FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Zadání bakalářské práce

| | |
|---|---|
| **Název:** | Aplikace pro bezpečnostní analýzu bezdrátové komunikace pomocí SDR |
| **Student:** | Aleksei Kravtsov |
| **Vedoucí:** | Ing. Jiří Dostál, Ph.D. |
| **Studijní program:** | Informatika |
| **Obor / specializace:** | Bezpečnost a informační technologie |
| **Katedra:** | Katedra počítačových systémů |
| **Platnost zadání:** | do konce letního semestru 2021/2022 |

## Pokyny pro vypracování

Softwarově definovaná rádia (SDR) se často používají pro testování zabezpečení bezdrátové komunikace. S jejich cenovou dostupností tak o ně roste zájem i ze strany útočníků. Umožňují různé typy útoků. např. jamming - zarušení frekvenčního pásma, což znemožní bezdrátovou komunikaci v daném pásmu, nebo replay attack - útok přehráním, kterým útočník může nahrát signál a následně ho použít, nebo tampering - zásah do komunikace, a další typy útoků. Cílem práce je navrhnout a realizovat aplikaci, která usnadní realizovat tyto útoky pro účely penetračního testování. Aplikace by měla umožňovat vizualizaci a zachycení signálů, demodulaci, dekódování a následnou editaci. Výslednou aplikace otestujte na reálných scénářích a zdokumentujte.

---

*Elektronicky schválil/a prof. Ing. Pavel Tvrdík, CSc. dne 30. ledna 2021 v Praze.*

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

# Aplikace pro bezpečnostní analýzu bezdrátové komunikace pomocí SDR

***Aleksei Kravtsov***

Katedra informační bezpečnosti
Vedoucí práce: Ing. Jiří Dostál, Ph.D.

13. května 2021

# Poděkování

Chtěl bych poděkovat vedoucímu práce, panu
Ing. Jiřímu Dostálovi, Ph. D., za vedení mé práce, konzultace, vysvětlení problematických bodů, jakož i za zapůjčení potřebného vybavení k testování funkčnosti vytvořené aplikace a provádění útoků na zařízení. Chtěl bych také poděkovat mým rodičům a přátelům za pomoc a podporu během celého studia.

# Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 2373 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu) licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 13. května 2021 . . . . . .

### Odkaz na tuto práci

Kravtsov, Aleksei. *Aplikace pro bezpečnostní analýzu bezdrátové komunikace pomocí SDR*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2021.

# Abstrakt

Účelem této práce je prozkoumat některé ze stávajících typů útoků prováděných pomocí SDR a také vytvořit aplikaci, která tyto útoky usnadňuje pomocí USRP B210 pro penetrační testování. Aplikace musí podporovat následující typy útoků: jamming, replay a reinjection.

Teoretická část práce popisuje základní prvky SDR, některé typy modulace signálu, stávající řešení pro provádění útoků a některé typy útoků na zařízení využívající bezdrátovou komunikaci.

Praktická část práce popisuje proces vývoje softwaru pro provádění útoků a také popisuje postup testování softwaru na scénářích útoků v laboratorních a reálných podmínkách na zařízení, jako je bezdrátový zvonek UBZ4 a meteorologická stanice DIVA GO 30.3018, vyráběná společností TFA.

**Klíčová slova** SDR, jamming attack, replay attack, reinjection attack, Universal Radio Hacker, GNU Radio, USRP B210, ASK, FSK, PSK, aplikace pro bezpečnostní analýzu bezdrátové komunikace pomocí SDR

# Abstract

The purpose of this work is to explore some of the existing types of attacks performed using SDR and also to create an application that facilitates these attacks using USRP B210 for penetration testing. The application must support the following types of attacks: jamming, replay and reinjection.

The theoretical part describes the basic elements of SDR, some types of signal modulation, existing solutions for performing attacks and some types of attacks on devices using wireless communication.

The practical part of the work describes the process of software development for attacks and also describes the procedure of software testing on attack scenarios in laboratory and real conditions on devices such as wireless bell UBZ4 and weather station DIVA GO 30.3018, manufactured by TFA.

**Keywords** SDR, jamming attack, replay attack, reinjection attack, Universal Radio Hacker, GNU Radio, USRP B210, ASK, FSK, PSK, SDR application for cybersecurity analysis of wireless communication

# Obsah

# Seznam obrázků

# Seznam tabulek

# Úvod

Bezdrátová komunikace je ve světě velmi využívaná. Na rozdíl od kabelové komunikace poskytují větší mobilitu, ale mají nižší rychlost příjmu a přenosu dat ve srovnání s drátovými komunikacemi, a je také obtížnější vyvinout prostředky pro příjem a přenos informací (je nutné vyřešit problém modulace a demodulace, a také dekódování signálu).

Při použití bezdrátové komunikace může útočník v zásadě narušit komunikaci (jamming attack), zachytit signál, zaznamenat a po chvíli jej znovu odeslat (replay attack) nebo jej změnit (reinjection attack). Proto je nutné zajišťovat bezpečnost bezdrátové komunikace. Například k ochraně standardu GSM se používá šifrovací algoritmus A5/1 nebo A5/2 [1]. K ochraně před replay attack používá mnoho výrobců automobilů rolling codes [2].

Ne všechna zařízení využívající bezdrátovou komunikaci však mají schopnost šifrovat data pro přenos nebo je chránit před různými typy útoků jiným způsobem. To je často způsobeno skutečností, že mnoho takových zařízení (bezdrátový zvonek, meteorologická stanice, další IoT zařízení) jsou zaměřena na nižší spotřebu energie, a pokud by byly použity šifrovací algoritmy a jiné metody ochrany před útoky, jejich spotřeba energie by byla vysoká.

Taková zařízení se tak mohou stát cílem útočníků. Je možné analyzovat bezdrátovou komunikaci těchto zařízení pomocí SDR. S rozvojem technologie softwarově definovaného rádia se tato zařízení stávají dostupnějšími, za 30$ je možné zakoupit zařízení, schopné pracovat v rozsahu 500 kHz - 1,7 GHz (bezdrátový zvonek popsaný v práci používá frekvenci 433,92 MHz, meteorologická stanice používá 868 MHz). Vzhledem k dostupnosti tohoto zařízení pro útočníka je nutné řešit problém zabezpečení bezdrátové komunikace.

## Cíl práce

Cílem rešeršní části práce je prostudování základních prvku SDR, typů modulace signálu, typů útoků na zařízení využívajících bezdrátovou komunikaci,

jakož i prostudování stávajících řešení pro provádění útoků.

Cílem praktické části práce je vytvořit aplikaci pro práci s SDR USRP B210, která usnadní jamming, replay a reinjection útoky a provést testování na zařízeních s nízkou úrovní zabezpečení (bezdrátový zvonek, meteorologická stanice).

Práce je rozdělena na 2 části: teoretickou a praktickou. Teoretická část obsahuje kapitoly „Základní prvky SDR“, „Typy modulace signálu“, „Typy útoků na zařízení využívající bezdrátovou komunikaci“ a „Stávající řešení pro provádění útoků“. Praktická část obsahuje kapitoly „Návrh funkce aplikace“, „Implementace aplikace“ a „Provádění útoků pomocí aplikací“.

Kapitola 1

# Základní prvky SDR

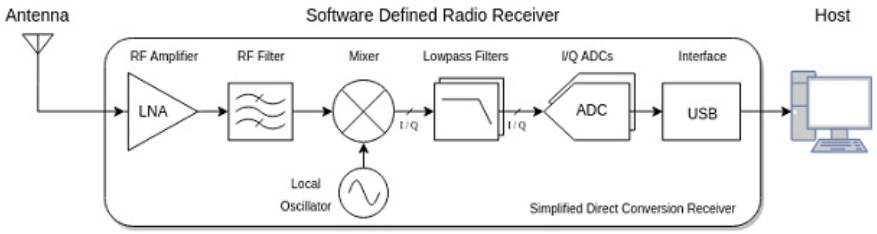
Tato kapitola popisuje princip SDR, jeho hlavní součásti a komunikační mody, které SDR může podporovat.

SDR je rádiový přijímač a/nebo rádiový vysílač využívající technologii, ve které jsou komponenty tradičně implementované v hardwaru (zesilovače, filtry, modulátory atd.) a jsou zodpovědné za zpracování signálu, implementovány pomocí softwaru. Také SDR během provozu umožňuje měnit mnoho parametrů, jako je frekvenční rozsah, typ modulace, citlivost atd. [3].

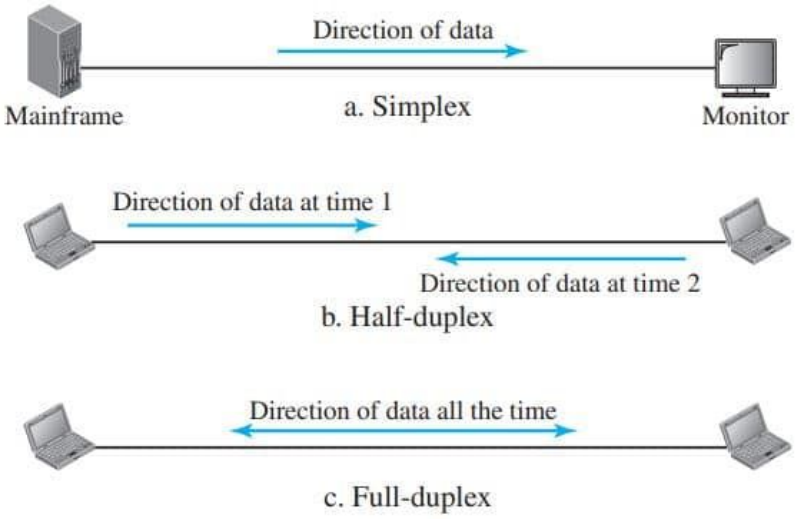
SDR lze použít nejen k implementaci rádiových modemů (GSM, WiFi atd.), ale také ke prozkoumání rádiových protokolů používaných zařízeními využívajícími bezdrátovou komunikaci a také k provádění penetračních testů zařízení využívajících bezdrátové komunikace.

Jak je popsáno v článku [3], SDR se v ideálním případě skládá z antény a ADC, v tomto případě digitální signálový procesor čte signály přímo z ADC a podle potřeby je představuje pomocí softwaru. Ideální případ není proveditelný z důvodu technických omezení. Hlavním problémem je obtížnost převodu signálu z analogové formy na digitální formu a to s vysokou rychlostí a vysokou přesností, bez vzniku rušení a bez pomoci elektromagnetické rezonance.

Článek [4] tedy popisuje následující základní prvky SDR: anténa, směšovač, dolní propust a ADC. Obrázek 1.1 ukazuje hlavní prvky přijímače SDR.




Obrázek 1.1: Základní prvky SDR přijímače. Převzato z [3]




Obrázek 1.2: Komunikační režimy. Převzato z [5]

## 1.1 Anténa

Jak je popsáno v článku [6], anténa je elektrotechnické zařízení pro příjem nebo odesílání rádiového signálu. Antény lze rozdělit na přijímací antény, vysílací antény a vysílací a přijímací antény (takové antény mohou buď přijímat nebo odesílat signál, ale nemohou to dělat současně).

SDR tedy podporují několik komunikačních režimů: simplexní (komunikace probíhá pouze v jednom směru) a poloduplexní (komunikace probíhá v obou směrech, ale v jednom okamžiku může nastat buď příjem, nebo přenos signálu. USRP B210, popsané v kapitole „Stávající řešení pro provádění útoků“, a některé další SDR, mohou také pracovat v plně duplexním režimu (komunikace probíhá v obou směrech a v jednom okamžiku může dojít k příjmu i přenosu signálu) pomocí několika antén [8]. Obrázek 1.2 ukazuje tyto režimy komunikace.

Důležitými parametry antén jsou

1. Zisk antény
2. Šířka přenášeného pásma
3. Směrovost antény

Zisk antény udává, kolikrát větší výkon přijímací anténa poskytuje buď vůči půlvlnnému dipólu nebo vůči teoretické dokonale všesměrové anténě, tzv. izotropnímu zářiči, jednotkou je 1 decibel, zkratkou dBi se vyjadřuje zisk antény v porovnání s izotropní anténou, dBd zisk v porovnání s půlvlnným dipólem [6].

Šířka pásma je rozdíl mezi nejvyšší a nejnižší frekvencí přenášeného signálu [7]:

$$B = f_H - f_L$$

Vyjadřuje se v hertzech (Hz).

Všesměrové antény vysílají signál rovnoměrně ve všech směrech, na rozdíl od směrových antén, které vysílají signál pouze do konkrétního sektoru, což zvyšuje výkon v tomto sektoru.

## 1.2 Směšovač

Jak je uvedeno v učebnicí [9], většina moderních přijímačů je postavena jako superheterodyn. Založen na kmitočtové přeměně kmitočtu signálu $f_s$ na vhodnější kmitočet mezifrekvenční $f_{mf}$ pomocí signálu heterodynu o kmitočtu $f_h$.

V směšovači dochází k vlastnímu procesu směšování, každý měnič kmitočtu vytváří různé kombinace obou vstupních signálů $f_s$ a $f_h$.

Pro výstupní signál pak platí

$$f_{mf} = kf_h + lf_L, k, l \in Z$$

Pokud koeficienty mají hodnoty $k$ = *1*, $l$ = *-1* výsledný vztah se bude jmenovat rozdílový směšovací produkt. Rozdílový směšovací produkt $f_h - f_s$ se většinou používá v přijímačové technice, protože vytváří nízký kmitočet $f_{mf}$ a dobře se v následujících obvodech přijímače zpracovává.

## 1.3 Dolní propust

Dolní propust je filtr, který efektivně předává frekvenční spektrum signálu pod určitou frekvenci a potlačuje frekvence nad touto frekvencí.

Ideální dolní propust zcela potlačuje všechny frekvence vstupního signálu nad určitou frekvenci a předává všechny frekvence pod touto frekvencí beze změny. Mezi frekvencí potlačení a propustného pásma neexistuje žádná přechodová zóna. Ideální dolní propust lze teoreticky realizovat pouze vynásobením spektra (Fourierova transformace) vstupního signálu pravoúhlou funkcí ve frekvenční doméně nebo převodem signálu v časové doméně pomocí sinc funkce.

Takový filtr však nelze v praxi implementovat, protože sinc funkce má nenulové hodnoty pro všechny časy až do nekonečna a impulsní odezva ideálního filtru je nenulová pro časy menší než nula.

Rádiové vysílače používají dolní propusti k blokování harmonických emisí, které mohou interagovat s nízkofrekvenčními užitečnými signály a interferovat s jinými elektronickými zařízeními [10].

## 1.4 ADC

ADC jsou zařízení, která přijímají analogové vstupní signály a generují odpovídající digitální signály vhodné pro zpracování mikroprocesory a jinými digitálními zařízeními. Postup analogově-digitálního převodu spojitých signálů lze rozdělit na dvě nezávislé operace: vzorkování a kvantování.

Diskretizace spojitých signálů je založena na základní možnosti jejich reprezentace ve formě vážených součtů

$$U(t) = \sum_j a_j f_j(t)$$

Kde $a_j$ jsou počty, které charakterizují původní signál v diskrétních časech, $f_j(t)$ je sada základních funkcí používaných k obnovení signálu z jeho vzorků.

Nejběžnější formou vzorkování je jednotné vzorkování, které je založeno na vzorkovací větě. Podle této věty by měly být jako koeficienty $a_j$ použity okamžité hodnoty signálu $U(\mathrm{t}_j)$ v diskrétních časových okamžicích $t_j = j\Delta t$ a perioda vzorkování by měla být vybrána z podmínky $\Delta t = 1/2F_m$, kde $F_m$ je maximální frekvence spektra převedeného signálu [11].

Kapitola 2

# Typy modulace signálu

Tato kapitola popisuje principy analogové a digitální modulace signálu. V téměř každém radiotechnickém zařízení jsou informace přenášeny elektromagnetickými vlnami, jejichž frekvence je mnohem vyšší než frekvence informačního signálu. V tomto ohledu je nutné změnit parametry vysílacího signálu v souladu se zákony o změně parametrů informačního signálu. Nejběžnějšími proměnnými parametry jsou amplituda, fáze a frekvence.

Modulace je proces převodu informačního, obecně nízkofrekvenčního signálu na vysokofrekvenční signál určený k přenosu přes rádiové spojení, se změnou kteréhokoli z jeho parametrů v souladu s přenášeným signálem [12].

## 2.1 Analogové modulace

Analogová modulace je technika fyzického kódování, při které se informace kódují změnou amplitudy, frekvence nebo fáze signálu sinusové nosné [13]. Obrázek 2.1 ukazuje nosné frekvence a typy analogové modulace.

### 2.1.1 AM

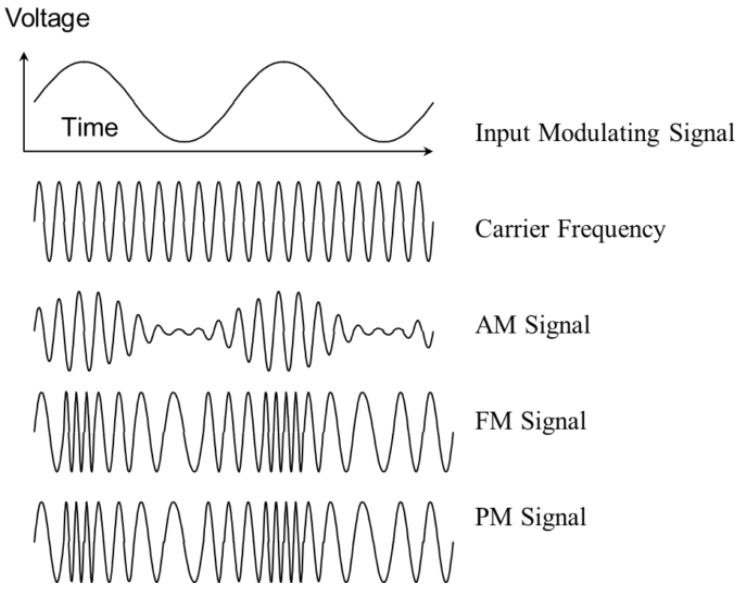
Jak je uvedeno v článku [14], amplitudová modulace je jedním z nejjednodušších typů analogové modulace. V závislosti na změně modulačního signálu se mění amplituda nosného signálu. Frekvence ani fáze nosné vlny se u této modulace nemění. Předpokládejme, že nosnou vlnu modulujeme jednoduchým harmonickým modulačním signálem o konstantní frekvenci. Nosnou vyjádříme následujícím vztahem:

$$n(t) = Nsin(\Omega t)$$

Kde $N$ je amplituda nosné a $\Omega$ je její úhlová frekvence.

Jednoduchý harmonický signál $m(\mathrm{t})$ jímž chceme nosnou modulovat můžeme popsat vztahem:

$$m(t) = Msin(\omega t + \phi)$$




Obrázek 2.1: Typy analogové modulace. Převzato z [15]

Kde $\phi$ je fázový posuv vůči nosné $n$(t). Amplitudová modulace vznikne přidáním signálu $m$(t) k amplitudě nosné $N$.

Dosadíme-li do vztahu pro nosnou, dostáváme:

$$y(t) = (N + Msin(\omega t + \phi))sin(\omega t)$$

### 2.1.2 FM

Jak je uvedeno v článku [16], principem frekvenční modulace je závislost okamžité frekvence nosné vlny na změnách amplitudy modulačního signálu. Informace je tedy kódována nikoliv změnou amplitudy nebo fáze, ale změnou frekvence nosné vlny. Obecně bude mít nosná vlna následující průběh:

$$u_n(t) = U_n sin(\Omega t + \phi)$$

Kde $U_n$ je amplituda nosné, $\Omega$ je úhlová frekvence nosné a $\phi$ fáze. V případě frekvenční modulace je funkcí času právě úhlová frekvence $\Omega$.

Úhlovou frekvenci jako harmonickou funkci času můžeme vyjádřit vztahem:

$$\Omega t = \Omega + \Delta\Omega cos(\omega t)$$

Kde $\Delta\Omega$ je frekvenční zdvih, $\omega$ pak úhlová frekvence modulační vlny.

Po dosazení do rovnice nosné vlny a položením fázového posuvu $\phi = 0$ (jeho velikost je konstantní a nemá vliv na výsledek dalších odvození a výpočtů) dostáváme vztah:

$$u_n(t) = U_n sin(\Phi(t, \omega))$$

Kde funkce $\Phi(t, \omega)$ je okamžitá fáze napětí a pro $\phi = 0$ je integrálem úhlové frekvence $\Omega(t)$ podle $t$.

Platí tedy:

$$\Phi(t,\omega) = \int \Omega(t)\,\mathrm{d}t = \int(\Omega + \Delta\Omega\cos(\omega t))\mathrm{d}t = \Omega t + \frac{\Delta}{\Omega}\omega\sin(\omega t)$$

Dále zavádíme parametr zvaný modulační index FM označený $m_{FM}$:

$$m_{FM} = \frac{\Delta\Omega}{\omega} = \frac{2\pi\Delta f}{2\pi f_m}$$

Kde $\Delta f$ je frekvenční zdvih a $f_m$ frekvence modulačního signálu.

Dosazením funkce $\Phi(t,\omega)$ zpět do rovnice $u_n = U_n sin(\Phi(t,\omega))$ dostáváme obvyklý tvar rovnice frekvenčně modulované vlny:

$$u_n(t) = U_n sin(\Omega t + m_{FM} sin(\omega t))$$

### 2.1.3 PM

Jak je uvedeno v článku [17], fázová modulace je druh modulace, u které mění modulační signál fázi nosné vlny. Předpokládejme, že modulační signál má frekvenci $\omega_m$ a fázi $\phi_m$. Lze ho tedy popsat rovnicí:

$$m(t) = Msin(\omega_m t + \phi_m)$$

Nosnou lze podobně popsat rovnicí:

$$c(t) = Csin(\omega_c t + \phi_c)$$

Po dosazení je modulovaný signál popsán vztahem:

$$y(t) = Csin(\omega_c t + m(t) + \phi_c)$$

## 2.2 Digitální modulace

Jak je uvedeno v článku [18], hlavní myšlenkou digitální modulace je, že každá možná hodnota přenášených symbolů je spojena s některými parametry analogové nosné vlny. Obrázek 2.2 ukazuje typy digitální modulace.

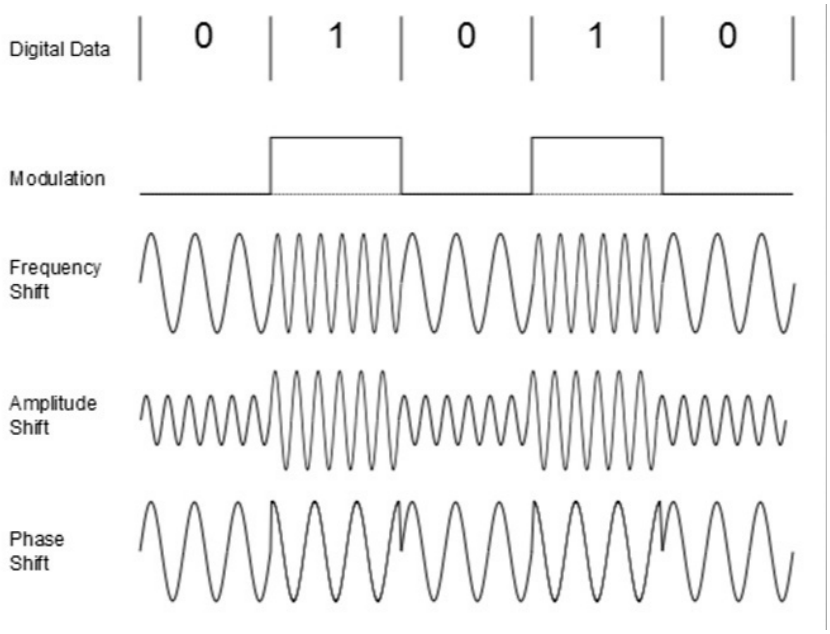
### 2.2.1 ASK

Jak je uvedeno v článku [19], klíčování amplitudovým posuvem je forma amplitudové modulace, která reprezentuje digitální data pomocí změn amplitudy nosné vlny.

Každá digitální modulace používá pro reprezentaci digitálních dat konečný počet diskrétních signálů. ASK používá konečný počet amplitud, a každé z nich je přiřazen určitý vzorek binárních čísel. Obvykle každá amplituda kóduje stejný počet bitů. Každý bitový vzorek tvoří symbol, který je reprezentován konkrétní amplitudou.

### 2.2.2 FSK

Jak je uvedeno v článku [20], klíčování frekvenčním posuvem je metoda frekvenční modulace, u které se přenáší digitální informace pomocí diskrétních změn frekvence nosné vlny.




Obrázek 2.2: Typy digitální modulace. Převzato z [21]

Nejjednodušší FSK je binární FSK, která používá dvou frekvencí pro přenos binární informace (jedniček a nul). U binární FSK se frekvence použitá pro přenos jedničky nazývá značková frekvence, frekvence pro přenos nuly mezerová frekvence.

### 2.2.3 PSK

Jak je uvedeno v článku [22], klíčování fázovým posuvem je metoda digitální modulace, která pro přenos informací používá změny fáze referenčního signálu (nosné vlny).

Digitální modulace používají pro reprezentaci digitálních dat konečný počet signálů. U PSK se tyto signály liší různými posuvy fáze, z nichž každý reprezentuje určitou hodnotu jednoho nebo několika bitů. U většiny metod každá fáze kóduje stejný počet bitů. Každý bitový vzor tvoří tak zvaný symbol, který je reprezentován určitým fázovým posuvem.

Kapitola 3

# Typy útoků na zařízení využívající bezdrátovou komunikaci

Tato kapitola popisuje některé typy útoků na zařízení využívající bezdrátovou komunikaci a také způsoby obrany proti nim. V praktické části práce popisuje kapitola „Provádění útoků pomocí aplikací“ provedení útoků v laboratorních a reálných podmínkách na zařízení, která nepoužívají bezpečnostní nástroje pro zabezpečení bezdrátovou komunikaci.

## 3.1 Jamming útok

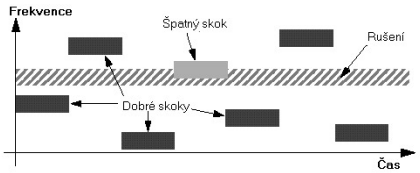
Jamming útok je jeden z nejjednodušších typů útoků na zařízení využívající bezdrátovou komunikaci. Pri provedeni útoku na vybranou frekvenci generuje špatný signál, ktery může snížit rychlost přenosu dat nebo zcela znemožnit komunikaci na této frekvenci [23].

Jak je popsáno v článku [24], existují 4 nejběžnější typy jamming útoků:

1. Constant jammer. Při útoku útočník nepřetržitě vysílá náhodny signál nebo náhodnou sekvenci bitů, která ruší komunikaci na dané frekvenci. S tímto útokem je frekvence neustále zaneprázdněná, ale provedení tohoto typu útoku vyžaduje spoustu energie.

2. Deceptive jammer. Tento útok je podobný útoku popsanému v constant jammer, ale útočník neposílá náhodnou sekvenci bitů, ale informace v normální formě, ve které je nejake zařízení může přijímat.

3. Random jammer. Na rozdíl od constant a deceptive jammeru signál není odesílán nepřetržitě, ale jammer mění svůj stav mezi aktivním a deaktivovaným režimem.




Obrázek 3.1: Přeskakování frekvenci. Převzato z [25]

4. Reactive jammer. Na rozdíl od random jammeru je v deaktivovaném režimu a analyzuje frekvenci a vychází z deaktivovaného režimu pouze při zahájení přenosu dat.

Článek [24] popisuje několik způsobů obrany před tímto útokem:

1. Snížení vysílacího výkonu může pomoci proti reactive jammeru, protože je obtížnější detekovat přenos dat při nízkém vysílacím výkonu.

2. Rozsíření spectru frekvence a přeskakování frekvenci. V tomto případě se informace odesílají v paketech, frekvence se mění podle určitého algoritmu, na kterém se přijímací a vysílací zařízení dohodly před zahájením přenosu.

3. Využiti směrových antén. Na rozdíl od všesměrových antén směrové antény vysílají a přijímají informace pouze v jednom směru. Pokud je však jammer umístěn ve stejném směru jako anténa, je možné provést úspěšný útok.

## 3.2 Replay útok

Jeden z nejběžnějších typů útoků je založen na zachycení signálu a jeho odeslání ve správnou chvíli pro útočníka. První fází útoku je určení centrální frekvence, na které zařízení pracuje. Útočník pak může poslouchat tuto frekvenci a zaznamenávat signály odesilany ze zařízení. Dalším krokem v útoku je odstranění šumu ze signálu, aby zůstaly pouze nezbytné informace. Poté, po zpracování signálu, může útočník buď začít odesílat signál nepřetržitě, nebo jej odeslat v určitých časech [26].

V důsledku útoku popsaného v kapitole „Provádění útoků pomocí aplikací“ zvonek neustále pracoval, meteorologická stanice zobrazovala nesprávná data.

Článek [27] popisuje několik způsobů obrany před tímto útokem:

1. Použití náhodného šifrovacího klíče, který je platný pouze pro jednu komunikační relaci.

2. Použití časových značek k omezení platnosti dat ve zprávě.

3. Použití hesel, která jsou pro každou komunikační relaci jedinečná.

Článek [2] také popisuje jednu z metod obrany: rolling codes.
Zařízení, které odesílá signál, a zařízení, které přijímá signál, musí mít stejný generátor pseudonáhodných čísel. V tomto případě zařízení, které vysílá signál, generuje kód, který je odeslán spolu se zprávou. Zařízení, které přijímá signál, také generuje kód a kontroluje, zda se kódy shodují. Pokud se kódy shodují, obě zařízení vygenerují nový kód, který bude použit v další komunikační relaci.

Jelikož existuje možnost, že zařízení, které přijímá signál, jej nezjistí (například kvůli jamming útoku na frekvence) a dojde k desynchronizaci - při každém použití kódu se navíc vytvoří seznam následujících kódů. Odesláním některého z těchto kódů se zařízení synchronizují.

## 3.3 Reinjection útok

Jak je popsáno v článku [28], reinjection útok je podobný replay útoku, ale v tomto případě se před odesláním zaznamenaného signálu změní jeho obsah.

První kroky útoku se shodují s replay útokem, ale v tomto případě je po zpracování a extrakci signálu nutné jej demodulovat a dekódovat a provést reverzní analýzu použitého protokolu. Pro reverzní analýzu protokolu je často nutné zaznamenat mnoho signálů obsahujících různá data a poté ze zprávy extrahovat části payloadu pro jejich následnou úpravu.

K ověření integrity dat se často taký používá funkci cyklického redundantního součtu [29]. V tomto případě při provádění reverzní analýzy protokolu je nutné najít parametry funkce (generující polynom atd.). To je často obtížný úkol. Po provedení zpětné analýzy protokolu a změně dat je nutné vypočítat CRS, v případě potřeby zakódovat signál a provést jeho modulaci. Poté zbývá pouze začít vysílat signál neustále nebo v určitém okamžiku.

V této práci byla pri provedení tohoto typu útoku provedena reverzní analýza protokolu, který využívá meteorologická stanice TFA DIVA GO 30.3018. Proces a výsledek reverzní analýzy je popsán v podkapitole „Reverzní analýza použitého protokolu“.

Kapitola 4

# Stávající řešení pro provádění útoků

Tato kapitola popisuje existující software používaný v této práci k vytváření softwaru nebo k provádění útoků, a taký SDR používané k provádění útoků.

Software URH popsaný v této kapitole byl použit k provedení reinjection útoku na meteorologickou stanici, což je popsáno v kapitole „Provádění útoků pomocí aplikací“, toolkit GNU Radio, taký popsaný v této kapitole byl použit k vytvoření vlastní aplikace pro provádění jamming, replay a reinjection útoků. Proces vytváření aplikace je popsán v kapitolách „Návrh funkce aplikace“ a „Implementace aplikace“.

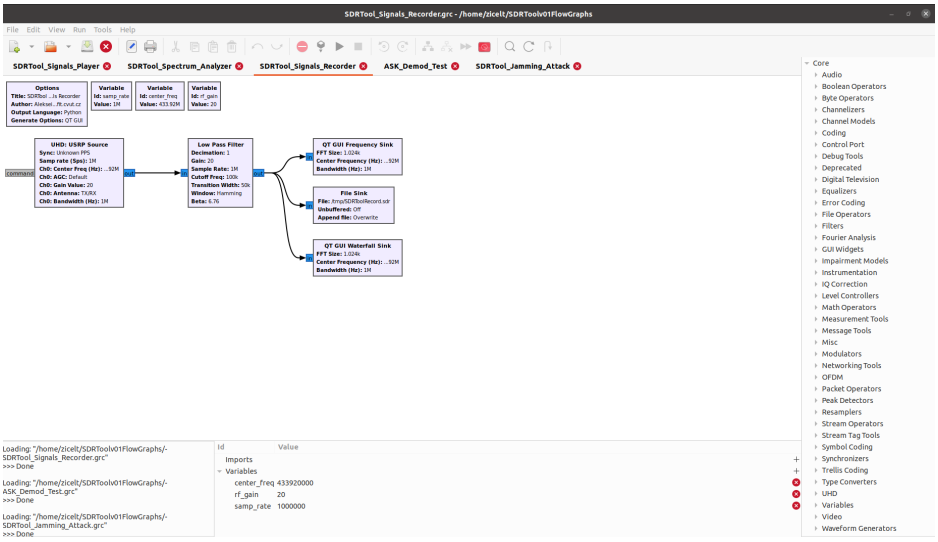
## 4.1 GNU Radio

GNU Radio poskytuje framework a nástroje pro tvorbu a spouštění softwarových rádií a aplikací určených ke zpracování signálu. Samotné GNU Radio aplikace jsou nazývány jako „flow grafy“, což jsou série vzájemně propojených bloků zpracování signálu. Tyto flow grafy mohou být napsány v programovacích jazycích C++ nebo Python. Jádro GNU Radio je napsáno v C++, spousta uživatelských nástrojů je však napsána v Pythonu.

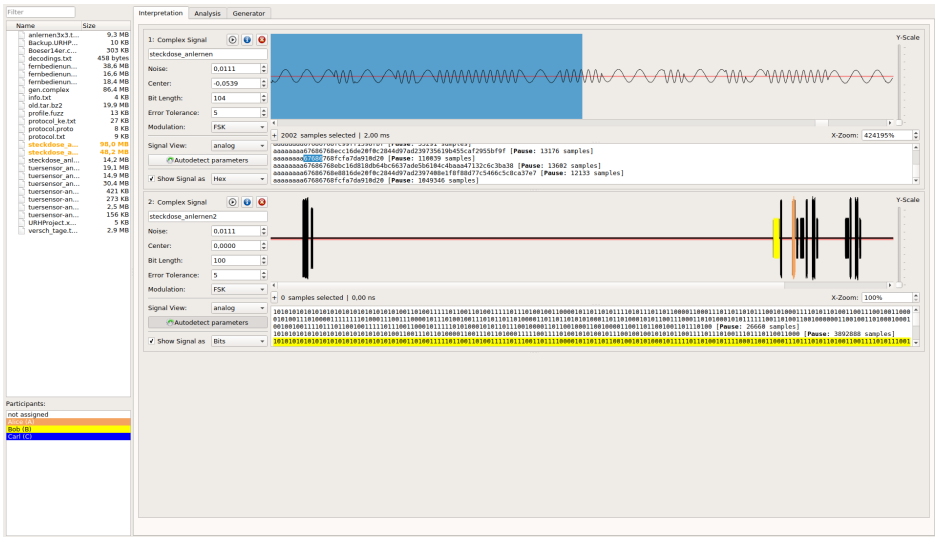
GNU Radio je publikováno jako svobodný software pod licencí GNU General Public License [30]. Při vývoji aplikace v rámci této práce byla použita verze GNU Radio 3.10. Na obrázku 4.1 uveden GUI GNU Radio Companion.

## 4.2 Universal Radio Hacker

Universal Radio Hacker (URH) je kompletní sada pro prozkoumání bezdrátových protokolů s nativní podporou mnoha běžných SDR. URH umožňuje snadnou demodulaci signálů v kombinaci s automatickou detekcí modulačních para-



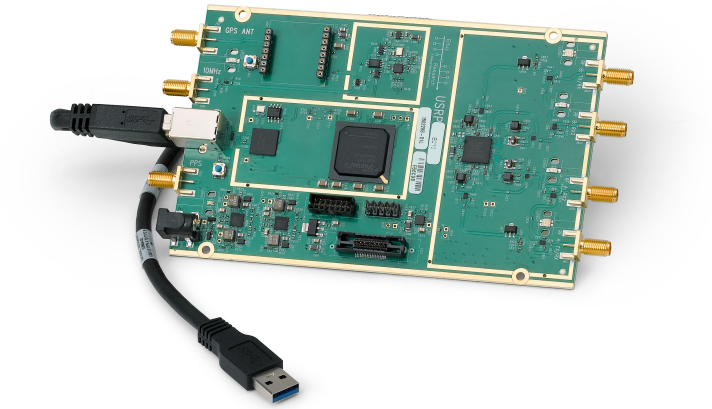
Obrázek 4.1: GUI GNU Radio Companion v 3.10



Obrázek 4.2: GUI URH. Převzato z [31]

metrů. Jelikož se data před přenosem často kódují, nabízí URH přizpůsobitelné dekódování. Pokud jde o reverzní inženýrství protokolů, URH je užitečné dvěma způsoby. Můžete buď ručně přiřadit pole protokolu a typy zpráv, nebo nechat URH automaticky odvodit pole protokolu [31].

K provádění útoků popsaných v kapitole „Provádění útoků pomocí aplikací“ se používá URH verze 2.9.1. Na obrázku 4.2 uveden GUI URH.



Obrázek 4.3: USRP B210, převzáto z [32]

## 4.3 USRP B210

USRP B210 je plně integrované jednodeskové zařízení od společnosti Ettus Research. Má frekvenční rozsah 70 MHz - 6 GHz a díky transceiveru AD9361 RFIC podporuje v reálném čase šířku pásma až 56 MHz. SDR podporuje half duplex a full duplex, má konfiguraci 2x2 MIMO, díky níž je možné použít dvě antény pro odesílání a dvě antény pro příjem signálu [32].

USRP B210 je podporován v GNU Radio pomocí USRP Hardware Driver, který umožňuje použití tohoto SDR k vytváření a testování vlastního softwaru pro provédení útoků.

Kapitola 5

# Návrh funkce aplikace

Tato kapitola popisuje požadovanou funkčnost vytvořeného softwaru, architekturu softwaru a navrhuje implementaci softwarových funkcí pomocí nástroje GNU Radio, popsaného v kapitole „Stávající řešení pro provádění útoků“.

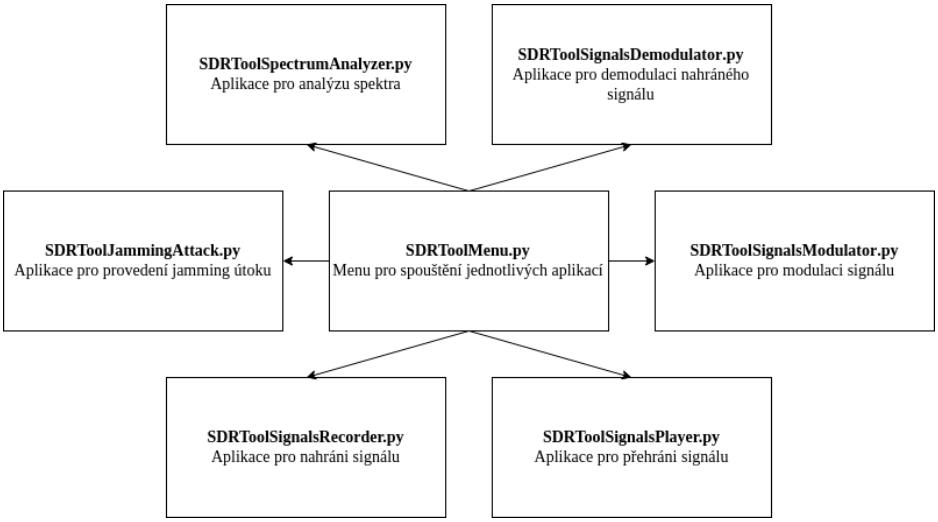
Kapitola „Stávající řešení pro provádění útoků“ také popisuje SDR USRP B210, vytvořený software je připraven pro použití s tímto typem SDR. Chcete-li přijímat a odesílat signály z USRP B210 v GNU Radio, existují bloky USRP Source a USRP Sink používané v flowgraphech při vytváření této aplikace.

Vytvořená aplikace by měla usnadnit proces provádění útoků popsaných v kapitole „Typy útoků na zařízení využívající bezdrátovou komunikaci“. Proto musí aplikace podporovat následující funkce:

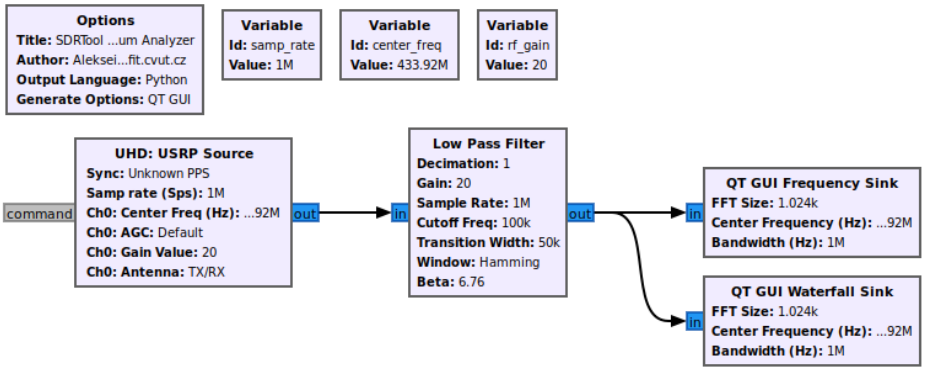
1. Analyzátor spektra
2. Provedení jamming útoku
3. Nahrávání signálu
4. Přehrání signálu
5. Modulace a demodulace signálu

## 5.1 Architektura aplikace

Software se bude skládat z několika aplikací, z nichž každá bude plnit jednu z funkci, které jsou popsány na začátku kapitoly. Spuštění každé z aplikací bude provedeno pomocí samostatné položky v menu. Obrázek 5.1 ukazuje navrhovanou softwarovou architekturu.




Obrázek 5.1: Navrhovaná softwarová architektura

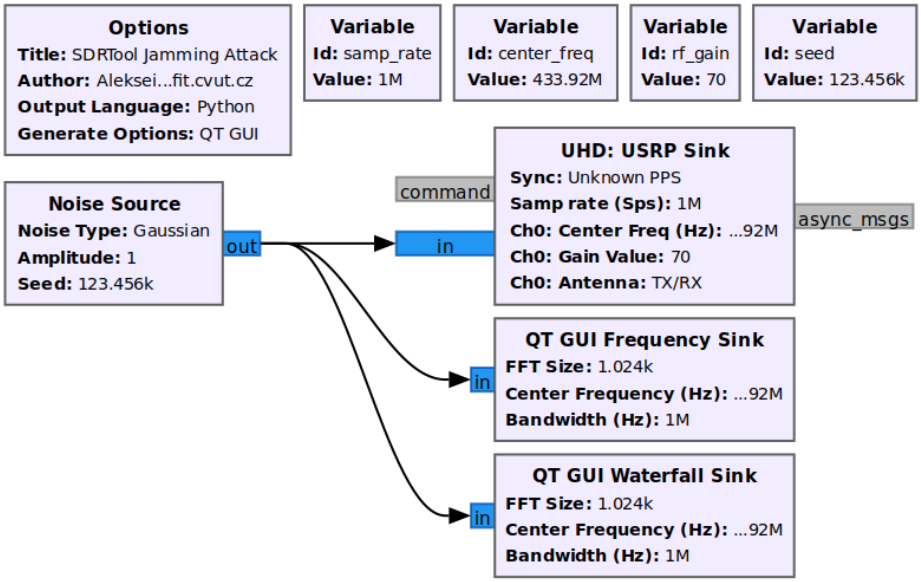



Obrázek 5.2: Flowgraph pro analyzátor spektra

## 5.2 Analyzátor spektra

Při provádění útoků je prvním krokem často určení centrální frekvence, na které zařízení využívající bezdrátovou komunikaci pracuje. Tuto schopnost poskytuje aplikace SDRTool Spectrum Analyzer. Jak již bylo zmíněno výše, GNU Radio má blok USRP Source, který umožňuje přijímat signály pomocí USRP B210. Poté je signál veden přes dolní propust a je zobrazen na dvou grafech: vodopádovém a frekvenčním.

Vzhledem k tomu, že aplikace má GUI a pro zahájení práce přijímá data od uživatele, jsou v GNU Radio vytvořeny proměnné, které přijímají informace o vzorkovací frekvenci (samp_rate), střední frekvenci (center_freq) a citlivosti (rf_gain). Obrázek 5.2 ukazuje výsledný flowgraph analyzátoru spektra.




Obrázek 5.3: Flowgraph pro provedení jamming útoku

## 5.3 Provedení jamming útoku

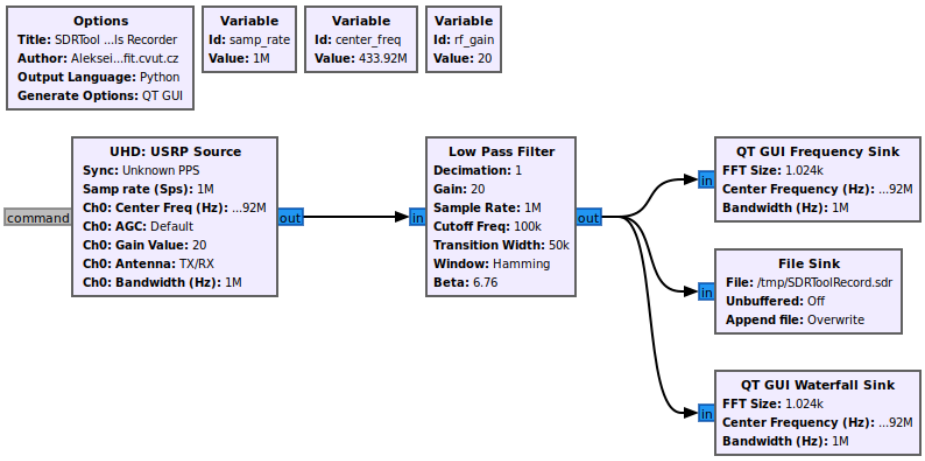
K provedení útoku bude použit generátor šumu, v GNU Radio se nazývá Noise Source. Kromě proměnných uvedených v podkapitole 5.2 byla přidána proměnná, která je vyžadována k inicializaci generátoru pseudonáhodných čísel (seed). Signál bude odeslán do bloku USRP Sink popsaného na začátku této kapitoly. Obrázek 5.3 ukazuje výsledný flowgraph pro provedení jamming útoku.

## 5.4 Nahrávání signálu

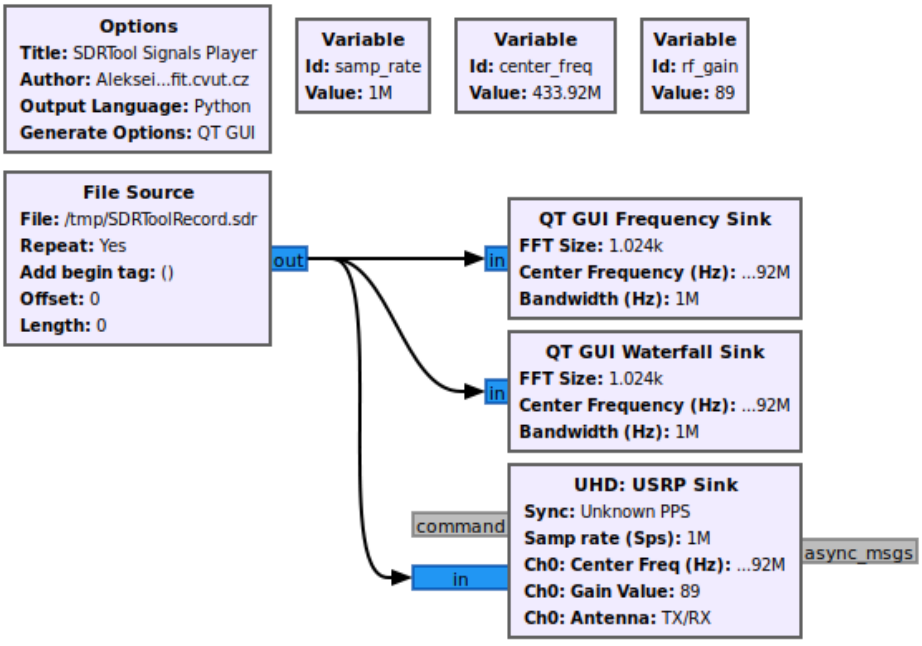
Flowgraph pro záznam signálu je do značné míry stejný, jak je popsáno v podkapitole 5.2, ale pro záznam signálu do souboru byl přidán blok s názvem File Sink. Obrázek 5.4 ukazuje výsledný flowgraph pro nahrávání signálu.

## 5.5 Přehrání signálu

Signál je odeslán do USRP B210 pomocí bloku s názvem File Source. V nastavení tohoto bloku lze nejen vybrat cestu k souboru obsahujícímu signál, ale také určit, zda má být signál odeslán jednou, nebo zda má být odeslán nepřetržitě. Obrázek 5.5 ukazuje výsledný flowgraph pro přehrání signálu.




Obrázek 5.4: Flowgraph pro nahrávání signálu




Obrázek 5.5: Flowgraph pro přehrání signálu

## 5.6 Modulace a demodulace signálu

Během vývoje softwaru bylo vytvořeno a otestováno několik flowgraphu na demodulaci a modulaci signálů v režimech ASK a FSK, testování nepotvrdilo funkčnost žádné z verzí, proto po dohodě s vedoucím práce tato funkce nebyla vytvořena, pro reinjection útoky bylo použito řešení Universal Radio Hacker popsané v kapitole „Stávající řešení pro provádění útoků“.

Kapitola 6

# Implementace aplikace

Tato kapitola popisuje strukturu softwaru, proces kontroly parametrů zadaných uživatelem a také implementaci aplikací, jejichž funkce jsou popsány v kapitole „Návrh funkce aplikace“. Jak je uvedeno v kapitole „Stávající řešení pro provádění útoků“ a v kapitole „Uživatelský manuál“, k vytvoření softwaru byly použity GNU Radio Companion v 3.10 a Python verze 3.8.5.

## 6.1 Struktura softwaru

Jak je navrženo v kapitole „Návrh funkce aplikace“, software byl rozdělen do několika aplikací, z nichž každou lze spustit pomocí menu SDRToolMenu.py. Všechny aplikace jsou psány pomocí knihovny tkinter, což usnadňuje vytváření GUI.

## 6.2 Menu

SDRToolMenu.py je nejjednodušší aplikace vytvořená v rámci bakalářskou práci. Nepoužívá třídy, používá pouze main funkci, která vytváří okno a volá funkci configureWindow pro konfiguraci okna a vytváření položek menu. Každá z položek menu, když na ni kliknu, spustí konkrétní program pomocí příkazu os.system.

## 6.3 Kontrola zadaných parametrů

Tento software byl navržen pro práci s USRP B210, ale pomocí GNU Radio lze jeho funkčnost rozšířit na práci s jinými SDR. Pokud USRP B210 při zadávání nesprávných parametrů (například RF Gain mimo povoleného rozsahu) vydá varování a neumožní spuštění aplikace, další SDR nemusí mít tuto funkci a při spuštění bude poškozeno.

V tomto ohledu obsahuje každý z vytvořených programů kontrolu dat zadaných uživatelem. V každém z programů je za tuto kontrolu zodpovědná funkce checkInputParameters. Kód 1 zobrazuje kód této funkce v aplikaci, která slouží k provedení jamming útoku.

Pokud funkce detekuje nesprávná data, vydá varování a pokud je to možné, nahradí nesprávná data standardními daty. Standardní hodnoty jsou uložené v souboru USRP_B210_Constants.py.

## 6.4 Analyzátor spektra

Aplikace vytvořená pro analýzu spektra vytvoří okno pro zadávání parametrů uživatelem pomocí funkce configureWindow, po potvrzení zadání dat pomocí této funkce zkontroluje zadané parametry popsané v podkapitole 6.3, pokud jsou parametry zadány správně, nebo byly nahrazeny standardními, volá se funkce mainSpectrumAnalyzer, která vytvoří objekt třídy SDRTool_Spectrum_Analyzer a spustí analýzu spektra. Tato třída byla vytvořena pomocí flowgraphu popsaného v kapitole „Návrh funkce aplikace“.

## 6.5 Provedení jamming útoku

Aplikace vytvořená k provedení jamming útoku byla vytvořena podle zásady popsané v části 6.4. Rozdíl je v tom, že ve funkce mainJammingAttack je vytvořen objekt třídy SDRTool_Jamming_Attack, který je zodpovědný za zahájení útoku ihned po kontrole dat od uživatele.

## 6.6 Nahrávání signálu

Aplikace pro nahrávání signálu se rovněž byla vytvořena podle principu popsaného v podkapitolách 6.4 a 6.5. Funkce pro kontrolu zadaných dat také kontroluje možnost vytvoření souboru se zadaným názvem v zadaném adresáři a v případě chyby vytvoří soubor s názvem SDRToolRecord.sdr v adresáři /tmp.

## 6.7 Přehrání signálu

Aplikace pro přehrání signálu se také byla vytvořena podle principu popsaného v podkapitolách 6.4 a 6.5. Funkce pro kontrolu zadaných dat také kontroluje existenci souboru se zadaným názvem v zadaném adresáři a v případě chyby vydá varování. Uživatel si může vybrat, zda bude signál přehrán jednou nebo opakovaně.

```
def checkInputParameters():
"""Check if input parameters are correct."""
    try:
        float(centerFrequency.get())
        except ValueError:
        centerFrequency.set(B210CENTERFREQUENCY)
        errorMessage = "Center frequency is not valid.
        Set default:" + str(B210CENTERFREQUENCY)
        mb.showerror("Error", errorMessage)
    try:
        float(sampleRate.get())
        except ValueError:
        sampleRate.set(B210SAMPLERATE)
        errorMessage = "Sample rate is not valid.
        Set default: "+str(B210SAMPLERATE)
        mb.showerror("Error", errorMessage)
    try:
        float(rfGain.get())
        except ValueError:
        rfGain.set(B210RFGAIN)
        errorMessage = "RF Gain is not valid.
        Can be from 0 to 89 dB. Set default: "
        +str(B210RFGAIN)
        mb.showerror("Error", errorMessage)
    try:
        int(seedRandom.get())
        except ValueError:
        seedRandom.set(B210SEED)
        errorMessage = "Seed is not valid.
        Can be from 0 to 89 dB. Set default: "
        +str(B210SEED)
        mb.showerror("Error", errorMessage)
    if (float(rfGain.get())<0
        or float(rfGain.get())>89):
        rfGain.set(B210RFGAIN)
        errorMessage = "RF Gain is not valid.
        Can be from 0 to 89 dB. Set default: "
        + str(B210RFGAIN)
        mb.showerror("Error", errorMessage)
    if __name__ == '__main__':
        mainJammingAttack()
```

Kod 1: Funkce pro kontrolu zadaných parametrů pro jamming útok

Kapitola 7

# Provádění útoků pomocí aplikací

Tato kapitola popisuje postup a výsledky jamming, replay a reinjection útoků na bezdrátový zvonek UBZ4 [33] a meteostanice TFA DIVA GO 30.3018 [34]. Útoky byly proveděny jak v laboratorných, tak i ve realných podmínkách. Při provádění útoků bylo použito SDR USRP B210, popsané v kapitole „Stávající řešení pro provádění útoků“, a také antény Vert900 [35].

Při provádění reinjection útoku byl použit nejen software vytvořený v rámci bakalářské práce, ale také software Universal Radio Hacker popsaný v kapitole „Stávající řešení pro provádění útoků“, protože při vývoji aplikace v rámci bakalářské práce nebyla dosáhnuta funkčnost programu pro modulaci a demodulaci signálu.

## 7.1 Bezdrátový zvonek UBZ4

Prvním cílem útoků byl bezdrátový zvonek UBZ4 pracující na frekvenci 433,92 MHz. Bezdrátová komunikace mezi ovladačem a zvonkem není zabezpečená, takže pro útočníka není těžké provádět útoky, ale pro obyvatele místnosti, kde se takový zvonek používá, může být útok problémem.

K útoku na bezdrátový zvonek bylo nutné nastavit centrální frekvenci, vzorkovací frekvenci a citlivost. Centrální frekvence byla odvozena z charakteristik zvonku a je 433,92 MHz. Vzorkovací frekvence byla nastavena na 1 Msps.

### 7.1.1 Jamming útok

#### 7.1.1.1 Laboratorní podmínky

V laboratorních podmínkách byly zvonek, ovladač a SDR umístěny na stejném povrchu ve vzdálenosti půl metru od sebe. Mezi nimi byl otevřený prostor bez

| Center frequency | Sample rate | RF gain | Výsledek (odeslano/přijato signálu) |
|---|---|---|---|
| 433,92 MHz | 1 Msps | 20 dB | Zvonek funguje (5/5) |
| 433,92 MHz | 1 Msps | 40 dB | Zvonek funguje (5/5) |
| 433,92 MHz | 1 Msps | 60 dB | Zvonek funguje (5/5) |
| 433,92 MHz | 1 Msps | 80 dB | Zvonek funguje castecne (3/5) |
| 433,92 MHz | 1 Msps | 89 dB | Zvonek nefunguje (0/5) |

Tabulka 7.1: Jamming útok na zvonek, laboratorní podmínky

| Center frequency | Sample rate | RF gain | Výsledek (odeslano/přijato signálu) |
|---|---|---|---|
| 433,92 MHz | 1 Msps | 20 dB | Zvonek funguje (5/5) |
| 433,92 MHz | 1 Msps | 40 dB | Zvonek funguje (5/5) |
| 433,92 MHz | 1 Msps | 60 dB | Zvonek nefunguje (0/5) |
| 433,92 MHz | 1 Msps | 80 dB | Zvonek nefunguje (0/5) |
| 433,92 MHz | 1 Msps | 89 dB | Zvonek nefunguje (0/5) |

Tabulka 7.2: Jamming útok na zvonek, reálné podmínky

překážek. V každém testu byla z ovladače do zvonku odeslána sekvence 5 signálů.

Pro první test byla zvolena citlivost 20 dB. S těmito parametry nebyl útok úspěšný a zvonek fungoval bez problémů. S každým dalším útokem se citlivost zvýšila o 20 dB, první částečně úspěšný útok byl proveden s citlivostí 80 dB. Zvonek obdržel pouze 3 signály z 5 odeslaných. Poslední test byl proveden s maximální citlivostí 89 dB. Test byl úspěšný, zvonek přestal přijímat signály z ovladače a reagovat na ně.

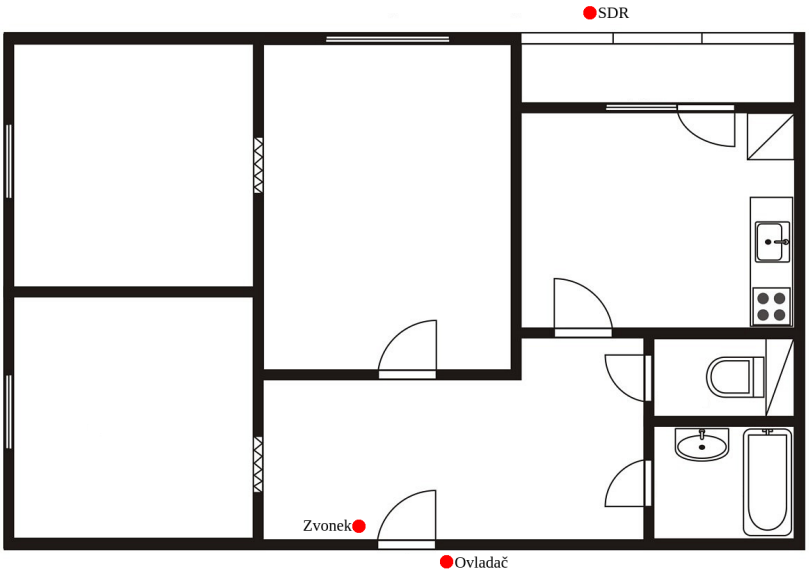
Výsledky útoku v laboratorních podmínkach jsou popsány v tabulce 7.1.

#### 7.1.1.2 Reálné podmínky

V reálných podmínkách byl ovladač umístěn za dveřmi bytu, zvonek byl umístěn nad dveřmi uvnitř bytu, SDR bylo umístěno na ulici před bytem. Mezi SDR a zvonkem byly tři zdi. Umístění je znázorněno na obrázku 7.1.

První útok byl proveden se stejnými parametry jako první útok v laboratorních podmínkách a byl neúspěšný, zvonek přijal signály. K prvnímu úspěšnému útoku došlo, když citlivost byla nastavena na 60 dB, zvonek přestal přijímat signály.

Výsledky útoku v reálných podmínkach jsou popsány v tabulce 7.2.




Obrázek 7.1: Umístění zařízení při provedení útoků na zvonek v reálných podmínkach [36]

### 7.1.2 Replay útok

#### 7.1.2.1 Laboratorní podmínky

Při provádění tohoto útoku v laboratorních podmínkach bylo umístění zařízení stejné jako při jamming útoku, popsaného v podkapitole 7.1.1.1. Přijímání a odesílání signálu bylo proveděno pomocí aplikace vytvořené v rámci bakalářské práce.

Během prvního útoku byla pro příjem a odeslání signálu zvolena citlivost 20 dB, bylo možné signál zaznamenat, ale zvonek na jeho odeslání nereagoval, útok nebyl úspěšný. Druhý útok byl úspěšný, citlivost pro příjem signálu byla 20 dB, pro odeslání signálu 40 dB, signál byl odeslán nepřetržitě, zvonek také fungoval bez zastavení.

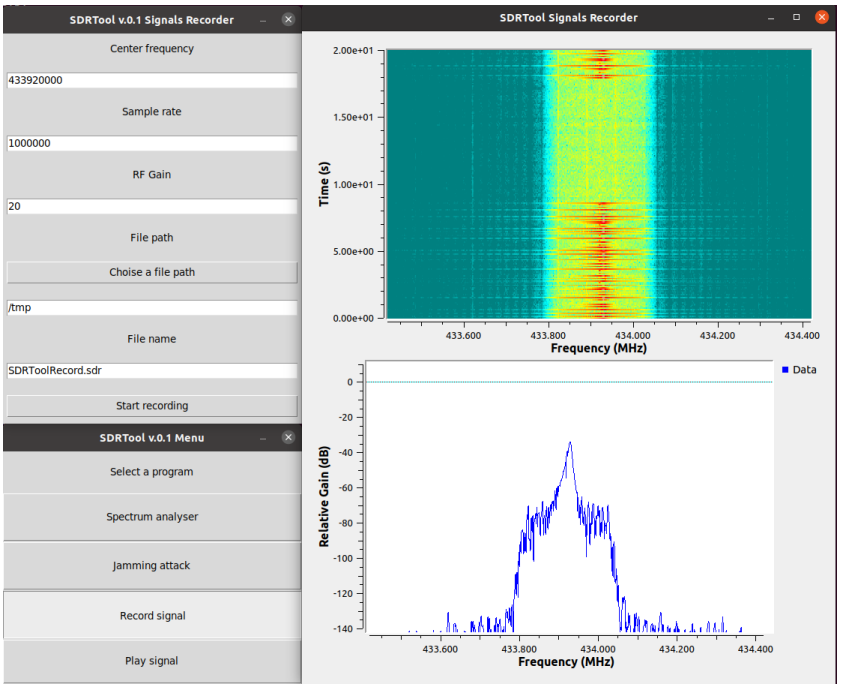
Výsledky útoku v laboratorních podmínkach jsou popsány v tabulce 7.3. Na obrázku 7.2 je zobrazen proces provádění útoku pomocí vytvořené aplikace.

| Center frequency | Sample rate | RF gain příjem/vysílani | Výsledek |
|---|---|---|---|
| 433,92 MHz | 1 Msps | 20 dB/20 dB | Podářilo se nahrat signal, ale na jeho odesíláni zvonek nereagoval |
| 433,92 MHz | 1 Msps | 20 dB/40 dB | Podářilo se nahrat signal a odeslat ho, zvonek fungoval nepretržite |

Tabulka 7.3: Replay útok na zvonek, laboratorní podmínky

| Center frequency | Sample rate | RF gain příjem/vysílani | Výsledek |
|---|---|---|---|
| 433,92 MHz | 1 Msps | 20 dB/20 dB | Podářilo se nahrat signal, ale na jeho odesíláni zvonek nereagoval |
| 433,92 MHz | 1 Msps | 20 dB/40 dB | Podářilo se nahrat signal, ale na jeho odesíláni zvonek nereagoval |
| 433,92 MHz | 1 Msps | 20 dB/60 dB | Podářilo se nahrat signal a odeslat ho, zvonek fungoval nepretržite |

Tabulka 7.4: Replay útok na zvonek, reálné podmínky




Obrázek 7.2: Replay útok na zvonek

#### 7.1.2.2 Reálné podmínky

V tomto útoku se umístění zařízení shodovalo s umístěním popsaným v podcapitole 7.1.1.2 a na obrázku 7.1.

Útoky s nastavením citlivosti pro příjem signálu na 20 dB a pro odesílání na 20 a 40 dB byly neúspěšné. Signál bylo možné zaznamenat, ale zvonek nereagoval na jeho odesilání. Úspěšný útok byl proveden s nastavením citlivosti 20 dB pro příjem a 60 dB pro vysílání.

Výsledky útoku v reálných podmínkach jsou popsány v tabulce 7.4.

## 7.2 Meteostanice TFA DIVA GO 30.3018

Dalším cílem útoků byla meteorologická stanice TFA DIVA GO 30.3018. Zobrazuje údaje o vnitřní i venkovní teplotě. Přijímá údaje o vnitřní teplotě z interního snímače, ale údaje o venkovní teplotě se odesílají z bezdrátového teploměru (simplex). Tato data se odesílají každé 4 sekundy a nepoužívají se žádné prostředky pro zabezpečení bezdrátové komunikace.

Na rozdíl od útoku na zvonek může útok na meteorologickou stanici poškodit mnohem více, protože meteorologické stanice se často používají například v zemědělství a na základě údajů z nich lze rozhodnout o nutnosti zavlažovat pole atd. Pokud je tedy meteorologická stanice napadena a zobrazuje nesprávná data, existuje riziko zhoršení nebo ztráty rostlin v důsledku nesprávné údržby pole.

Charakteristiky této meteorologické stanice naznačují, že k přenosu dat dochází na frekvenci 868 MHz, pro získání přesnějších informací o centrální frekvenci byl použit software vytvořený v rámci této práce. To umožnilo zjistit, že bezdrátový teploměr a meteorologická stanice používají frekvenci 868,3 MHz. Vzorkovací frekvence byla nastavena na 1 Msps.

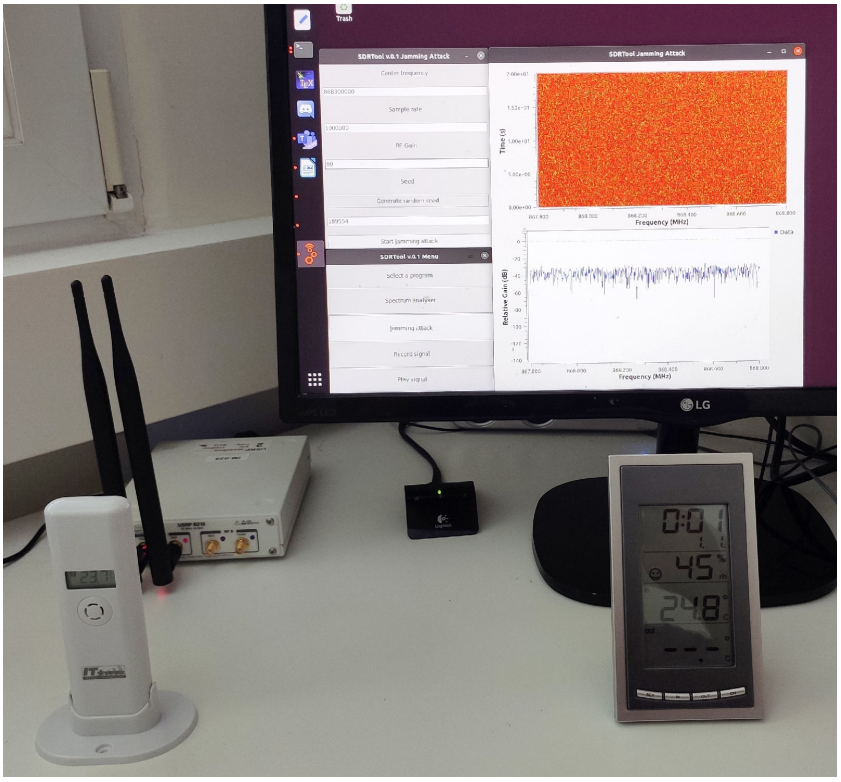
### 7.2.1 Jamming útok

#### 7.2.1.1 Laboratorní podmínky

Při útoku na meteorologickou stanici v laboratorních podmínkach byla meteorologická stanice, teplotní senzor a SDR umístěny na stejném povrchu. Obrázek 7.3 ukazuje umístění zařízení v době úspěšného útoku.

Během prvního útoku byla citlivost nastavena na 20 dB, ale útok nebyl úspěšný, meteorologická stanice přijímala data bez poruch. S každým dalším útokem se citlivost zvýšila o 20 dB, druhý a třetí útok byly částečně úspěšné, meteorologická stanice ne vždy přijímala data z teploměru a přepinala se do režimu vyhledávání druhého teploměru. Při posledním útoku byla použita citlivost 80 dB, útok byl zcela úspěšný, meteorologická stanice přestala přijímat data.

Výsledky útoku v laboratorních podmínkach jsou popsány v tabulce 7.5.



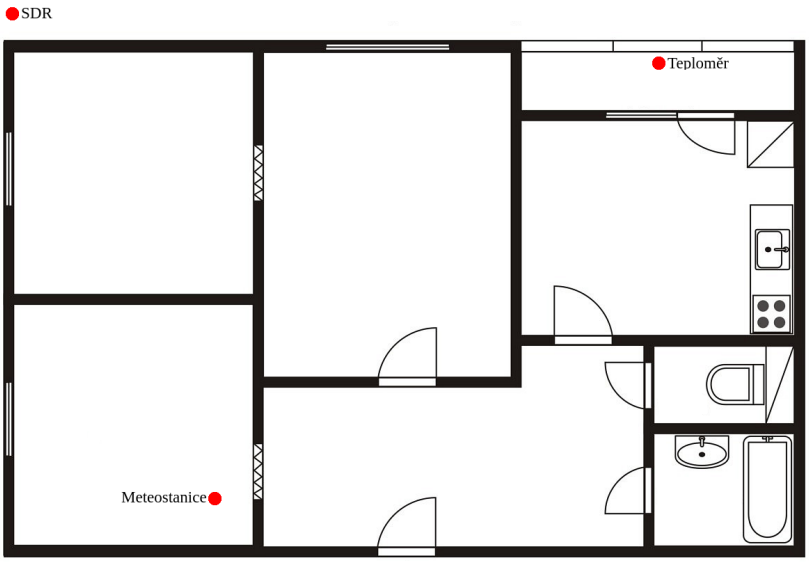

Obrázek 7.3: Jamming útok na meteostanice, laboratorní podmínky

| Center frequency | Sample rate | RF gain | Výsledek |
|---|---|---|---|
| 868,3 MHz | 1 Msps | 20 dB | Meteostanice přijímala data bez problemu |
| 868,3 MHz | 1 Msps | 40 dB | Meteostanice přijímala data, ale připojeni nebylo stabilně, proto meteostanice se přepinala mezi režímy přijmu dat od 1. nebo 2. teploměru (meteostanice podporuje příjem dat ze 3 teploměru, v útoku byl pouzit pouze jeden) |
| 868,3 MHz | 1 Msps | 60 dB | Meteostanice přijímala data, ale připojeni nebylo stabilně, proto meteostanice se přepinala mezi režímy přijmu dat od 1. nebo 2. teploměru |
| 868,3 MHz | 1 Msps | 80 dB | Meteostanice nepřijímala data vubec, komunikace byla narušena |

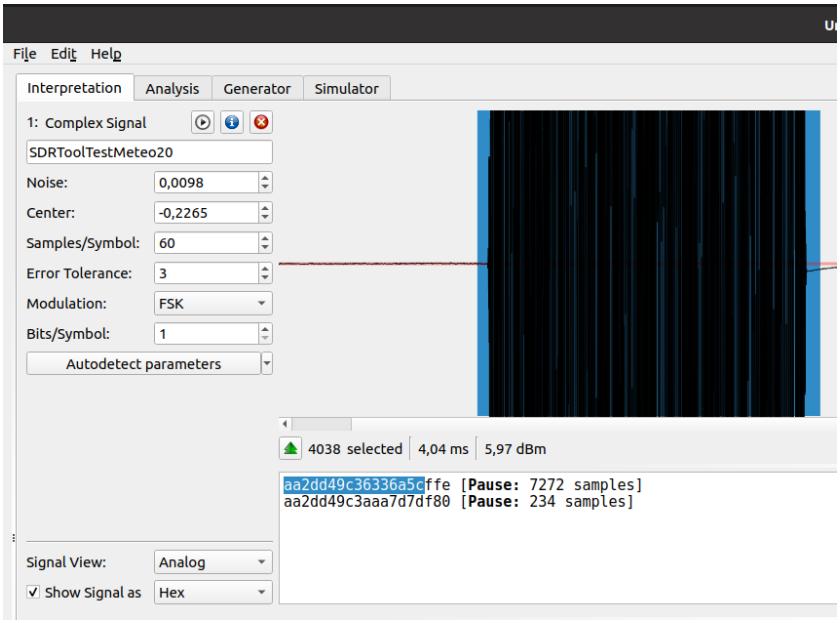
Tabulka 7.5: Jamming útok na meteostanice, laboratorní podmínky

| Center frequency | Sample rate | RF gain | Výsledek |
|---|---|---|---|
| 868,3 MHz | 1 Msps | 20 dB | Meteostanice přijímala data, ale připojeni nebylo stabilně, proto meteostanice se přepinala mezi režímy přijmu dat od 1. nebo 2. teploměru |
| 868,3 MHz | 1 Msps | 40 dB | Meteostanice přijímala data, ale připojeni nebylo stabilně, proto meteostanice se přepinala mezi režímy přijmu dat od 1. nebo 2. teploměru |
| 868,3 MHz | 1 Msps | 60 dB | Meteostanice přijímala data, ale připojeni nebylo stabilně, proto meteostanice se přepinala mezi režímy přijmu dat od 1. nebo 2. teploměru |
| 868,3 MHz | 1 Msps | 80 dB | Meteostanice nepřijímala data vubec, komunikace byla narušena |

Tabulka 7.6: Jamming útok na meteostanice, reálné podmínky




Obrázek 7.4: Umístění zařízení při provedení útoků na meteostanice v reálných podmínkach [36]




Obrázek 7.5: Příprava signálu pro replay útok na meteostanice

#### 7.2.1.2 Reálné podmínky

V reálných podmínkách byla meteorologická stanice umístěna v místnosti, bezdrátový teploměr byl instalován na lodžii, SDR byla umístěna na ulici před bytem. Obrázek 7.4 ukazuje umístění zařízení.

První útok používal nastavení citlivosti 20 dB a byl částečně úspěšný, stejně jako další dva útoky využívající citlivost 40, respektive 60 dB. Meteorologická stanice stále zobrazovala správná data z teploměru, ale připojení nebylo stabilní a meteorologická stanice se přepinala na režim vyhledávaní druhého teploměru. Čtvrtý útok s nastavením citlivosti 80 dB byl zcela úspěšný, meteorologická stanice přestala přijímat data.

Výsledky útoku v reálných podmínkach jsou popsány v tabulce 7.6.

### 7.2.2 Replay útok

#### 7.2.2.1 Laboratorní podmínky

Při provádění tohoto útoku v laboratorních podmínkach bylo umístění zařízení stejné jako při jamming útoku, popsaného v podkapitole 7.2.1.1.

Již první útok s použitím citlivosti 20 dB pro příjem a odeslání signálu byl úspěšný. Signál byl zaznamenán, ale protože meteorologická stanice přijímá data z teploměru každé 4 sekundy, pro úspěšný útok nestačilo jen začít vysílat signál zpět. K provedení útoku byl použit software URH popsaný v kapitole „Stávající řešení pro provádění útoků“. Pomocí tohoto softwaru byla ze signálu

| Center frequency | Sample rate | RF gain příjem/vysílani | Výsledek |
|---|---|---|---|
| 868,3 MHz | 1 Msps | 20 dB/– dB | Podářilo se nahrát signal ale při jeho úpravě v URH bylo zjišteno že obsáhuje pouze čast dat |
| 868,3 MHz | 1 Msps | 25 dB/20 dB | Podářilo se nahrát signal a odeslát ho, ale meteostanice ukazovala správna data |
| 868,3 MHz | 1 Msps | 25 dB/40 dB | Podářilo se nahrát signal a odeslát ho, ale meteostanice ukazovala správna data |
| 868,3 MHz | 1 Msps | 25 dB/60 dB | Podářilo se nahrát signal a odeslát ho, meteostanice ukazovala špátna data |

Tabulka 7.7: Replay útok na meteostanice, reálné podmínky

extrahována pouze nezbytná část obsahující datový paket. Proces úpravy signálu je uveden na obrázku 7.5.

Po přípravě signálu pomocí aplikace vytvořené v rámci bakalářské práce bylo zorganizováno nepřetržité odesílání signálu, protože nelze zaručit, že pokud je signál vyslán jednou, spadne do požadovaného intervalu, kdy bude meteorologická stanice přijímát data (jednou za 4 sekundy). Meteorologická stanice začala zobrazovat nesprávná data a ignorovala údaje z teploměru.

#### 7.2.2.2 Reálné podmínky

Při provádění tohoto útoku v reálných podmínkach bylo umístění zařízení stejné jako při jamming útoku, popsaného v podkapitole 7.2.1.2.

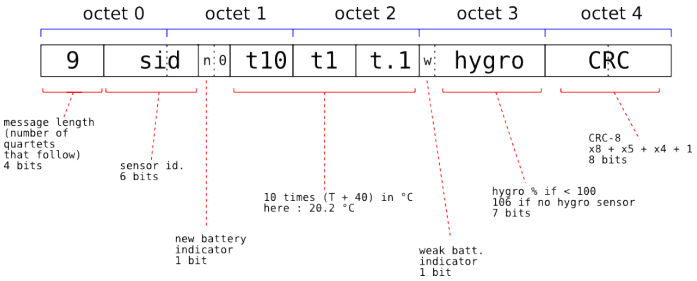
Algoritmus provádění útoku v reálných podmínkách se neliší od algoritmu popsaného v části 7.2.2.1. Prvním krokem bylo zaznamenat signál odeslaný z teploměru do meteorologické stanice. Při prvním útoku byla pro příjem signálu použita citlivost 20 dB, ale při přípravě signálu v URH bylo zjištěno, že obsahuje pouze část dat. Útok s tímto nastavením citlivosti proto nebyl úspěšný.

Při dalším útoku byla citlivost pro příjem signálu nastavena na 25 dB, signál byl přijat a obsahoval všechny potřebné informace, ale když byl odeslán s citlivostí 20 dB, meteorologická stanice stále úkazovala správná data. Stejná situace nastala při nastavování citlivosti pro odesílání signálu na 40 dB. Úspěšný útok byl proveden až po nastavení citlivosti na 60 dB.

Výsledky útoku v reálných podmínkach jsou popsány v tabulce 7.7.

| Zaznamenaný signal | Teplota |
|---|---|
| aa2dd49b3631ea6d | 23,1 °C |
| aa2dd49b3632ea40 | 23,2 °C |
| aa2dd49b3633eab4 | 23,3 °C |
| Proveden restart teploměru | – |
| aa2dd4963644eaa8 | 24,4 °C |
| Proveden restart teploměru | – |
| aa2dd496b643ead3 | 24,3 °C |

Tabulka 7.8: Zaznamenané signály pro reverzní analýzu protokolu meteostanice




Obrázek 7.6: TX29 protokol. Prevzáto z [37]

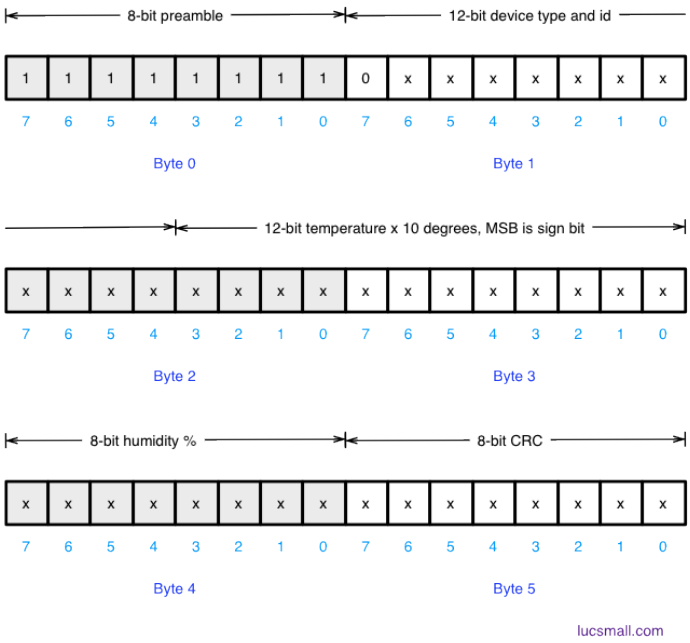
### 7.2.3 Reverzní analýza použitého protokolu

K provedení reinjection útoku, jak je popsáno v části 3.3, je nutné provést zpětnou analýzu protokolu, který meteorologická stanice používá k získávání údajů z teploměru.

Z tohoto důvodu jsem zaznamenal 5 různých signálů z teploměru, a provedl jich demodulace pomoci URH. Nejprve jsem zaznamenal 3 signály s různými teplotami, poté jsem resetoval teploměr a zaznamenal nový signál, poté jsem resetoval teploměr znovu a zaznamenal poslední signál. Restartování teploměru bylo nutné, aby bylo možné určit, které bajty jsou informacemi o ID teploměru (pokud existují). Zaznamenané signály a naměřené teploty jsou popsány v tabulce 7.8.

Poté jsem našel 3 články popisující zpětnou analýzu protokolů jiných meteorologických stanic. Obrázek 7.6 ukazuje obsah protokolu TX29, tento protokol je popsán v záznamu [37]. Obrázek 7.7 ukazuje obsah protokolu WH2, tento protokol je popsán v záznamu [38]. Obrázek 7.8 ukazuje obsah protokolu TFA Spring Weather Station, tento protokol je popsán v záznamu [39].

Po každém restartu zůstala následující část beze změny: aa2dd49. Navrhl jsem, že by to mohla být preambule. Další 2 bajty byly změněny po každém restartu teploměru, toto je ID teploměru. Další 3 bajty jsou teplota kódovaná pomocí metody popsané v článku [37], příklad: 631/10 - 40 = 23,1 °C.




Obrázek 7.7: WH2 protokol. Prevzáto z [38]

**TFA Spring weather station**
**433 MHz Temperature/Humidity Sensor 30.3206.02**
**Data Map**

12 Equals packets example:

...
01011101010000101111110000011110001010101010####
01011101010000101111110000011110001010101010####
01011101010000101011111100000111100010101010####
...
#### - Sync impulses

| color | start bit | length | description | value |
|---|---|---|---|---|
| 0101 1101 | 0 | 8 | sensor id, changes after sensor reset | |
| 0 | 8 | 1 | battery weak<br>0 – battery good, 1 – battery weak | 0 |
| 0010 1111 1100 | 12 | 12 | Temperature<br>ABC->decimal / 10 - 50 = °C | 0b001011111100 →<br>0x2fc →<br>764 →<br>76.4 →<br>26.4 °C |
| 0001 1110 | 24 | 8 | Relative Humidity<br>AB->decimal = % | 0b00011110 →<br>0x1e->30% |

Result: Temperature 26.4 °C, Humidity: 30%, Battery good.

Obrázek 7.8: TFA protokol. Prevzáto z [39]

| Data | Význam |
|---|---|
| aa | Preambule |
| 2dd4 | Synchronizační slovo |
| 9 | ? |
| b3 | ID senzoru |
| 631 | Teplota vypočtená podle vzorce (T + 40)*10 |
| ea | Informace, že senzor nepodporuje měření vlhkosti |
| 6d | CRC, vypočtený z 7 až 14 bajtu, použít polynom $x^8 + x^5 + x^4 + 1$ |

Tabulka 7.9: Protokol používaný meteorologickou stanicí TFA DIVA GO 30.3018

Jak je uvedeno v článku [37], pokud senzor nepodporuje měření vlhkosti, odešle namísto údajů o vlhkosti 0xEA. Senzor použitý v práci podporuje pouze měření teploty, takže další 2 bajty jsou informace, že měření vlhkosti není podporováno. Poslední 2 bajty jsou CRC, nevíme, jaká data z datového paketu se používa k jeho výpočtu a jaké parametry se použijí. Pozdějí v článku [40] jsem našel informace, které mi umožnily dokončit zpětnou analýzu protokolu. Konečná podoba protokolu je popsána v tabulce 7.9.

### 7.2.4 Reinjection útok

Po provedení zpětné analýzy protokolu mohu vytvořit svůj vlastní datový paket k provedení útoku.

Podle mých údajů bude teplota 12,1 °C, (12,1 + 40) * 10 = 521. Datový paket bez CRC bude mít následující formát: aa2dd49b3521ea. S pomocí [41] mohu vypočítat CRC, je to C9. Zbývá pouze určit parametry modulace signálu pomocí URH, modulovat signál a začít jej odesílat. Parametry modulace signálu jsou zobrazeny na obrázku 7.9, použíta modulace FSK.

#### 7.2.4.1 Laboratorní podmínky

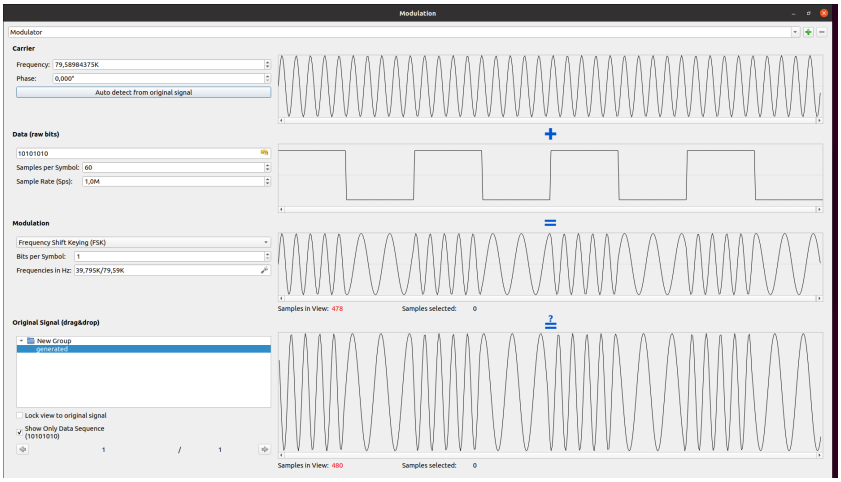
Při provádění tohoto útoku v laboratorních podmínkach bylo umístění zařízení stejné jako při jamming útoku, popsaného v podkapitole 7.2.1.1.

Při odesílání modulovaného signálu s citlivostí 20 dB a 40 dB nebyl útok úspěšný, meteorologická stanice přiímala správná data. Když byla citlivost zvýšena na 60 dB, útok byl úspěšný.

Výsledky útoku v láboratorních podmínkach jsou popsány v tabulce 7.10.

#### 7.2.4.2 Reálné podmínky

Při provádění tohoto útoku v reálných podmínkach bylo umístění zařízení stejné jako při jamming útoku, popsaného v podkapitole 7.2.1.2.




Obrázek 7.9: Modulace signálu v URH

| Center frequency | Sample rate | RF gain | Vysledek |
|---|---|---|---|
| 868,3 MHz | 1 Msps | 20 dB | Meteostanice ukazuje správna data |
| 868,3 MHz | 1 Msps | 40 dB | Meteostanice ukazuje správna data |
| 868,3 MHz | 1 Msps | 60 dB | Meteostanice ukazuje špátna data |

Tabulka 7.10: Reinjection útok na meteostanice, laboratorní podmínky

| Center frequency | Sample rate | RF gain | Vysledek |
|---|---|---|---|
| 868,3 MHz | 1 Msps | 20 dB | Meteostanice ukazuje správna data |
| 868,3 MHz | 1 Msps | 40 dB | Meteostanice ukazuje správna data, ale přípojeni není stabilně, meteostanice se stára dostat data ještě z jiného teploměru |
| 868,3 MHz | 1 Msps | 60 dB | Meteostanice ukazuje špátna data |

Tabulka 7.11: Reinjection útok na meteostanice, reální podmínky

Při odesílání modulovaného signálu s citlivostí 20 dB nebyl útok úspěšný, meteorologická stanice přiímala správná data. S citlivostí 40 dB byl útok částečně úspěšný, meteorologická stanice přiímala správná data, ale přípojení nebylo stabilní. Když byla citlivost zvýšena na 60 dB, útok byl úspěšný.

Na obrázku 7.10 je zobrazen úspěšný útok. Výsledky útoku v reálných podmínkach jsou popsány v tabulce 7.11.


Obrázek 7.10: Demonstrace reinjection útoku v realných podmínkách

## 7.3 Výsledek

Jak je ukázáno v kapitole, útoky prováděné na zařízení používající bezdrátovou komunikaci bez dostatečné úrovně ochrany jsou snadno proveditelné (kromě reinjection útoku) a vzhledem ke zvyšující se cenové dostupnosti SDR je nutné se vypořádat s problémem zabezpečení bezdrátových komunikace na všech zařízeních, i když jsou navržena s cílem minimalizovat spotřebu energie.

# Závěr

Cílem práce bylo prostudovat některé ze stávajících typů útoků na zařízení využívajících bezdrátovou komunikaci a také vytvořit aplikaci, která zajistí rychlé provedení těchto útoků pomocí USRP B210.

Práce popisuje základní prvky SDR, typy modulace signálu, stávající řešení pro provádění útoků a typy útoků na zařízení využívající bezdrátovou komunikaci. Výsledkem práce byla také realizace různých typů útoků, která ukazuje bezpečnostní problémy zařízení využívajících bezdrátovou komunikaci.

V rámci práce byl navržen, implementován a otestován software pro různé typy útoků. Vytvořený software nemá plnou funkčnost analogů, jako je Universal Radio Hacker, a byl vytvořen pro jednoduché použití a umožňuje provádět jamming a replay útoky, stejně jako reinjection útoky, ale v tom případě je nutné použití aplikace třetí strany.

V budoucnu může být software díky použití GNU Radio rozšířen o moduly pro demodulaci, modulaci a dekódování signálu, které umožní provedení reinjection útoků bez použití programů třetích stran.

Příloha A

# Uživatelský manuál

## A.1 Minimální systémové požadavky

Aby aplikace fungovala správně, musíte mít GNU Radio Companion verze 3.10 nebo vyšší a Python verze 3.8.5 nebo vyšší.

Verzi GNU Radio Companion můžete zkontrolovat pomocí příkazu

gnuradio-config-info –version

Verzi Python můžete zkontrolovat pomocí příkazu

python3 –version

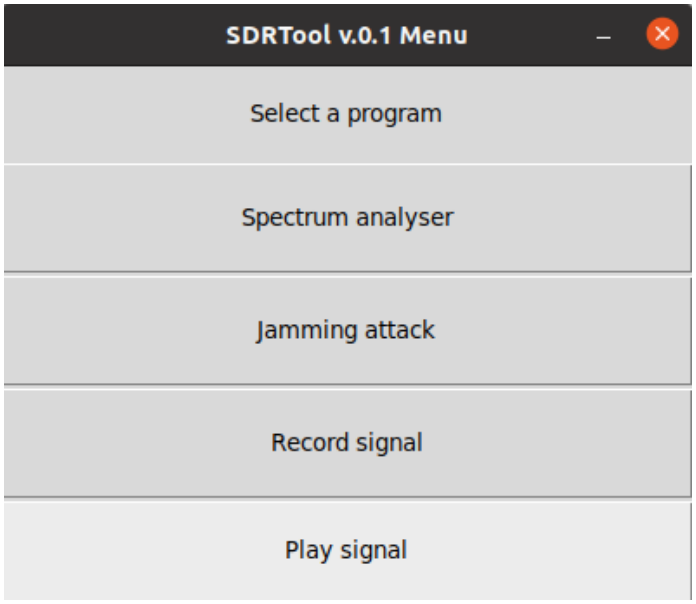
## A.2 Spuštění aplikace

Chcete-li spustit aplikaci, musíte spustit soubor SDRToolMenu.py, který je umístěn ve složce SDRTool, můžete to provést pomocí příkazu

python3 SDRToolMenu.py

Otevře se menu (zobrazeno na obrázku A.1), ve které můžete vybrat požadovaný software. V současné době má software následující funkce:

1. Analyzátor spektra
2. Provedení jamming útoku
3. Záznam signálu
4. Přehrání signál




Obrázek A.1: SDRTool menu

## A.3 Vstupní parametry

Aby aplikace fungovala správně, je třeba dodržovat následující omezení:

1. Centrální frekvence (USRP B210 podporuje 70 MHz - 6GHz)
2. Citlivost (USRP B210 podporuje 0 dB - 89 dB)

V případě nesprávního vstúpu aplikace vypíše varování a nastaví standardní hodnoty, kde je to možné.

## A.4 Analyzátor spektra

Chcete-li spustit analyzátor spektra, vyberte v menu položku „Spectrum analyzer“. V okně, které se otevře, zadejte následující parametry:

1. Centrální frekvence
2. Vzorkovací frekvence
3. Citlivost

A klikněte na tlačítko „Start visualisation“. V novém okně budou vytvořeny dva grafy zobrazující aktuální stav vysílání na vybrané frekvenci. Chcete-li zastavit proces visualizace, stačí uzavřít okno s grafy.

## A.5 Provedení jamming útoku

Chcete-li spustit jamming útok, vyberte v menu položku „Jamming attack“. V okně, které se otevře, zadejte následující parametry:

1. Centrální frekvence
2. Vzorkovací frekvence
3. Citlivost
4. Číslo pro inicializaci generátoru pseudonáhodných čísel

Číslo pro inicializaci generátoru pseudonáhodných čísel můžete zadat ručně nebo vygenerovat pomocí tlačítka „Generate random seed“. Pokud toto pole zůstane prázdné, program vypíše varování a nastaví standardní hodnotu.

Stisknutím tlačítka „Start jamming attack“ zahájíte útok. Chcete-li útok zastavit, uzavřete okno s grafy.

## A.6 Nahrávání signálu

Pokud chcete nahrát signál pro jeho další použití při replay útoku nebo demodulaci, vyberte v nabídce položku „Record signal“. V okně, které se otevře, zadejte následující parametry:

1. Centrální frekvence
2. Vzorkovací frekvence
3. Citlivost
4. Cesta k uložení souboru
5. Název souboru

Pokud cesta k uložení souboru není k dispozici nebo není možné soubor s tímto názvem uložit, program vydá varování, výsledný soubor se uloží do složky /tmp a bude mít název SDRToolRecord.sdr

Stisknutím tlačítka „Start recording“ zahájite nahrávání signálu. Chcete-li nahrávání zastavit, uzavřete okno s grafy.

## A.7 Přehrání signálu

Pokud chcete přehrát signál, vyberte v nabídce položku „Play signal“. V okně, které se otevře, zadejte následující parametry:

1. Centrální frekvence

2. Vzorkovací frekvence
3. Citlivost
4. Je li nutné neustále vysílat signál
5. Název souboru a cesta k souboru

Pokud soubor neexistuje nebo je poškozen, program napíše varování. Stisknutím tlačítka „Play signal“ zahájite přehrání signálu. Chcete-li přehrání zastavit, uzavřete okno s grafy.

Příloha B

# Seznam použitých zkratek

**AM** Amplitude modulation

**ASK** Amplitude-shift keying

**FM** Frequency modulation

**FSK** Frequency-shift keying

**GSM** The Global System for Mobile Communications

**GUI** Graphical user interface

**MIMO** Multiple-input multiple-output

**PSK** Phase-shift keying

**SDR** Software-defined radio

**URH** Universal Radio Hacker

**USRP** Universal Software Radio Peripheral

Příloha C

# Obsah přiloženého CD

- `readme.txt` ..... stručný popis obsahu USB
- `SDRTool` ..... adresář se spustitelnou formou implementace
- `src`
  - `impl` ..... zdrojové kódy implementace
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `BP_Kravtsov_Aleksei_2021.pdf` ..... text práce ve formátu PDF

# Literatura


[1] A5/1 Stream Cipher. *Asecuritysite.com* [online]. 2021-05-11 [cit. 2021-5-11]. Dostupné z: https://asecuritysite.com/encryption/a5

[2] What is a Rolling Code? *InfoBloom* [online]. [cit. 2021-5-11]. Dostupné z: https://www.infobloom.com/what-is-a-rolling-code.htm

[3] Software-defined radio. *Wikipedia* [online]. 2021-05-10 [cit. 2021-5-11]. Dostupné z: https://en.wikipedia.org/wiki/Software-defined_radio

[4] What is Software Defined Radio (SDR). *Digitrode.ru* [online]. 2018-01-02 [cit. 2021-5-12]. Dostupné z: http://digitrode.ru/articles/1224-chto-takoe-programmno-opredelyaemaya-radiosistema-sdr.html

[5] Data flow (simplex, half-duplex, and full-duplex). *Pinterest* [online]. 2021-05-12 [cit. 2021-5-12]. Dostupné z: https://www.pinterest.com/pin/301600506298489756/

[6] Anténa. *Wikipedia* [online]. 2021-04-28 [cit. 2021-5-12]. Dostupné z: https://cs.wikipedia.org/wiki/Anténa

[7] Šířka pásma. *Wikipedia* [online]. 2021-04-28 [cit. 2021-5-12]. Dostupné z: https://cs.wikipedia.org/wiki/Šířka_pásma

[8] Duplex, Simplex. *eArchiv: Archiv článků a přednášek Jiřího Peterky* [online]. 2021-05-12 [cit. 2021-5-12]. Dostupné z: https://www.earchiv.cz/a92/a245c120.php3

[9] PUNČOCHÁŘ, Josef. *Analýza elektronických obvodů (AEO)*. Ostrava, 2011.

[10] Low-pass filter. *Wikipedia* [online]. 2021-05-10 [cit. 2021-5-12]. Dostupné z: https://en.wikipedia.org/wiki/Low-pass_filter

[11] ODINETS, Aleksandr a Aleksandr NAUMENKO. *Digital devices: ADC and DAC*. Omsk, 2006.

[12] Typy modulace signálu. *Pue8.ru* [online]. 2020-11-12 [cit. 2021-5-12]. Dostupné z: https://pue8.ru/silovaya-elektronika/494-vidy-modulyatsii-signalov.html

[13] Radio Frequency Modulation Made Easy. *Technicacuriosa.com* [online]. 2021-05-12 [cit. 2021-5-12]. Dostupné z: https://popularelectronics.technicacuriosa.com/2017/03/08/radio-frequency-modulation-made-easy/

[14] Amplitudová modulace. *Wikipedia* [online]. 2021-04-28 [cit. 2021-5-12]. Dostupné z: https://cs.wikipedia.org/wiki/Amplitudová_modulace

[15] Modulace. *Solidstate.karelia.ru* [online]. 2012-12-14 [cit. 2021-5-12]. Dostupné z: http://solidstate.karelia.ru/p/tutorial/informatics/chapter4/9/3.htm

[16] Frekvenční modulace. *Wikipedia* [online]. 2021-04-28 [cit. 2021-5-12]. Dostupné z: https://cs.wikipedia.org/wiki/Frekvenční modulace

[17] Fázová modulace. *Wikipedia* [online]. 2021-04-28 [cit. 2021-5-12]. Dostupné z: https://cs.wikipedia.org/wiki/Fázová_modulace

[18] Digitální modulace. *Studme.org* [online]. 2021-05-12 [cit. 2021-5-12]. Dostupné z: https://studme.org/171324/tehnika/tsifrovaya_modulyatsiya

[19] Klíčování amplitudovým posuvem. *Wikipedia* [online]. 2021-04-28 [cit. 2021-5-12]. Dostupné z: https://cs.wikipedia.org/wiki/Klíčování_amplitudovým_posuvem

[20] Klíčování frekvenčním posuvem. *Wikipedia* [online]. 2021-04-28 [cit. 2021-5-12]. Dostupné z: https://cs.wikipedia.org/wiki/Klíčování_frekvenčním_posuvem

[21] Digital modulation basics, part 1. *5G Technology and Engineering - 5G Technology World* [online]. 2021-05-12 [cit. 2021-5-12]. Dostupné z: https://www.5gtechnologyworld.com/digital-modulation-basics-part-1/

[22] Klíčování fázovým posuvem. *Wikipedia* [online]. 2021-04-28 [cit. 2021-5-12]. Dostupné z: https://cs.wikipedia.org/wiki/Klíčování_fázovým_posuvem

[23] GUOBIN, Liu. *Jamming Attacks and Countermeasures in Wireless Area Networks*. Hong Kong Polytechnic University (People's Republic of China). 2012. ISBN 9781267623218.

[24] VADLAMANI, Satish, Burak EKSIOGLU, Hugh MEDAL a Apurba NANDI. Jamming attacks on wireless networks: A taxonomic survey. *International Journal of Production Economics*. **2016**(172), 76-94. ISSN 0925-5273. Dostupné z: doi:https://doi.org/10.1016/j.ijpe.2015.11.008

[25] Bezdrátové rádiové datové sítě. In: *Elektrorevue.cz* [online]. 2009-04-07 [cit. 2021-04-17]. Dostupné z: http://www.elektrorevue.cz/clanky/02009/index.html

[26] Understanding SDR-Based Attacks on IoT. *Datafloq* [online]. 2017-10-01 [cit. 2021-5-11]. Dostupné z: https://datafloq.com/read/understanding-sdr-based-attacks-on-iot/3735

[27] What Is a Replay Attack? *Kaspersky Cybersecurity Solutions for Home and Business* [online]. 2021-04-16 [cit. 2021-04-16]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/replay-attack

[28] SDR and its role in cybersecurity. *INCIBE-CERT* [online]. 2021-02-18 [cit. 2021-5-11]. Dostupné z: https://www.incibe-cert.es/en/blog/sdr-and-its-role-cybersecurity

[29] CRC (kontrolní součet). *Root.cz* [online]. 2003-01-30 [cit. 2021-5-11]. Dostupné z: https://www.root.cz/clanky/crc-kontrolni-soucet/

[30] GNU Radio. *Wikipedia* [online]. 2021-04-27 [cit. 2021-5-11]. Dostupné z: https://cs.wikipedia.org/wiki/GNU_Radio

[31] Universal Radio Hacker. *GitHub* [online]. 2021-04-22 [cit. 2021-5-11]. Dostupné z: https://github.com/jopohl/urh

[32] USRP B210 (Board Only). *Ettus Research* [online]. 2021-05-11 [cit. 2021-5-11]. Dostupné z: https://www.ettus.com/all-products/ub210-kit/

[33] Bezdrátový zvonek UBZ4-1. *ELEKTROBOCK CZ* [online]. 2021-04-16 [cit. 2021-04-16]. Dostupné z: https://www.elektrobock.cz/bezdratovy-zvonek/p12

[34] Wireless thermometer DIVA GO 30.3018. *TFA Dostmann* [online]. 2021-04-16 [cit. 2021-04-16]. Dostupné z: https://www.tfa-dostmann.de/en/product/wireless-thermometer-diva-go-30-3018/

[35] VERT900 Antenna. *Ettus Research* [online]. 2021-05-11 [cit. 2021-5-11]. Dostupné z: https://www.ettus.com/all-products/vert900/

[36] Byt 3+1+L. *Reality.idnes.cz* [online]. [cit. 2021-5-11]. Dostupné z: https://reality.idnes.cz/detail/prodej/byt/pardubice-erno-kostala/607bd97e24d6976a351424f2/

[37] TX29 Protocol. *Fred's web site* [online]. 2011-07-11 [cit. 2021-5-11]. Dostupné z: http://fredboboss.free.fr/articles/tx29.php

[38] Hacking the WH2 Wireless Weather Station Outdoor Sensor — Part 2: Protocol Specification. *Lucsmall.com* [online]. 2018-03-17 [cit. 2021-5-11]. Dostupné z: https://lucsmall.com/2012/04/29/weather-station-hacking-part-2/

[39] TFA Spring Weather Station Sensor Protocol Reverse Engineering. *Sudonull.com* [online]. 2016-12-22 [cit. 2021-5-11]. Dostupné z: https://sudonull.com/post/91524-TFA-Spring-Weather-Station-Sensor-Protocol-Reverse-Engineering

[40] Tfrec - A SDR tool for receiving wireless sensor data. *GitHub* [online]. 2019-03-15 [cit. 2021-5-11]. Dostupné z: https://github.com/baycom/tfrec/tree/547f037dbf1aaf6064acc670b061028036ba33b4

[41] CRC Calculator (Javascript). *Sunshine's Homepage* [online]. 2019-01-12 [cit. 2021-5-11]. Dostupné z: http://www.sunshine2k.de/coding/javascript/crc/crc_js.html