED <=

Elapsed time: 3.78 seconds

martin@martin-VirtualBox:~$
```

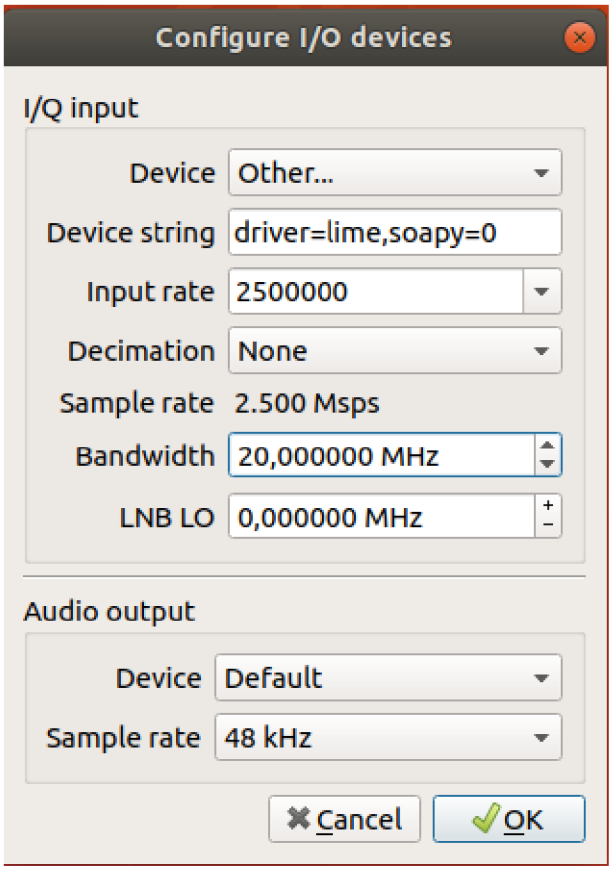
Obr. B.1: Výsledek LimeQuickTest v Linuxovém prostředí.



Obr. B.2: Zpětnovazební diagram programu Lime Suite.



Obr. B.3: Screenshot programu CubicSDR před jeho pádem.



Obr. B.4: Screenshot nastavených parametrů programu GQRX v Ubuntu Linux.

C Obsah přiloženého DVD

Obsahem přiloženého média jsou převážně .pcap soubory obsahující zachycenou komunikaci. Pro otevření .pcap souborů byl použit program Wireshark verze 3.2.3. Dále jsou přiloženy projekty programu GNU Radio verze 3.7.

```
/ ..... kořenový adresář přiloženého DVD
├── Projekty GNU Radia
│   ├── bladeRF_rx.grc
│   ├── Spektrozor.grc
│   ├── wifiprijimac.grc
│   ├── wifiprijimacrftap.grc
│   ├── wifiprijimac_s_LImeSDR.grc
│   ├── wifiprijimac_s_osmocom.grc
│   ├── wifi_phy_hier.grc
│   └── wifi_tx_s_LimeSDR.grc
├── Bezdrátová karta
│   ├── uvnitr_site.pcapng
│   └── vne_site.pcapng
├── bladeRF
│   ├── 2.4.1
│   │   ├── blade log.txt
│   │   ├── blade.pcap
│   │   ├── karta.pcapng
│   │   ├── LimeSDR log.txt
│   │   ├── LimeSDR.pcap
│   │   └── screen.png
│   ├── 2.4.2
│   │   ├── blade log.txt
│   │   ├── blade.pcap
│   │   └── karta.pcapng
│   └── 2.4.3
│       ├── blade log.txt
│       ├── blade.pcap
│       ├── karta.pcapng
│       └── záznam.mkv
└── LimeSDR
    ├── 2.3.4
    │   ├── karta.pcapng
    │   ├── karta_offset_6MHz.pcapng
    │   ├── karta_offset_11MHz.pcapng
    │   ├── log_offset_6MHz.txt
    │   ├── log_offset_11MHz.txt
    │   ├── SDR.pcap
    │   ├── SDR_offset_6MHz.pcap
    │   └── SDR_offset_11MHz.pcap
    └── 2.3.5
```

- karta.pcapng
- log.txt
- SDR.pcap
- 2.3.7
  - filesink
  - log.txt
  - SDR.pcap
  - záznam.mp4
- 2.3.8
  - karta.pcapng
  - log.txt
  - SDR.pcap
- 2.3.9
  - karta.pcapng
  - log.txt
  - SDR.pcap
  - záznam.mp4
- 2.3.10
  - log.txt
  - SDR.pcap
  - záznam.mkv
- obhajoba.pdf ..... prezentace k obhajobě
- prace.pdf ..... diplomová práce