FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání diplomové práce

Název:	Přenosné zařízení pro odposlech NFC komunikace pomocí SDR založené na platformě Raspberry Pi
Student:	Bc. Martin Balko
Vedoucí:	Ing. Pavel Kubalík, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Počítačová bezpečnost
Katedra:	Katedra informační bezpečnosti
Platnost zadání:	do konce letního semestru 2023/2024

Pokyny pro vypracování

Prozkoumejte existující nástroje určené k analýze NFC komunikace.
Analyzujte technologií SDR (softwarově definovaného rádia).
Analyzujte technologii NFC, zejména princip komunikace mezi NFC čtečkou a NFC kartou (MIFARE Classic, MIFARE DESFire, MIFARE Plus).
Analyzujte a navrhněte způsob pro odposlech NFC komunikace pomoci SDR.
Navrhněte přenosné zařízení, které bude umožňovat odposlech, záznam a prvotní analýzu NFC komunikace.
Zařízení bude schopné odchytit UID karty a komunikaci směrem od čtečky. Pokud bude signál dostatečně silný, zaznamená i komunikaci směrem od karty.
Navržené řešení zrealizujte na platformě Raspberry Pi.
Pro výsledné zařízení napište v jazyce Python obslužnou aplikaci.
Výsledné zařízení řádně otestujte.

Elektronicky schválil/a prof. Ing. Róbert Lórencz, CSc. dne 6. února 2023 v Praze.

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Diplomová práca

Přenosné zařízení pro odposlech NFC komunikace pomocí SDR založené na platformě Raspberry Pi

Bc. Martin Balko

Katedra počítačových systémů
Vedúci práce: Ing. Pavel Kubalík, Ph.D.

2. mája 2023

Poďakovanie

Ďakujem môjmu vedúcemu práce za praktické rady, prínosné konzultácie a celkovú pomoc v priebehu tvorby práce. Taktiež veľká vďaka patrí Tomášovi Přeučilovi, rodine a priateľom za ich podporu.

Prehlásenie

Prehlasujem, že som predloženú prácu vypracoval(a) samostatne a že som uviedol(uviedla) všetky informačné zdroje v súlade s Metodickým pokynom o etickej príprave vysokoškolských záverečných prác.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Sb, autorského zákona, v znení neskorších predpisov. V súlade s ustanovením § 46 odst. 6 tohoto zákona týmto udeľujem bezvýhradné oprávnenie (licenciu) k používaniu tejto mojej práce, a to vrátane všetkých počítačových programov ktoré sú jej súčasťou alebo prílohou a tiež všetkej ich dokumentácie (ďalej len „Dielo“), a to všetkým osobám, ktoré si prajú Dielo používať. Tieto osoby sú oprávnené Dielo používať akýmkoľvek spôsobom, ktorý neznižuje hodnotu Diela, ale len pre nezárobkové účely. Toto oprávnenie je časovo, územne a množstevne neobmedzené.

V Prahe 2. mája 2023 . . . . . .

Odkaz na túto prácu

Balko, Martin. *Přenosné zařízení pro odposlech NFC komunikace pomocí SDR založené na platformě Raspberry Pi*. Diplomová práca. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2023.

Abstrakt

Práca sa zameriava na návrh prenosného zariadenia pre odpočúvanie NFC pomocou SDR. Súčasťou práce je analýza existujúcich riešení, analýza technológie NFC a jej možných zraniteľností. Pri návrhu riešenia je kladený dôraz na jeho použitie s platformou Raspberry Pi. Navrhnuté riešenie je implementované spolu s užívateľskou aplikáciou v podobe webovej aplikácie, ku ktorej užívateľ pristupuje pomocou Wi-Fi. Riešenie je implementované pomocou programovacieho jazyka Python. Súčasťou práce je aj testovanie implementovaného riešenia.

Klíčová slova SDR, NFC, odpočúvanie komunikácie, prenosné zariadenie, RTL-SDR, Raspberry Pi, Python

Abstract

This master thesis focuses on the design of a portable device for NFC eavesdropping using SDR. The work includes analysis of existing solutions, analysis of NFC technology and its possible vulnerabilities. In the design of the solution, emphasis is placed on its use with a Raspberry Pi computer. The proposed solution is implemented along with a user application in the form of a web application, which is accessed by using Wi-Fi. The solution is implemented using Python programming language. Testing of the implemented solution is also part of the work.

Keywords SDR, NFC, communication eavesdropping, portable device, RTL-SDR, Raspberry Pi, Python

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Bezdrôtová komunikácia sa v uplynulých rokoch stáva základným spôsobom komunikácie mnohých zariadení využívaných v každodennom prostredí. Medzi technológie bezdrôtovej komunikácie sa radí aj technológia NFC, ktorá sa sama o sebe dostala medzi tie najvyužívanejšie. Prakticky každý mobilný telefón vyrobený v posledných rokoch dokáže s touto technológiou pracovať. Okrem mobilných telefónov sa využíva technológia NFC aj v takzvaných NFC kartách, ktoré sa využívajú pre bezhotovostné a bezkontaktné platby v obchodoch. NFC čipy sú vkladané do osobných dokladov pre jednoduchšiu a rýchlejšiu prácu a vyhľadávanie na úradoch a vo verejných systémoch, NFC tagy sú využívané ako náhrady kľúčových systémov v zamestnaniach.

V rovnakej miere sa v technologickej sfére rozširuje aj technológia softvérovo definovaného rádia. Zariadenie veľkosti prenosného USB kľúča, v spolupráci s nepreberným množstvom bezplatného softvéru, umožňuje využívať všetky vlastnosti a schopnosti klasického rádiového prijímača. Okrem toho umožňuje signál z rôznych frekvencií jednoducho zaznamenávať pre ďalšie spracovávanie a analýzu.

Napriek tomu, že je technológia NFC určená pre komunikáciu zariadení na veľmi krátku vzdialenosť, existuje tu možnosť odpočúvania takejto komunikácie. V tejto práci sa zaoberám analýzou, návrhom, implementáciou a testovaním prenosného zariadenia, ktoré by takéto odpočúvanie umožňovalo. Zároveň sa v práci snažím zodpovedať otázku, aké všetky informácie je možné pomocou softvérovo definovaného rádia z takejto komunikácie získať.

V prvej časti práce analyzujem existujúce riešenia pre analýzu technológie NFC. Následnou analýzou NFC a softvérovo definovaného rádia skúmam možné spôsoby odpočúvania komunikácie. V ďalšej časti prebieha návrh prenosného zariadenia, ktorého implementácia pre platformu Raspberry Pi je zdokumentovaná v tretej časti práce. Posledná časť tejto práce sa zaoberá testovaním zrealizovaného riešenia.

Kapitola 1

Cieľ práce

Cieľom diplomovej práce je preskúmať a vytvoriť prenosné zariadenie, ktoré bude užívateľovi umožňovať odpočúvanie, zaznamenávanie a prvotnú analýzu bezdrôtovej NFC komunikácie s využitím technológie softvérovo definovaného rádia.

Cieľom rešeršnej časti práce je preskúmať a analyzovať existujúce riešenia pre analýzu NFC komunikácie bez ohľadu na použitie softvérovo definovaného rádia či iných technológií. Ďalším cieľom je analýza technológie softvérovo definovaného rádia a jej možné využitie pre odpočúvanie a zaznamenávanie NFC komunikácie. V tejto časti je taktiež cieľom analyzovať bezdrôtovú technológiu typu NFC s dôrazom na komunikáciu medzi NFC čítačkou a NFC čipovými kartami. Medzi primárne typy čipových kariet patria karty MIFARE Classic, MIFARE DESFire a MIFARE Plus. Po preskúmaní oboch technológií sa uskutoční analýza možných spôsobov, akým dosiahnuť odpočúvanie NFC komunikácie pomocou softvérovo definovaného rádia. V tejto časti taktiež prebehne analýza možného spracovania signálu pomocou programovacieho jazyka Python.

Cieľom praktickej časti je návrh prenosného zariadenia pre odpočúvanie NFC komunikácie pomocou softvérovo definovaného rádia, výber vhodnej implementačnej metódy a spôsobu prvotnej analýzy zachytenej komunikácie. Dôležitou súčasťou tejto časti je okrem vyššie uvedeného aj návrh obslužnej aplikácie, ktorá bude užívateľovi umožňovať prácu s navrhnutým prenosným zariadením.

Obslužná aplikácia bude užívateľovi umožňovať zachytávanie a analýzu komunikácie využívajúcej technológiu NFC, zobrazovanie už uskutočnených analýz a ich sťahovanie. Finálny návrh spoločne s obslužnou aplikáciou bude naprogramovaný v programovacom jazyku Python s dôrazom na kompatibilitu s platformou Raspberry Pi.

Kapitola 2

Analýza

V rámci tejto časti mojej práce postupne preskúmam existujúce riešenia pre analýzu NFC komunikácie. Následne analyzujem samotnú technológiu NFC, pričom sa zameriavam na komunikáciu medzi NFC čítačkou a NFC kartou. Analýza je zameraná hlavne na komunikáciu s NFC čipovými kartami typu MIFARE Classic, MIFARE DESFire a MIFARE Plus. Neskôr skúmam tému technológie a princípov softvérovo definovaného rádia, na ktorú nadväzujem analýzou spôsobov využitia softvérovo definovaného rádia na zachytenie a odpočúvanie NFC komunikácie. Časť analýzy ukončujem diskusiou o možných postupoch, ako takto zachytenú komunikáciu spracovať a získať z nej informácie.

2.1 Existujúce riešenia

V tejto sekcii predstavím existujúce riešenia pre analýzu komunikácie, ktorá využíva technológiu NFC. Vo väčšine z existujúcich riešení popisovaných v ďalších častiach sa jedná o sériovo vyrábané hardvérové súčiastky, ktoré pracujú s otvoreným zdrojovým kódom. Špecificky sa jedná o riešeni *Proxmark 3*, *HydraNFC* a *ChameleonMini*. Analýzu existujúcich riešení zakončím diskusiou o nástroji *ComProbe NFC Protocol Analyzer*.

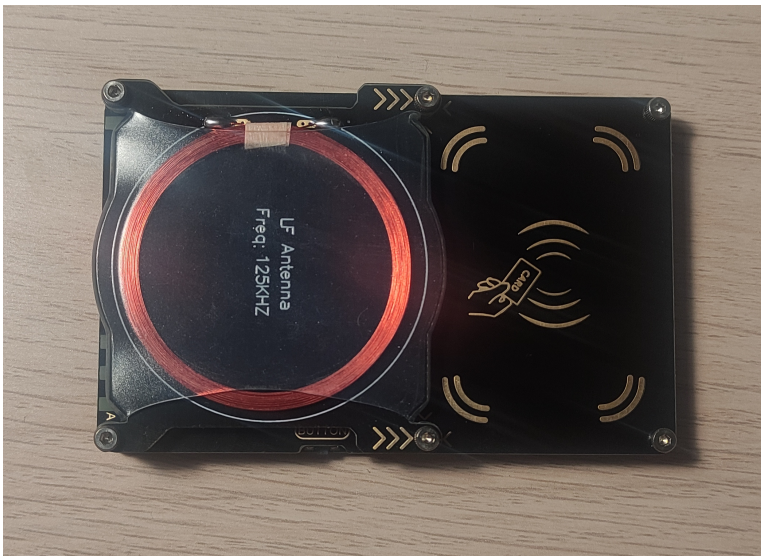
2.1.1 Proxmark 3

Platforma *Proxmark 3* je pravdepodobne najznámejšou radou nástrojov pre analýzu RFID komunikácie. V čase písania tejto práce existuje 5 nástrojov, ktoré umožňujú užívateľovi zachytávať, analyzovať, klonovať, emulovať a všeobecne pracovať s RFID systémami. Užívateľ používa nástroj pomocou terminálovej aplikácie na zariadení (počítač, notebook, atď.), do ktorého je nástroj pripojený cez USB rozhranie. [1]

Firmvéry pre všetky nástroje tejto platformy sú vyvíjané s otvoreným zdrojovým kódom. Do jeho písania sa aktívne zapájajú členovia komunity, pričom

zdrojový kód je dostupný vo verejnom Github repozitári. Ku dňu písania tejto práce existuje niekoľko aktívne vyvíjaných verzií firmvérov. [2]

V rámci písania tejto práce taktiež využívam jeden z nástrojov tejto platformy - *Proxmark 3 Easy*. Vďaka jeho funkcionalitám som schopný v ďalších častiach overiť správnosť svojho návrhu ako aj finálnej realizácie.



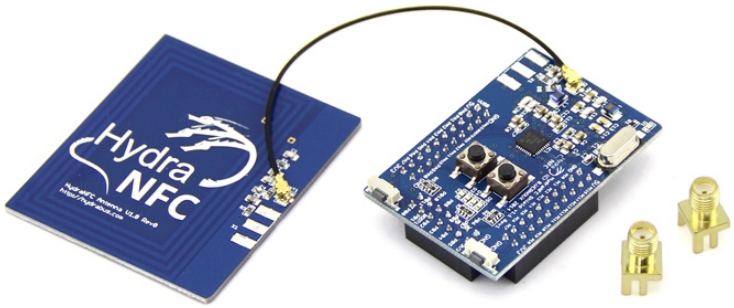
Obr. 2.1: *Proxmark 3 Easy*. Foto autor

2.1.2 HydraNFC

Druhým existujúcim riešením je nástroj *HydraNFC*. V tomto prípade sa nejedná o platformu, ale špecializovanú hardvérovú sučiastku. Je primárne určená pre mikrokontroler *HydraBus*, avšak vývojári uvádzajú, že je súčiastka vyvíjaná, čo sa kompatibility týka tak, aby bola použiteľná aj s inými zariadeniami. Umožňuje zachytávanie, čítanie, zápis a emuláciu NFC tagov. [3]

Rovnako ako v predchádzajúcom prípade sa jedná o nástroj, ktorého firmvér sa vyvíja ako otvorený zdrojový kód. Tento kód je aktívne vyvíjaný a dostupný vo verejnom repozitári. Taktiež ako v predchádzajúcom prípade predstavuje užívateľské rozhranie terminálová aplikácia, ktorá sa prípaja k mikrokontroleru, ku ktorému je *HydraNFC* pripojená, pomocou sériového portu. [4]

V čase písania tejto práce je *HydraNFC* dostupný v oficiálnom internetovom obchode [5]. Mikrokontroler *HydraBus*, ktorý je primárne kombatibilný mikrokontroler pre toto riešenie, je avšak nedostupný [6].

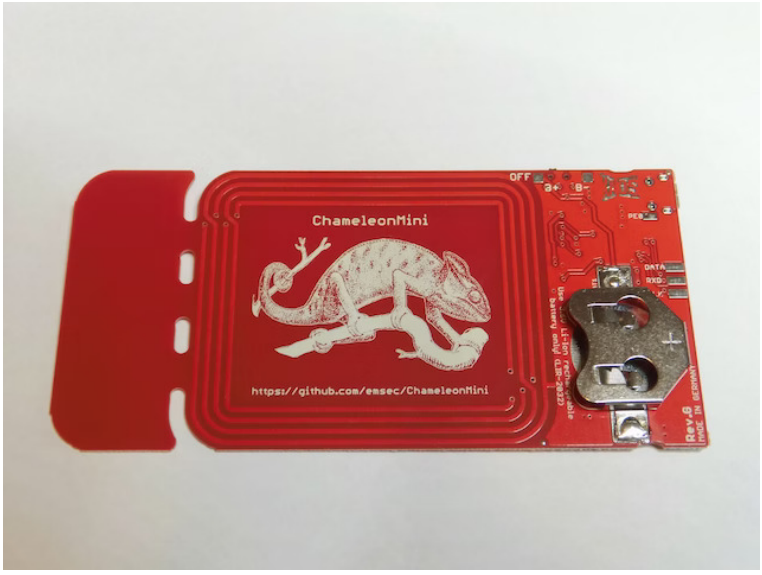


Obr. 2.2: *HydraNFC*. Prevzaté z [3]

2.1.3 ChameleonMini

Tretím existujúcim riešením je nástroj *ChameleonMini*. Medzi jeho hlavné prednosti patrí funkcia klonovania a emulácie NFC karty. Nástroj dokáže naklonovať dôležité informácie o NFC karte a interne si dáta uložiť. Tie potom môžu byť využité pre emuláciu na tom istom nástroji. Vzhľadom aj veľkosťou je podobný NFC karte. [7]

Rovnako ako pri nástrojoch uvedených v predchádzajúcich častiach sa jedná o zariadenie, ktorého firmvér je vytváraný s otvoreným zdrojovým kódom. Ten je prístupný vo verejnom repozitári, do ktorého môže ktokoľvek prispieť svojim príspevkom. [9]



Obr. 2.3: *ChameleonMini*. Prevzaté z [8]

2.1.4 ComProbe NFC Protocol Analyzer

Ako posledné existujúce riešenie uvádzam *ComProbe NFC Protocol Analyzer*. Na rozdiel od prechádzajúcich sa jedná o stopercentne proprietárny nástroj, ktorý bol vyvíjaný firmou *Teledyne LeCroy*. Táto firma stojí aj za vytvorením obslužnej aplikácie *Frontline NFC Protocol Analyzer*. V čase písania tejto práce už nástroj nie je vyvíjaný a je označený za nedostupný. [10]

2.1.5 Zhrnutie

Všetky existujúce riešenia uvádzané v predchádzajúcich častiach spája niekoľko negatívnych vlastností. Prvou z nich je predajná cena. Keďže sa jedná o veľmi špecializované hardvérové zariadenia, ich výrobné náklady spôsobujú pomerne vysokú predajnú cenu. Tento fakt spôsobuje aj druhú negatívnu vlastnosť, ktorou je zhoršená dostupnosť týchto nástrojov na trhu.

Ako sa ukáže v nasledujúcej časti analýzy a s ohľadom na tieto negatíva, javí sa softvérovo definované rádio ako sľubný kandidát na využitie pre analýzu bezdrôtovej komunikácie využívajúcej technológiu NFC.

2.2 Softvérovo definované rádio

V tejto časti práce predstavím technológiu softvérovo definovaného rádia. Analyzujem jej základné vlastnosti a porovnám s existujúcimi riešeniami diskutovanými v predchádzajúcej časti. Nakoniec opíšem aký typ softvérovo definovaného rádia využívam v tejto práci.

2.2.1 Technológia

Ak nie je uvedené inak, čerpám v tejto časti z [11].

Softvérovo definované rádio, bežne označované taktiež skratkou *SDR*, je rádiokomunikačné zariadenie slúžiace na príjem a spracovanie rádiového signálu. Hlavným rozdielom oproti klasickým zariadeniam tohto druhu je, že všetky komponenty, ktoré sú u zariadení klasického typu implementované analógovo, sú v prípade SDR implementované softvérovo. Jedná sa o komponenty ako modulátory, demodulátory, tunery a podobne.

Tento fakt prináša hneď niekoľko výhodných vlastností oproti klasickým rádiokomunikačným systémom. SDR je schopné rovnako kvalitného zachytenia a spracovania rádiového signálu, avšak s využitím menej prostriedkov s lacnejšími produkčnými nákladmi a menšej veľkosti zariadenia. Súčasne dostupné SDR sú veľkostne porovnateľné s prenosnými USB kľúčmi.

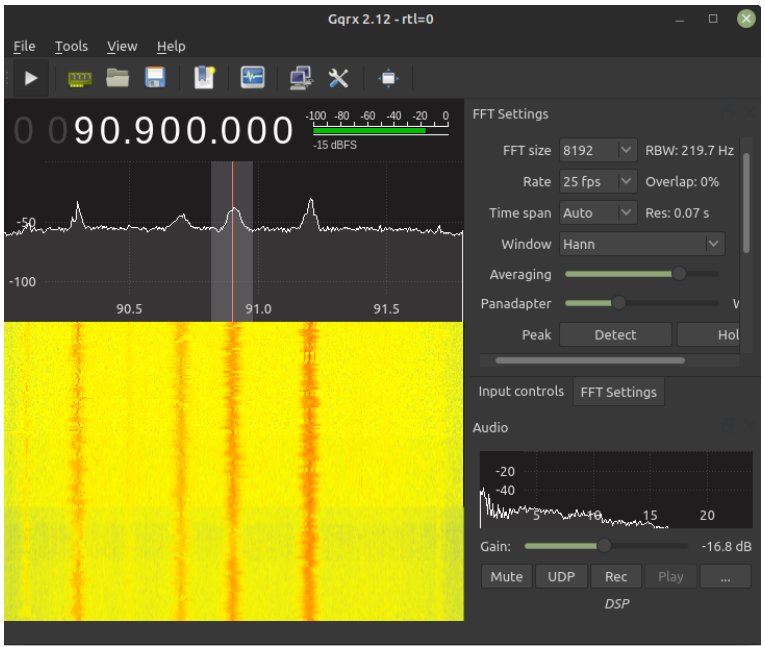
Základným princípom softvérovo definovaného rádia je analógový vstup, ktorý zachytáva analógový rádiový signál. Tento signál je následne posunutý softvéru v zariadení, ktorý ho prevedie a spracuje už digitálne. To umožňuje

veľmi flexibilné zachytávanie aj spracovávanie rádiového signálu z veľkého rozsahu frekvencií. [12]

Existuje veľa druhov bežne dostupných SDR zariadení. Zatiaľ, čo tie lacnejšie dokážu signál iba prijímať, drahšie SDR zariadenia sú schopné okrem prijímania aj signál vysielať. Keďže táto práca sa zaoberá odchytávaním, záznamom a analýzou komunikácie, nie je vysielanie signálu dôležité a ponúka sa tu možnosť využiť aj menej finančne náročné SDR zariadenia.

2.2.2 Porovnanie s existujúcimi riešeniami

V porovnaní s riešeniami diskutovanými v predchádzajúcej časti práce má softvérovo definované rádio hneď niekoľko výhod. Zatiaľ čo diskutované riešenia sú špecializované nástroje určené výhradne na analýzu technológie NFC (prípadne jej nadmnožiny RFID), SDR je schopné zachytávať rádiový signál z väčšej škály rádiových frekvencií. Zároveň je ako technológia omnoho dostupnejšia, keďže je využiteľná v oveľa väčšom množstve odvetví. Týom pádom taktiež existuje veľké množstvo aplikácií, ktoré umožňujú so softvérovo definovaným rádiom pracovať (napríklad *Gqrx* zobrazená na obrázku 2.4).



Obr. 2.4: Zachytávanie signálu pomocou SDR v aplikácii Gqrx. Foto autor

Priamym následkom je značne väčší dopyt a tým pádom väčší výber z rozličných typov a značiek SDR zariadení. Existujú preto ako drahšie, tak aj pomerne lacné SDR zariadenia, ktoré ale dokážu rovnako zachytávať NFC komunikáciu.

Medzi nevýhody SDR patrí neschopnosť spracovania NFC komunikácie. Jedným z cieľov tejto práce je avšak tento problém vyriešiť a implementovať takéto spracovanie dát.

2.2.3 RTL-SDR

V rámci tejto práce pracujem so zariadením značky *RTL-SDR*. V čase písania tejto práce je jeho predajná cena polovičná oproti najlacnejšiemu riešeniu uvedenému v predchádzajúcej časti. Jedná sa o jedno z najrozšírenejších softvérovo definovaných rádií v súčasnosti. Ak neuvádzam inak, čerpám v tejto časti informácie z [11].

Obr. 2.5: *RTL-SDR*. Foto autor

RTL-SDR je softvérovo definované rádio založené na čipe *RTL2832U*. Jedná sa o čip, ktorý sa využíva primárne pre príjem televízneho *DVB-T* signálu. Zistilo sa však, že sa tento čip môže využiť aj pre potreby SDR zariadení a vďaka jeho pomerne nízkej cene sa masívne v rámci SDR trhu rozšíril.

Toto rádio je schopné pracovať na frekvenciách od 13MHz do 1776MHz. Maximálna rýchlosť zachytávania vzoriek je až 3 200 000 vzoriek za sekundu. Autori tohto zariadenia zároveň dodávajú, že zariadenie dokáže spoľahlivo, to znamená bez strát vzoriek, zachytávať až 2 560 000 vzoriek za sekundu.

2.3 NFC

V tejto časti práce predstavím technológiu NFC. Analyzujem základné charakteristiky komunikácie pomocou tejto technológie. Na záver analyzujem možné spôsoby ako možno SDR využiť pre zachytávanie takejto komunikácie.

2.3.1 Základný princíp

Ak nie je uvedené inak, čerpám v tejto časti informácie z [13].

Technológia NFC (z anglického *Near Field Communication*) je technológia bezdrôtovej komunikácie. Je definovaná štandardom ISO 1443. V súčasnosti hrá táto technológia dôležitú úlohu hlavne pri bezkontaktných platbách, identifikácii pomocou NFC kariet a podobne. Pre zjednodušenie v rámci tejto práce budem používať NFC ako názov a skratku tejto technológie (pojem *NFC komunikácia* označuje teda komunikáciu pomocou tejto technológie). Základným princípom NFC je komunikácia medzi *pasívnym* a *aktívnym* zariadením.

Aktívne zariadenie si možno predstaviť ako serverovú stranu komunikácie. Jedná sa napríklad o čítačky NFC kariet, bezkontaktné platobné terminály, mobilné telefóny s integrovanou NFC funkcionalitou a podobne, ktoré sú aktívne napájané a aktívne hľadajú zariadenia v okolí. Tieto zariadenia generujú elektromagnetické pole. Taktiež pravidelne vysielajú signály, na ktoré dokážu ostatné NFC zariadenia (ako *pasívne*, tak aj *aktívne*) zareagovať a tým inicializovať komunikáciu.

Pasívne zariadenie si možno predstaviť ako užívateľskú časť. Jedná sa napríklad o NFC tagy, karty a podobne. Nie sú aktívne napájané, avšak elektromagnetické pole generované *aktívnymi zariadeniami* im umožňuje krátkodobé fungovanie a komunikáciu. Keďže pre fungovanie *pasívneho* zariadenia musí byť toto zariadenie dostatočne blízko k zdroju elektromagnetického poľa, je komunikácia pomocou NFC možná len na vzdialenosť jednotiek centimetrov.

Vďaka rozdielnemu napájaniu oboch typov zariadení je veľký rozdiel medzi silou vysielaného signálu *aktívneho* a *pasívneho* zariadenia. Analýza ukázala, že zatiaľ čo nie je problém zachytiť signál vysielaný čítačkou aj na niekoľko desiatok centimetrov, signál vysielaný NFC kartou môže byť problém zachytiť aj na menšie jednotky centimetrov.

2.3.2 Vlastnosti NFC

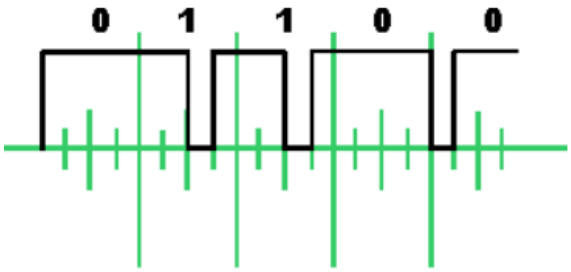
Technológia NFC operuje na frekvencii 13.56 MHz. Na tejto frekvencii operujú všetky zariadenia zapojené do komunikácie. Technológia NFC sa delí na 3 typy. Tieto typy sa líšia v rýchlosti prenášaných dát, modulácii signálu aj kódovaní informácií. V tabuľke nižšie uvádzam krátky prehľad hlavných vlastností jednotlivých typov NFC. [14]

Najrozšírenejším typom NFC je typ A. Jedná sa o typ NFC definovaný štandardom ISO 1443A. Prenos dát počas komunikácie prebieha rýchlosťou 106 000 bitov za sekundu. Modulácia a kódovanie prenášaných dát závisí od typu zariadenia. Dáta posielané aktívnymi zariadeniami sú najprv kódované upraveným Millerovým kódom. [19]

V rámci tohto kódovania sa logická hodnota 1 kóduje vždy ako pokles počas jednej bitovej periódy. Kódovanie logickej hodnoty 0 závisí na hodnote

Typ NFC	Typ zariadenia	Rýchlosť	Modulácia	Kódovanie
A	aktívne	106 Kbps	ASK 100%	upravený Miller
A	pasívne	106 Kbps	Load (ASK)	Manchester
B	aktívne	106 Kbps	ASK 10%	NRZ-L
B	pasívne	106 Kbps	Load (BPSK)	NRZ-L
F	aktívne	212/424 Kbps	ASK 10%	Manchester
F	pasívne	212/424 Kbps	Load (ASK)	Manchester

Tabuľka 2.1: Základné vlastnosti typov NFC. Údaje prevzaté z [15]

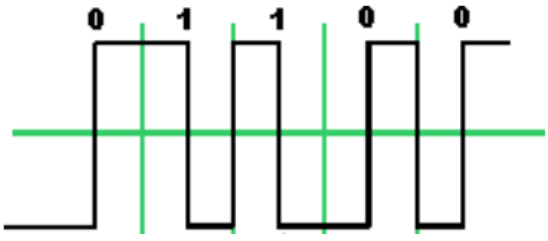


Obr. 2.6: Upravený Millerov kód. Prevzaté z [16]

predchádzajúceho bitu. V prípade predchádzajúcej hodnoty rovnej 0 sa logická hodnota 0 kóduje opačne ako logická hodnota 1, tj. nárast na začiatku bitovej periódy. V prípade, že sa predchádzajúca hodnota rovná hodnote 1, sa logická hodnota 0 kóduje ako zachovanie rovnakej úrovne po celú dobu bitovej periódy.

Po zakódovaní sa dáta prenášajú pomocou modulácie ASK 100%. Táto informácia je dôležitá pre rozpoznanie signálu pri jeho odpočúvaní.

Dáta vysielané pasívnymi zariadeniami sú kódované pomocou Manchester kódu. V porovnaní s kódovaním aktívnych zariadení je tento kód jednoduchší. Logická hodnota 1 sa kóduje ako pokles počas jednej bitovej periódy. Logická hodnota 0 sa kóduje opačným spôsobom. Následne sú zakódované dáta prenášané pomocou Load (ASK) modulácie.



Obr. 2.7: Manchester kód. Prevzaté z [16]

2.3.3 Karty MIFARE

Nasledujúca časť práce obsahuje základné informácie o NFC kartách značky *MIFARE*. Analyzujem najpoužívanejšie karty tejto značky, ich vlastnosti a rozdiely. V rámci práce sa sústredím na zachytávanie kariet typu *MIFARE Classic*, *MIFARE DESFire* a *MIFARE Plus*.

Karty značky MIFARE sa v priebehu posledných niekoľkých rokoch stali najpoužívanejším typom kariet pre integráciu NFC do každodenného života. Niekoľko MIFARE kariet si pravdepodobne nájde každý človek vo svojej peňaženke – sú štandardnou voľbou pre väčšinu bezkontaktných platobných kariet, využívajú sa v rámci občianskych preukazov a cestovných pasov. Taktiež študentské a učiteľské ISIC a ITIC karty sú vyrábané na platforme MIFARE kariet. Vyznačujú sa hlavne nízkou cenou a spoľahlivosťou.

Všetky MIFARE karty, na ktoré sa v rámci práce sústredím, využívajú pre komunikáciu NFC typu A. To znamená, že v rámci komunikácie pomocou NFC prenášajú dáta rýchlosťou 106 000 bitov za sekundu. Tieto bity sú kódované pomocou Manchester kódu a následne modulované pomocou Load (ASK) modulácie. [19]

2.3.4 Bezpečnosť NFC

V tejto časti analyzujem bezpečnosť technológie NFC. Diskutujem možné bezpečnostné slabiny a analyzujem možnosti využitia pri odpočúvaní komunikácie. Ak nie je uvedené inak, čerpám informácie z [17].

Dôležitým aspektom pri každej forme komunikácie je jej zabezpečenie. NFC sa v súčasnosti používa v mnohých systémoch každodenného života a rozširuje sa čoraz viac. Preto je dôležité, aby bola každá takáto komunikácia dostatočne zabezpečená.

Technológia NFC neposkytuje pri zahájení komunikácie žiadnu formu autentifikácie. Jediným bezpečnostným prvkom, na ktoré sa samotná technológia NFC spolieha, je nutnosť malej vzdialenosti (približne do 5 centimetrov) medzi zariadeniami. Táto malá vzdialenosť je nevyhnutná už z fyzikálnej podstaty technológie NFC - je nevyhnutná pre vygenerovanie elektromagnetického poľa a úspešného zahájenia komunikácie. Takáto krátka vzdialenosť je jednoznačne sťažením pre akéhokoľvek potenciálneho útočníka, neelimininuje ale možnosť útoku úplne.

Vďaka tomuto faktu vzniká priestor pre niekoľko rôznych scenárov, ktoré môžu bezpečnosť takejto komunikácie prelomiť:

- odpočúvanie a záznam komunikácie,
- manipulácia s prenášanými informáciami,
- útok prehrávaním zachytenej komunikácie,
- rušenie prebiehajúcej komunikácie.

Jedným z najefektívnejších riešení tohto bezpečnostného problému je implementovanie bezpečných kanálov šifrovaných takými šiframi, ktoré sú v súčasnosti preukázateľne bezpečné. Veľa iných komunikačných technológií (napríklad Bluetooth, Wi-Fi) má takéto bezpečné kanály implementované už vo svojom základe. V prípade technológie NFC je však nutné, aby boli takéto bezpečnostné prvky implementované na aplikačných vrstvách. Implementácie sú dodávané výrobcami a dodávateľmi a často sa jedná o komerčné a proprietárne riešenia.

Existuje však množstvo aplikácií, ktoré využívajú NFC, ale nemajú implementované žiadne ďalšie bezpečnostné prvky. Tieto aplikácie využívajú pasívne NFC zariadenia len ako identifikačný prvok osôb alebo subjektov, ktoré nimi majú disponovať (napríklad otváranie dverí alebo brán, identifikácia osoby pri spoločných tlačiarňach a podobne).

Rovnako, ako má každé sieťové zariadenie svoju unikátnu MAC adresu, má každé pasívne NFC zariadenie svoj unikátny identifikátor - *UID* (z anglického *Unique Identifier*). Hodnotou UID sa pasívne zariadenie identifikuje pri zahájení každej komunikácie pomocou technológie NFC. To umožňuje jednoduchším aplikáciam využívať pasívne NFC zariadenia ako identifikačný prvok - pre každého užívateľa má aplikácia uložené UID jeho pasívneho NFC zariadenia (napríklad NFC tag, NFC karta, alebo tiež mobilné zariadenie s podporou NFC). Pri nasnímaní pasívneho zariadenia aplikácia vyhľadá jeho UID vo svojej databáze a spracuje požiadavku.

Útočník ale môže tento fakt zneužiť. Keby bol schopný odchytiť a zaznamenať UID zariadenia, ktoré má prístup do aplikácie, existuje možnosť "naklonovania"tohto zariadenia a následného prístupu do aplikácie.

2.3.5 Komunikácia medzi zariadeniami

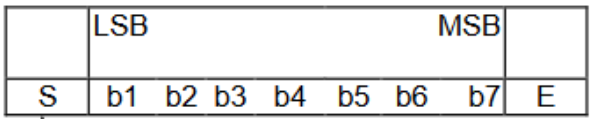
Nasledujúca časť obsahuje analýzu princípu komunikácie medzi aktívnym a pasívnym zariadením pomocou technológie NFC. Ak nie je uvedené inak, čerpám informácie z [18].

Štandard ISO 1443 definuje komunikáciu medzi zariadeniami pomocou technológie NFC s použitím rámcov. Tieto rámce sú definované pre aktívne aj pasívne zariadenia rovnako, na rozdiel od modulácie a kódovania. Zariadenia si pomocou rámcov vymieňajú všetky dáta v priebehu ich komunikácie – príkazy, prenášané údaje, aj kontrolné informácie zaisťujúce integritu samotných rámcov a validitu prenášaných údajov.

ISO 1443 definuje 3 základné typy rámcov:

- krátke rámce,
- štandardné rámce,
- antikolízne rámce.

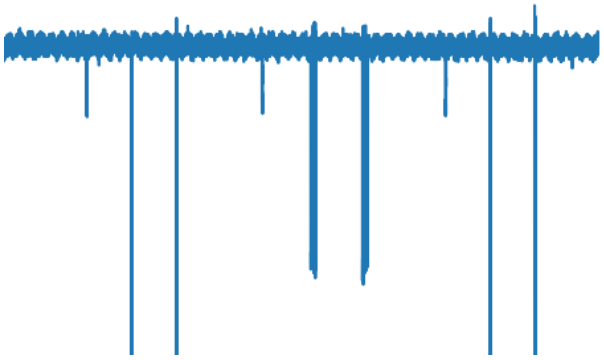
Krátke rámce využívajú najmä aktívne zariadenia na odosielanie príkazov pasívnym zariadeniam. Formát krátkych rámcov je jednoduchý a priamočiary. Prvý bit je označovaný ako *S-bit*, po ktorom nasleduje 7 dátových bitov, ktoré obsahujú prenášaný príkaz. Prvý dátový bit je *LSB* (najmenej významný bit), posledný dátový bit je *MSB* (najviac významný bit). Krátky rámec je ukončený bitom označovaným ako *E-bit*.



Obr. 2.8: Formát krátkeho rámca. Prevzaté z [18]

Medzi najpoužívanejšie príkazy, ktoré sa odosielajú pomocou krátkych rámcov, patria príkazy odosielané aktívnym zariadením s požiadavkou na oživenie pasívneho zariadenia a nadviazanie komunikácie. Najčastejšími takými príkazmi sú:

- *REQA (0x26)* - príkaz, ktorý aktívne zariadenie pravidelne vysiela do okolia,
- *WUPA (0x52)* - príkaz ktorým sa aktívne zariadenie snaží aktivovať pasívne zariadenie.

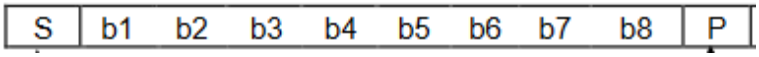


Obr. 2.9: Pravidelné vysielanie príkazu *REQA* čítačkou. Foto autor

Krátke rámce v sebe neobsahujú žiadny kontrolný bit, ktorý by zaisťoval integritu prenášaného príkazu. V prípade, že sa v priebeho fyzického prenosu rámec poškodí, pasívne zariadenie naň nijako nereaguje. Aktívne zariadenie zároveň príkazy odosiela v pravidelných intervaloch až do momentu, kedy nedostane odpoveď.

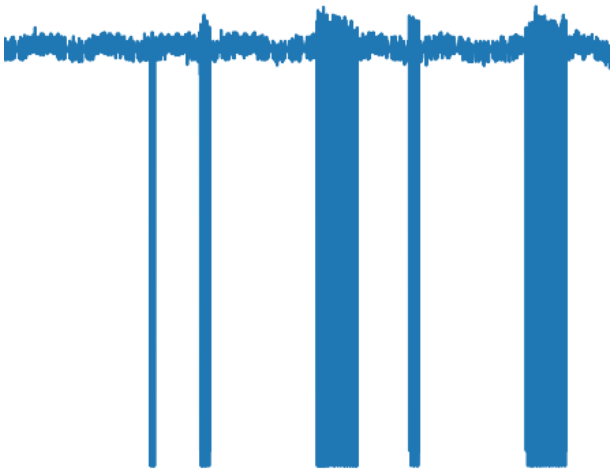
Štandardné rámce sa využívajú na prenos špecifickejších príkazov spolu s prenosom dát. Na ich začiatku sa znova objavuje *S-bit*, ktorý značí začiatok

rámca. Po tomto bite nasleduje *n * (8+1)* bitov pre *n* väčšie než 1, kde *n* môžeme považovať za počet sekcií v rámci jedného konkrétneho štandardného rámca. Každá táto časť obsahuje 8 dátových bitov a jeden kontrolný *P-bit* (parita). Rovnako ako pri krátkych rámcoch, aj v štandardných rámcoch je prvý dátový typ *LSB* a posledný (ôsmy) dátový bit v rámci svojej sekcie *MSB*.



Obr. 2.10: Formát štandardného rámca po prvý *P-bit*. Prevzaté z [18]

Antikolízne rámce sa využívajú pri nadväzovaní komunikácie medzi aktívnym a pasívnym zariadením. Štandard ISO 1443 pre ne definuje niekoľko pravidiel, ktoré majú zaručiť, že v prípade interakcie viacerých pasívnych zariadení s jedným aktívnym zariadením v jeden moment, nedôjde v rámci komunikácie ku ich kolízii.



Obr. 2.11: Antikolízne rámce vysielané aktívnym zariadením. Foto autor

Formát antikolíznych rámcov je rovnaký ako formát štandardných rámcov popísaný vyššie. Pre túto prácu je avšak dôležité zistenie, že v rámci antikolíznych rámcov sa medzi zariadeniami prenáša UID pasívneho zariadenia oboma stranami. V prípade odpočúvania tejto antikolíznej sekvencie pri zahájení komunikácie sa tým pádom naskytuje príležitosť pre zachytenie celej hodnoty UID pasívneho zariadenia, ktoré sa snaží o komunikáciu s aktívnym zariadením.

2.3.6 Nadviazanie komunikácie

Aktívne zariadenie pravidelne vysiela do svojho okolia príkaz *REQA*. Jedná sa o príkaz, ktorým vyzýva všetky pasívne zaradenia k zahájeniu komunikácie. V prípade, že sa pasívne zariadenie priblíži dostatočne blízko, elektromagnetické pole aktívneho zariadenia ho aktivuje. Pasívne zariadenie odpovedá na príkaz *REQA* príkazom *ATQA*, čím zahájí antikolíznu sekvenciu. Tento príkaz obsahuje, okrem iného, aj informáciu o veľkosti UID daného pasívneho zariadenia.

Podľa veľkosti UID pasívneho zariadenia sa UID rozdelí na 1 až 3 časti. Pasívne zariadenie informuje v príkaze *ATQA* aktívne zariadenie o tom, na koľko častí je nutné jeho UID rozdeliť. Prípustné veľkosti UID aktívneho zariadenia sú 4 bajty (nerozdeľuje sa), 7 bajtov (rozdeľuje sa na 2 časti) a 10 bajtov (rozdeľuje sa na 3 časti).

Aktívne zariadenie podľa tohto príkazu postupne odošle príkaz *SEL*. Tento príkaz má tri podoby - pre každú časť UID jednu. Tieto sú podľa potreby postupne odosielané pasívnemu zariadeniu. Pasívne zariadenie na tieto príkazy odpovedá hodnotami svojho UID. Po odoslaní smerom od pasívneho zariadenia odošle aktívne zariadenie znova príkaz *SEL*, tentokrát však s doplnenou časťou UID, ktorú obdržal od pasívneho zariadenia.

Prvý bajt odoslanej časti UID môže obsahovať ešte doplňujúce informácie. V prípade, že sa prvý bajt v prvej alebo druhej časti UID rovná hodnote *88*, táto hodnota nepatrí k samotnému UID. Signalizuje totiž, že UID nie je kompletné a je nutné odoslať ďalšiu jeho časť. V prípade, že sa UID skladá len z jednej časti (tj. jeho veľkosť sa rovná 4 bajtom), a prvý bajt sa rovná hodnote *08*, ostatné 3 bajty obsahujú náhodné hodnoty, ktoré sú generované dynamicky pri každom použití karty. Takéto UID majú napríklad cestovné pasy. Hodnota štvorbajtového fixne nastaveného UID karty by teda podľa štandardu ISO 1443-A nemala obsahovať na pozícii prvého bajtu hodnoty *08* a *88*.

Vďaka tomuto faktu je možné UID pasívneho zariadenia odchytiť aj zo silného signálu vysielaného aktívnym zariadením. Nie je nutné spoliehať sa na signál od pasívneho zariadenia, ktorý býva mnohonásobne slabší a tým pádom ťažší na odchytenie.

2.3.7 Zhrnutie

NFC je technológia bezdrôtovej komunikácie medzi aktívnym (čítačka, terminál) a pasívnym (karta, tag) zariadením využívajúca frekvenciu 13.56MHz. Existujú tri základné typy NFC, pričom najpoužívanejší je NFC typu A. Tento typ používajú aj karty MIFARE, ktoré sa radia medzi najpoužívanejšie NFC karty v súčasnosti. V rámci tejto práce sa teda sústredím na NFC typu A, avšak riešenie bude navrhované s dôrazom na možné rozšírenie na ostatné typy NFC v budúcnosti.

NFC technológia vo svojom základe neposkytuje žiadne šifrovanie ani formu autentifikácie. Spolieha sa len na malú vzdialenosť, ktorá je nutná pre nadviazanie komunikácie medzi aktívnym a pasívnym zariadením. To vytvára priestor pre prípadné odpočúvanie komunikácie.

Každé pasívne zariadenie je jednoznačne identifikované unikátnym identifikátorom – UID. Niektoré služby využívajú pre autentifikáciu len tento identifikátor. Spoločne s možným odpočúvaním sa stáva pre útočníka veľmi zaujímavou informáciou, ktorú sa môže pokúsiť odchytiť.

V rámci nadväzovania komunikácie sa počas antikolíznej sekvencie prenáša medzi aktívnym a pasívnym zariadením informácia o celom UID pasívneho zariadenia. V prípade odpočúvania tejto sekvencie môže útočník získať čiastočnú až úplnú informáciu o UID pasívneho zariadenia.

2.4 Odpočúvanie NFC pomocou SDR

V rámci tejto práce sa snažím využiť absenciu šifrovania a autentifikácie pri komunikácií pomocou technológie NFC. Popis tejto zraniteľnosti sa nachádza už v predchádzajúcich častiach tejtopráce. V nasledujúcej časti analyzujem možné spôsoby a postupy využitia softvérovo definované rádio na odpočúvanie, záznam a analýzu komunikácie pomocou NFC.

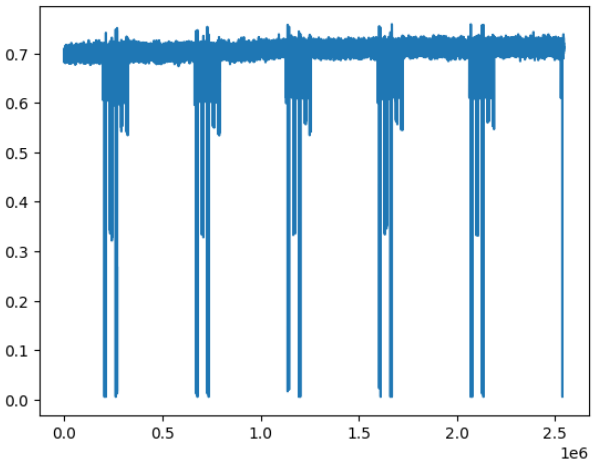
Pre túto prácu je dôležité, aby vybrané softvérovo definované rádio, v tomto prípade zariadenie RTL-SDR popísané v predchádzajúcich častiach práce, umožňovalo odpočúvanie na rovnakej frekvencii ako prebieha komunikácia pomocou technológie NFC, tj. 13.56MHz. RTL-SDR takéto odpočúvanie umožňuje, keďže dokáže pracovať na frekvenciách od 13MHz až do 1766 MHz. Taktiež je schopné dostatočne rýchlo zachytávať vzorky, keďže najrýchlejší typ NFC prenáša dáta rýchlosťou 424 000 bitov za sekundu. RTL-SDR spoľahlivo zachytáva až 2 560 000 vzoriek za sekundu, čím ponúka možnosť zachytávať dostatočný počet vzoriek na spoľahlivé dekódovanie prenášaných dát.

2.4.1 Rozpoznanie signálu

V tejto časti analyzujem, ako dobre je signál vysielaný NFC zariadeniami rozoznateľný pri zachytávaní pomocou RTL-SDR. Výsledky v tejto časti sú dosiahnuté opakovaným meraním. Dipólová anténa, ktorú som pri týchto meraniach spolu s RTL-SDR používal, bola umiestnená nad NFC čítačkou.

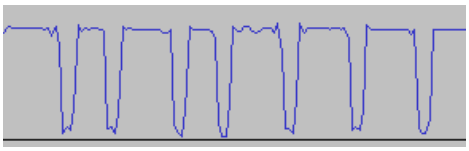
Prvé merania boli zamerané na lokalizovanie signálu vysielaného čítačkou. Pre tieto účely som zvolil zachytávanie dvoch sekúnd so vzorkovaciou frekvenciou 1 248 000 vzoriek za sekundu (tj. 12 vzoriek na jeden bit prenášaných dát) na frekvencii 13.56MHz s dipólovou anténou umiestnenou nad čítačkou. Výsledky tohto merania možno vidieť na nasledujúcom obrázku.

Na obrázku sú jasne viditeľné poklesy amplitúdy. Je teda pravdepodobné, že sa jedná o pravidelné správy vysielané čítačkou. V predchádzajúcich častiach



Obr. 2.12: Signál vysielaný NFC čítačkou. Foto autor

analýzy som zistil, že jedným z príkazov, ktoré čítačka (tj. aktívne zariadenie) pravidelne vysiela, je príkaz *REQA*. Priblíženie jedného z týchto poklesov je zobrazené na obrázku nižšie.



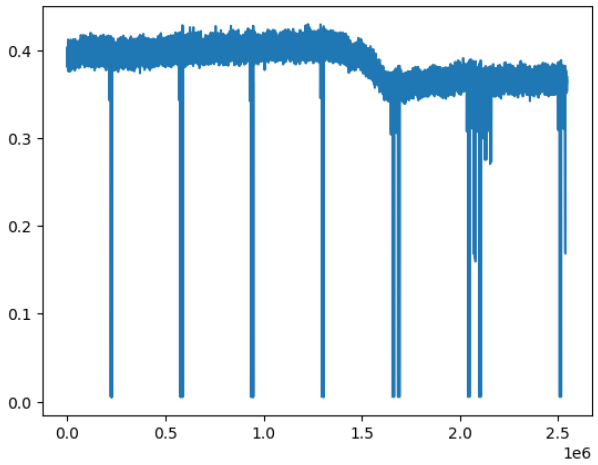
Obr. 2.13: Príkaz *REQA* vysielaný čítačkou. Foto autor

Z obrázku a získaných informácií z predchádzajúcich častí som zistil, že sa jedná o signál, ktorý je možné dekódovať pomocou upraveného Millerovho kódu. Po dekódovaní je možné signál interpretovať ako krátky NFC rámec príkazu *REQA*.

Nasledujúce merania som uskutočnil s rovnakým nastavením softvérovo definovaného rádia, avšak spoločne s interakciou rôznych NFC kariet s čítačkou. Výsledky týchto meraní ukázali miernu zmenu amplitúdy pri interakcii NFC karty s čítačkou. Táto zmena je pravdepodobne spôsobená elektromagnetickým poľom, ktoré čítačka vytvorila a z ktorého sa NFC karta nabila a aktivovala.

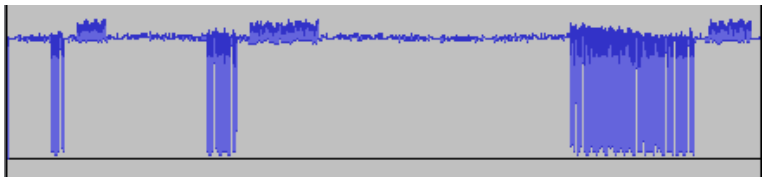
Po priblížení jednotlivých poklesov amplitúdy sa mi podarilo rozpoznať (okrem príkazov *REQA*) aj ďalšie príkazy vysielané aktívnymi zariadeniami. Jednalo sa o príkazy antikolíznej sekvencie opísanej v predchádzajúcich častiach práce. Jeden z týchto príkazov bol aj už opisovaný príkaz *SEL*, obsahujúci celé UID karty využitej pri tomto meraní.

V mnohých opakovaných meraniach som však nedokázal rozoznať signál



Obr. 2.14: Signál interakcie NFC čítačky s NFC kartou. Foto autor

vysielaný kartou. To sa mi podarilo iba pri jednom z meraní, pri ktorom bola zachytená celá antikolízna sekvencia.



Obr. 2.15: Antikolízna sekvencia zachytená pomocou SDR. Foto autor

Na predchádzajúcom obrázku možno vidieť príkaz *REQA* vyslaný čítačkou, na ktorý karta odpovedá príkazom *ATQA*. Tento príkaz obsahuje informáciu o tom, že UID tejto karty sa skladá iba z jednej časti, tj. jeho veľkosť je 4 bajty. Nasledujúcim príkazom *SEL* vyzýva čítačka kartu o zaslanie prvej (a efektívne jedinej) časti jej UID, ktorú čítačka následne vysiela. Posledný príkaz vysielaný čítačkou je znova *SEL*, doplnený o celé znenie prvej časti UID karty. Posledný príkaz vysielaný kartou je príkaz *SAL*, ktorým karta potvrdzuje kompletnosť UID.

Z meraní uskutočnených v tejto časti som zistil, že pri úspešnom zachytení a dostatočne silnom signále vysielanom oboma typmi zariadení je možné jednotlivé vysielané sekvencie spoľahlivo rozpoznať. Následne možno tieto sekvencie dekódovať a interpretovať ako jednotlivé príkazy podľa štandardu ISO 1443-A. Taktiež som zistil, že zatiaľ čo zachytávať signál vysielaný aktívnymi zariadeniami je možné aj na väčšiu vzdialenosť, signál vysielaný pasívnymi zariadeniami nie je jednoduché zachytiť. V ďalších častiach analýzy je teda nutné analyzovať spôsoby, ako signál vysielaný pasívnymi zariadeniami za-

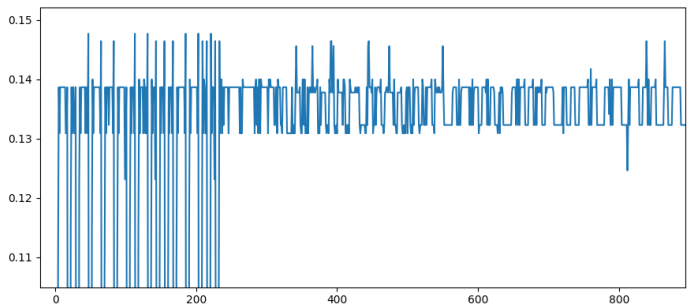
chytávať spoľahlivejšie a aké kritéria sú k takémuto zachytávaniu nutné.

2.4.2 Výber a konfigurácia antény

V tejto časti mojej práce opisujem postupný výber a nastavenie antény používanej v praktickej časti práce spoločne so softvérovo definovaným rádiom RTL-SDR. V priebehu tohto procesu som postupne analyzoval rôzne typy antén a ich konfigurácie, rovnako ako umiestnenie antény voči NFC karte a čítačke. Mojou snahou bolo získať čo najlepšie výsledky pri zachytávaní NFC signálu od oboch strán. V rámci tejto časti prezentujem aj výsledky meraní s rôznymi konfiguráciami skúšaných antén. Na obrázkoch je vždy viditeľná správa vysielaná smerom od čítačky, na ktorú odpovedala karta. Obrázky obsahujú celú správu od čítačky a celú správu od karty a následný signál, kedy nevysielalo žiadne zariadenie.

V prvotných fázach analýzy rôznych antén a ich konfigurácie som sa zameral na rôzne polohovanie antény medzi čítačkou a kartou. Po niekoľkých meraniach som zistil, že pri umiestnení antény medzi kartu a čítačku, sa najlepšie výsledky získavajú pri anténe umiestnenej pri karte, ktorá je zároveň umiestnená v najväčšej možnej vzdialenosti od čítačky. Pri umiestnení antény priamo na čítačku merania dosahovali slabšie výsledky.

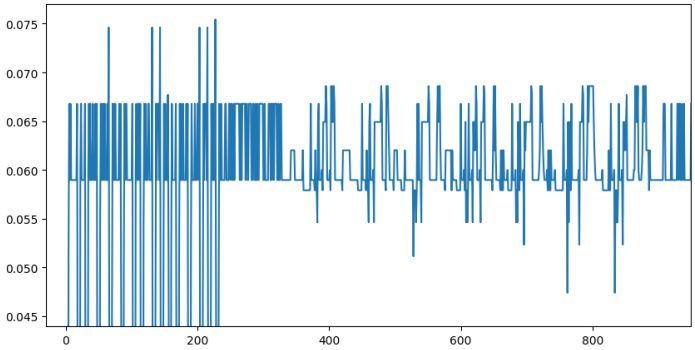
Softvérovo definované rádio RTL-SDR je dodávané s jednoduchou dipólovou anténou. Jej ramená je možné nastaviť na dĺžku od 5 centimetrov do približne 15 centimetrov. V rámci prvých meraní som zistil, že táto dipólová anténa nemá problém zachytiť vysielané správy smerom od NFC čítačky. Prvotné merania boli uskutočnené s ramenami vysunutými na maximálnu dĺžku. Anténa bola umiestnená medzi čítačku a kartu. Výsledné meranie bolo vždy veľmi podobné tomu, aké je viditeľné na obrázku 2.16.



Obr. 2.16: Meranie dipólovou anténou s vysunutými ramenami. Foto autor

Zatiaľ, čo signál vysielaný čítačkou bol odchytený bez väčších problémov, okolitý šum bol príliš výrazný pre zachytenie signálu od karty.

Pri skrátení ramien dipólovej antény na minimum (približne 5 centimetrov) som následne opakoval rovnaké meranie s veľmi podobnými výsledkami. Ako je viditeľné na obrázku 2.17, signál od karty je o niečo výraznejší, avšak okolitý šum stále sťažuje detekciu tohto signálu.



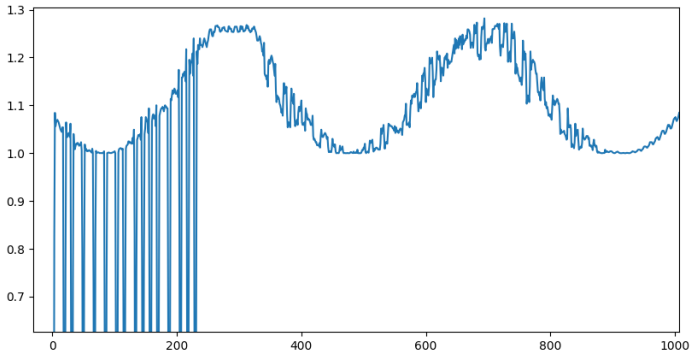
Obr. 2.17: Meranie dipólovou anténou so stiahnutými ramenami. Foto autor

Predchádzajúce merania dokázali, že zachytávať správy vysielané čítačkou nepredstavuje problém. Správy vysielané kartou sa ale ani pri malých zmenách v konfigurácií a umiestnení antény medzi čítačkou a kartou nepodarilo spoľahlivo zachytávať. Rozhodol som sa preto analyzovať iný typ antény.

Ďalšie merania som uskutočnil s anténou určenou priamo pre prácu s technológiou NFC. Na internete je možné zakúpiť takéto antény, ktoré sú podobné tým, ktoré využíva napríklad už existujúce riešenie HydraNFC diskutované v predchádzajúcich častiach práce. Na obrázku 2.18 je možné vidieť NFC anténu využitú v rámci tejto práce.

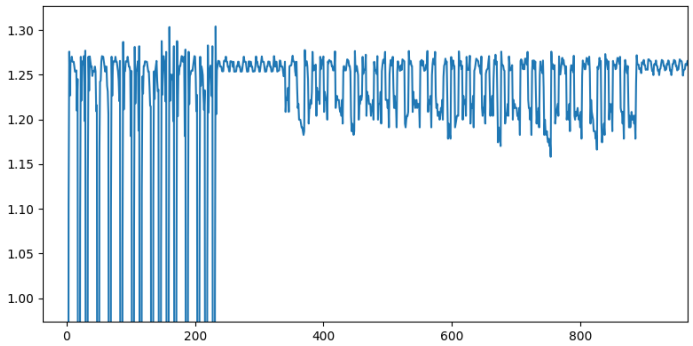
Obr. 2.18: NFC anténa. Foto autor

Po niekoľkých prvotných meraniach rôznych vzdialeností a umiestnení medzi anténou a čítačkou som dospel k rovnakým výsledkom — anténa najlepšie zachytáva signál pri umiestnení pri karte a zároveň čo najďalej od čítačky. Už v tejto fáze bolo jednoznačné, že anténa je s RTL-SDR plne kompatibilná a (ako je viditeľné na 2.19) dokáže zachytávať signál od karty.



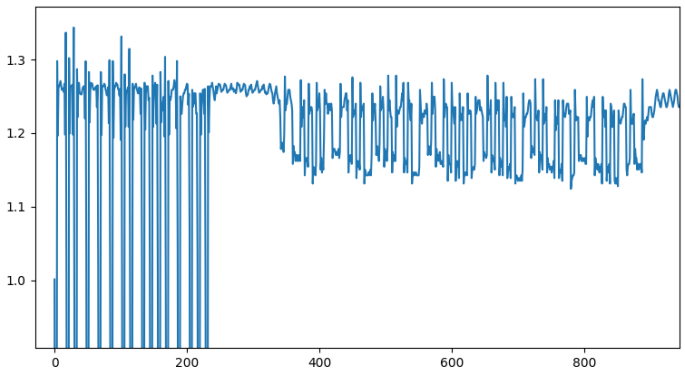
Obr. 2.19: Meranie NFC anténou na frekvencii 13.56MHz. Foto autor

Ako je z obrázku vyššie viditeľné, v zachytených dátach je správa vysielaná kartou výrazne viditeľnejšia než v predchádzajúcich meraniach uskutočnených s dipólovou anténou. Taktiež je viditeľné, že pre zlepšenie signálu je nutné upraviť hodnotu nastavenia stredovej frekvencie na rádiu. Po niekoľkých meraniach som zistil, že najlepšie výsledky získavam pri nastavení stredovej frekvencie na 13.56MHz s posunom o ďalších 750Hz. Zachytený signál s takto nastavenou stredovou frekvenciou je možné vidieť na obrázku 2.20.



Obr. 2.20: Meranie NFC anténou na stredovej frekvencii 13560750Hz. Foto autor

So snahou o ďalšie zlepšenie zachytávaného signálu som sa vrátil k rôznym umiestneniam antény voči odchytávaným zariadeniam. Prekvapivé výsledky priniesli merania so zmenou umiestnenia antény nad kartu a čítačku. Na obrázku 2.21 je viditeľné, že v takejto konfigurácií sa odchytený signál vysielaný čítačkou nezhorší a zároveň signál vysielaný kartou je ešte výraznejší.

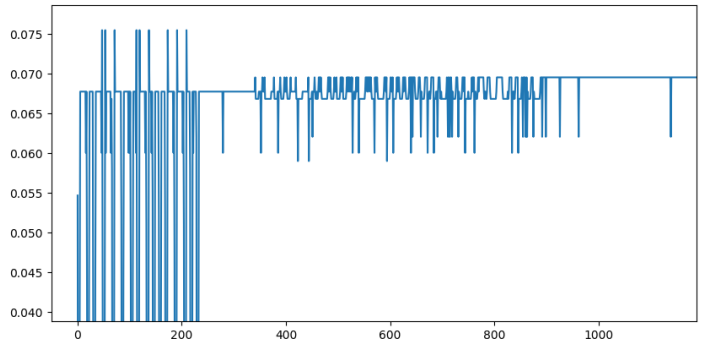


Obr. 2.21: Meranie NFC kartou umiestnenou nad kartu a čítačku. Foto autor

Opakované merania priniesli podobné výsledky. Signál vysielaný kartou je najvýraznejší pri umiestnení antény nad kartu a čítačku.

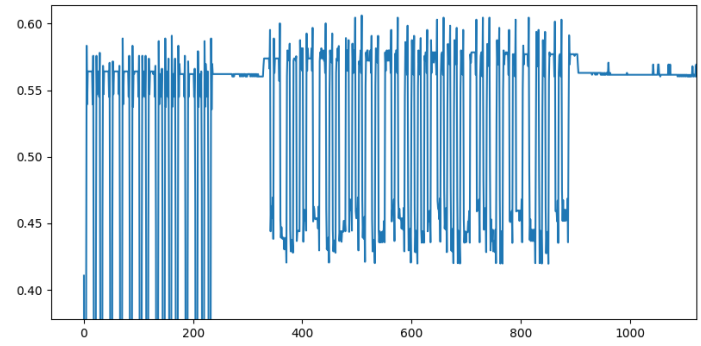
V nasledujúcej fáze analýzy a výberu antény som sa vrátil k práci s dipólovou anténou. Spolu so získanými informáciami z meraní s využitím NFC antény som umiestnil dipólovú anténu, s ramenami nastavenými na vzdialenosť približne 5 centimetrov, nad kartu a čítačku. Ako ukazuje 2.22, signál vysielaný kartou bol o čosi výraznejší ako pri predchádzajúcich meraniach s

dipólovou anténou, avšak v porovnaní s výsledkami NFC antény bol signál menej výrazný.



Obr. 2.22: Merania dipólovou anténou so stiahnutými ramenami umiestnenou nad kartu a čítačku. Foto autor

Prekvapivé výsledky priniesla posledná fáza testovania s dipólovou anténou. Zistil som, že pri vzájomnom spojení ramien dokáže dipólová anténa zachytiť signál vysielaný kartou rovnako dobre a niekedy dokonca lepšie než NFC anténa. Takéto výsledky sú viditeľné na 2.23.



Obr. 2.23: Meranie dipólovou anténou so spojenými ramenami. Foto autor

Analýza popísaná v tejto časti práce ukazuje, že pre ďalšie použite (najmä v praktickej časti práce) je možné využiť ako NFC anténu, tak aj dipólovú anténu so spojenými ramenami. Dôležitým predpokladom sa stalo aj umiestnenie antény, ktoré pre najlepšie výsledky predstavuje umiestnenie priamo nad kartu a čítačku tak, ako je možné vidieť na 2.24.

Obr. 2.24: Konfigurácia dipólovej antény s najlepšími výsledkami. Foto autor

Opakované merania s oboma typmi antén ukázali, že zachytávanie signálu vysielaného kartou nie je stopercentne spoľahlivé ani pri dodržaní vyššie spomenutých kritérií. Pre merania bolo použitých niekoľko typov kariet s rovnakým výsledkom. Pri návrhu riešenia je teda dôležité dbať na správne zachytávanie a analýzu najmä signálu vysielaného aktívnymi zariadeniami (v tomto prípade čítačkou NFC kariet).

2.5 Užívateľská aplikácia

Jedným z cieľov tejto práce je aj návrh a realizácia užívateľskej aplikácie. V tejto časti práce analyzujem rôzne možnosti realizácie takejto aplikácie.

2.5.1 Forma

Jedným z najdôležitejších rozhodnutí pri návrhu užívateľskej aplikácie je výber formy tejto aplikácie. Jedná sa primárne o spôsob, akým bude užívateľ k aplikácií pristupovať. Aplikácia má byť primárne určená pre použitie s platformou Raspberry Pi, ku ktorej bude pripojené softvérovo definované rádio. Jedná sa o minipočítače, ku ktorým sa dá pripojiť externý displej, avšak vlastný displej neobsahujú.

Po pripojení dotykového displeja môže užívateľ využívať Raspberry Pi ako každý iný bežný počítač. V prípade klasického, tj. nie dotykového displeja, je ale nutné pripojiť k Raspberry Pi taktiež klávesnicu a prípadne myš, čo nemusí byť pre užívateľa priestorovo výhodné v prípade, kedy s Raspberry Pi nechce pracovať (napríklad) v laboratórnych podmienkach.

Objavuje sa tu ďalší problém. K Raspberry Pi bude pripojené pomocou USB softvérovo definované rádio. K rádiu následne bude pripojená anténa. V prípade použitia externého displeja by bol užívateľ nútený byť fyzicky

prítomný pri Raspberry Pi, to znamená tiež k softvérovo definovanému rádiu a aj zariadeniu, ktoré sa snaží odchytiť.

Existuje však iná možnosť než využitie externého displeja. V [20] sa uvádza, že platforma Raspberry Pi ponúka možnosť vytvárať bezdrôtové Wi-Fi siete. Je teda možné pripojiť sa k takejto bezdrôtovej Wi-Fi sieti z druhého zariadenia, ktoré môže byť fyzicky spolu s užívateľom vzdialené aj niekoľko jednotiek metrov. Následne je možné pristupovať k Raspberry Pi ako ku každému inému zariadeniu umiestnenému v rovnakej sieti.

Naskytuje sa tu teda možnosť vytvoriť užívateľskú aplikáciu tak, aby bola dosiahnuteľná vzdialene po pripojení k bezdrôtovej sieti generovanej zariadením Raspberry Pi. užívateľsky prívetivá teda môže byť webová aplikácia, ktorá by užívateľovi umožňovala pracovať s celým riešením navrhnutým v tejto práci.

2.5.2 Funkcie

Užívateľská aplikácia má umožňovať zachytávanie a prvotnú analýzu NFC komunikácie. Pre plnohodnotné využitie navrhnutého riešenia by mala užívateľovi umožňovať okrem jednorazového zachytenia a analýzy NFC komunikácie tento krok vykonávať opakovane. K tomu bude potrebné navrhnúť užívateľskú aplikáciu tak, aby umožňovala správu už zachytenej a zanalyzovanej komunikácie.

Okrem toho môže užívateľ ďalej pracovať so zachytenou komunikáciou. K tomu môže chcieť využiť iné spôsoby než je užívateľská aplikácia. Z toho dôvodu by mala užívateľská aplikácia umožňovať sťahovať jednotlivé zachytené vzorky do zariadenia, z ktorého užívateľ bude k aplikácii pristupovať. Tieto stiahnuté dáta by mali obsahovať všetky informácie, ktoré navrhnuté riešenie zo zachytenej komunikácie dokázalo zistiť. Taktiež by mali obsahovať samotné zachytené vzorky tak, ako ich softvérovo definované rádio zachytilo.

Ak užívateľ nepotrebuje zachytenú a zanalyzovanú komunikáciu stiahnuť do svojho zariadenia, mala by užívateľská aplikácia umožňovať zobraziť čo najviac získaných informácií priamo v aplikácii.

V predchádzajúcich častiach analýzy som zistil, že pre správne a najlepšie zachytávanie NFC komunikácie je niekedy nutné upraviť základné nastavenie softvérovo definovaného rádia. K správnemu fungovaniu navrhnutého riešenia bude teda vhodné užívateľovi umožniť toto nastavenie zmeniť. Aplikácia by mala teda obsahovať sekciu, v ktorej budú jednotlivé hodnoty nastavenia softvérovo definovaného rádia, ktoré bude môcť užívateľ jednoducho upraviť.

Analýza rôznych antén tiež ukázala, že zachytávať správy vysielané aktívnym zariadením je možné aj na väčšiu vzdialenosť, avšak zachytávať správy vysielané pasívnym zariadením môže predstavovať problém aj na malé jednotky centimetrov. Ak si bude užívateľ vedomý toho, že navrhnuté riešenie nebude schopné zachytávať správy vysielané pasívnym zariadením, mala by užívateľská aplikácia umožňovať túto časť analýzy vypnúť.

2.5.3 Technológia

Samotné jadro navrhnutého riešenia má byť naprogramované v jazyku Python. Je preto vhodné využiť jazyk Python aj pre realizáciu užívateľskej aplikácie. Ako bolo diskutované v predchádzajúcich častiach, najlepším kandidátom pre užívateľskú aplikáciu je webová aplikácia. Pre programovací jazyk Python existuje množstvo frameworkov, ktoré umožňujú tvorbu webových aplikácií. Pre túto prácu je ale nutné myslieť aj na fakt, že navrhnuté riešenie bude spúšťané na platforme Raspberry Pi. Je preto vhodné vybrať pre tvorbu aplikácie taký framework, ktorý bude jednoduchý a nebude zbytočne zaťažovať zariadenie, na ktorom bude finálne riešenie spúšťané.

Jedným z najjednoduchších a najmenej výkonovo náročných frameworkov pre tvorbu webových aplikácií v programovacom jazyku Python je framework *Flask*. Okrem tvorenia webových aplikácií umožňuje bezproblémovo integrovať aj ďalšie súčasti navrhnutého riešenia. Bude možné teda ovládať aj nastavovať softvérovo definované rádio priamo prostredníctvom webovej aplikácie, rovnako ako ovládať všetky funkcie navrhnutého riešenia, ktoré bude zachytávať a analyzovať NFC komunikáciu.

Kapitola 3

Návrh

V tejto časti práce využívam informácie získané v predchádzajúcej kapitole práce a vytváram návrh prenosného zariadenia, ktoré bude umožňovať zachytávanie, zaznamenávanie a prvotnú analýzu komunikácie využívajúcu technológiu NFC. Postupne opisujem princípy, ktoré bude finálne riešenie využívať k tomu, aby spomenuté úkony boli užívateľovi umožnené vykonávať pomocou obslužnej aplikácie spúšťanej na platforme Raspberry Pi.

3.1 Práca so vzorkami

V rámci tejto časti opisujem návrh práce so vzorkami, ktoré bude riešenie zachytávať a následne v rámci prvotnej analýzy spracovávať. Dokumentujem postupy a metódy, ktoré bude navrhnuté riešenie využívať.

3.1.1 Zachytávanie komunikácie

Pre zachytávanie komunikácie bude využívané softvérovo definované rádio RTL-SDR. Pripojené bude k RPi minipočítaču pomocou USB. RPi bude softvérovo definované rádio obsluhovať a nastavovať. Zachytená komunikácia bude zaznamenávaná do pamäte RPi, kde bude následne prebiehať jej analýza. Všetky nutné úkony budú automatizované a naprogramované pomocou programovacieho jazyku Python.

3.1.2 Analýza komunikácie

Analýza zachytenej komunikácie bude prebiehať na minipočítači RPi. Na tento účel budú využité znalosti získané v predchádzajúcej kapitole.

V priebehu analýzy budú zachytené vzorky postupne digitalizované. Následne v digitalizovaných vzorkách bude nástroj vyhľadávať sekvencie vysielané aktívnymi a pasívnymi zariadeniami. Po ich dekódovaní ich nakoniec

preloží do podoby NFC rámcov. V závere analýzy sa vyhľadajú rámce obsahujúce UID pasívnych zariadení a tieto informácie sa extrahujú.

Celá logika analýzy bude naprogramovaná v programovacom jazyku Python. Kompletná analýza bude zaznamenaná do pamäte RPi, z ktorej ju bude možné načítať a prezerať.

3.2 Užívateľská aplikácia

Dôležitou súčasťou navrhovaného riešenia je užívateľská aplikácia. Pomocou tejto aplikácie bude užívateľ ovládať celé riešenie. Je preto dôležité ju navrhnúť tak, aby bol užívateľ schopný pracovať so všetkými súčasťami riešenia čo najefektívnejšie a užívateľsky najprívetivejšie.

3.2.1 Forma

Užívateľskú aplikáciu bude tvoriť webová aplikácia. Táto webová aplikácia bude spúšťaná na platforme Raspberry Pi. Bude prepájať samotné jadro navrhovaného riešenia popisované v predchadzajúcej časti práce s webovým prostredím, cez ktoré bude užívateľ riešenie ovládať.

Užívateľ bude k webovej aplikácií pristupovať zo svojho zariadenia. K tomu bude využívaná schopnosť RPi vytvárať bezdrôtové Wi-Fi siete. Po spustení aplikácie vytvorí RPi počítač takúto bezdrôtovú sieť, ku ktorej sa užívateľ pripojí zo svojho zariadenia. Následne bude schopný k webovej aplikácii pristupovať prostredníctvom webového prehliadača.

Webová aplikácia bude taktiež naprogramovaná pomocou programovacieho jazyka Python s využitím frameworku Flask. Takto naprogramovaná aplikácia bude jednoducho spolupracovať so samotným jadrom riešenia, ktoré bude zachytávať a analyzovať NFC komunikáciu a zároveň nebude zbytočne zaťažovať RPi, na ktorom bude aplikácia spúšťaná.

3.2.2 Funkcie

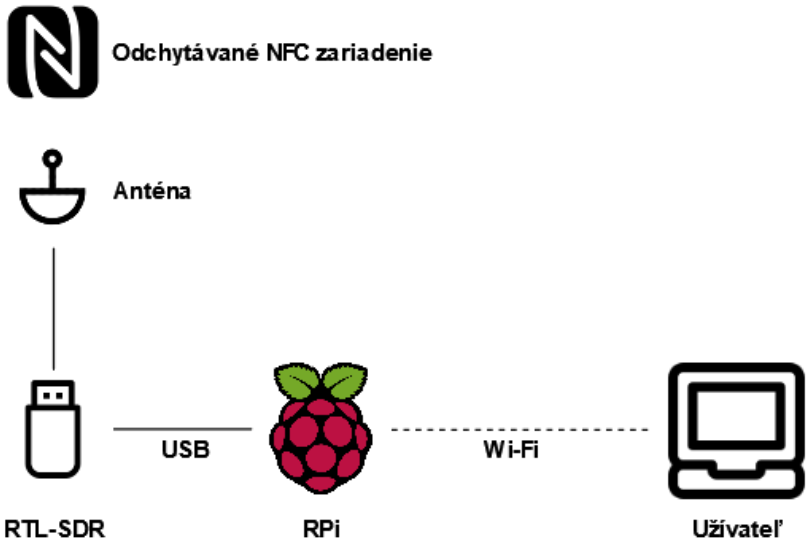
Užívateľská aplikácia bude obsahovať všetku funkcionalitu nutnú pre plnohodnotné ovládanie navrhnutého riešenia. K hlavným funkciám webovej aplikácie bude patriť schopnosť zachytávať komunikáciu po časový interval, ktorý nastaví užívateľ. Okrem toho bude užívateľ schopný prostredníctvom webovej aplikácie prezerať zachytenú a zanalyzovanú komunikáciu. Pre každú analýzu bude možné prezerať zachytené UID pasívnych zariadení a preložené NFC rámce. Každú analýzu bude užívateľ schopný stiahnuť do svojho zariadenia. Takto stiahnuté analýzy budú obsahovať všetky zachytené vzorky, rovnako ako všetky informácie, ktoré analýza pomocou navrhovaného riešenia získala. Takýmto spôsobom bude môcť užívateľ pokračovať v ďalšej analýze zachytenej komunikácie mimo navrhnuté riešenie na svojom zariadení.

Webová aplikácia bude taktiež umožňovať užívateľovi zmeniť základné nastavenie softvérovo definovaného rádia. V analýze v predchádzajúcej kapitole práce som zistil, že pre dosiahnutie najlepšieho výsledku odpočúvania NFC môže byť výhodné zmeniť nastavenie SDR. Preto bude takéto zmeny nastavenia umožňovať aj užívateľská aplikácia.

Jednou z funkcii užívateľskej aplikácie bude aj možnosť deaktivovať vyhľadávanie správ vysielaných pasívnym zariadením. Keďže analýza ukázala, že zachytávanie takýchto príkazov pomocou SDR môže byť veľmi náročné, môže byť pre užívateľa výhodné túto funkcionalitu vypnúť.

3.3 Zhrnutie

Navrhnuté riešenie bude zachytávať NFC komunikáciu pomocou softvérovo definovaného rádia RTL-SDR. To bude pripojené pomocou USB k RPi minipočítaču. Zachytávaná komunikácia bude zaznamenávaná na RPi, kde bude následne analyzovaná. Kompletné analýzy zachytených komunikácií budú uložené na RPi, kde ich bude užívateľ schopný prezerať pomocou užívateľskej aplikácie. Užívateľská aplikácia bude prístupná vo forme webovej aplikácie. Táto bude užívateľovi prístupná po pripojení k bezdrôtovej Wi-Fi sieti vytvorenej RPi minipočítačom. Užívateľská aplikácia bude okrem zachytávania a prezerania NFC komunikácie umožňovať aj sťahovanie kompletných analýz a nastavovanie softvérovo definovaného rádia.



Obr. 3.1: Diagram navrhovaného riešenia. Foto autor

Kapitola 4

Realizácia

Nasledujúca kapitola obsahuje postupnú dokumentáciu realizácie riešenia navrhnutého v predchádzajúcej časti práce. Celé riešenie je implementované v programovacom jazyku Python. Na úvod opisujem najdôležitejšie implementované triedy. Následne popisujem použité technológie a implementačné princípy, ktoré sú v implementovaných triedach využívané pre zachytávanie a analýzu NFC komunikácie. Na záver opisujem realizáciu užívateľskej aplikácie, jej konfiguráciu a postup inštalácie celého finálneho riešenia.

4.1 Trieda `NfcSdr`

Najdôležitejšou implementovanou triedou je trieda `NfcSdr`. Táto trieda predstavuje rozhranie, cez ktoré je možné ovládať zachytávanie a analýzu NFC komunikácie. Taktiež umožňuje zobrazovanie analyzovaných dát.

Pre jednoduchú implementáciu všetkých typov NFC využíva trieda `NfcSdr` niekoľko enumerácií, ktoré popisujú jednotlivé typy NFC:

- **`NfcType`** – enumerácia opisujúca všeobecný typ NFC. Je využívaná pre popis jednotlivých zachytených vzoriek. Môže nadobúdať hodnoty `NfcA`, `NfcB` a `NfcF`,
- **`NfcMessageType`** – enumerácia popisujúca zariadeniami vysielané správy. Jednoznačne popisuje typ NFC a zariadenia. Môže nadobúdať hodnoty `NfcActiveA`, `NfcPassiveA`, `NfcActiveB`, `NfcPassiveB`, `NfcActiveF` a `NfcPassiveF`.

Trieda `NfcSdr` obsahuje niekoľko metód, ktoré umožňujú plne ovládať celé riešenie:

- **`capture(time, type)`** – metóda umožňuje zachytávať komunikáciu podľa typu zvoleného užívateľom (argument `type`, využíva enumeráciu `NfcType`) po užívateľom zadanú dobu v sekundách (argument `time`),

- `analyze()` – metóda umožňuje analýzu doposiaľ nezanalyzovaných vzoriek, ktoré užívateľ zachytil pomocou metódy `capture`.

Okrem toho obsahuje niekoľko premenných, v ktorých sú uložené jednotlivé dáta a nastavenia ovplyvňujúce zachytávanie a analýzu komunikácie:

- `raw_records` – premenná, do ktorej sa ukladajú všetky vzorky zachytené metódou `capture`,
- `analyzed_records` – premenná, do ktorej sa ukladajú všetky vzorky zanalyzované pomocou metódy `analyze`,
- `sdr_center_freq` – hodnota stredovej frekvencie nastavovaná softvérovo definovanému rádiu,
- `sdr_bandwidth` – šírka pásma nastavovaná softvérovo definovanému rádiu,
- `search_card` – hodnota `True/False` rozhodujúca o vyhľadávaní sekvencií vysielaných pasívnymi zariadeniami v priebehu analýzy,
- `card_coefficient` – koeficient využívaný pri vyhľadávaní sekvencií vysielaných pasívnymi zariadeniami (princíp popísaný v ďalších častiach práce),
- `reader_coefficient` – koeficient využívaný pri vyhľadávaní sekvencií vysielaných aktívnymi zariadeniami (princíp popísaný v ďalších častiach práce).

K prehľadnej implementácií používa trieda `NfcSdr` niekoľko dátových tried, ktoré reprezentujú základné prvky NFC komunikácie.

4.1.1 Dátová trieda `NfcRawRecord`

Táto trieda reprezentuje zachytenú komunikáciu pomocou softvérovo definovaného rádia. Inštancie tejto triedy sú vytvárané metódou `capture` triedy `NfcSdr`. Obsahuje nasledujúce premenné:

- `raw_samples` – dáta tak, ako ich zachytilo softvérovo definované rádio,
- `digital_samples` – digitalizované dáta zachytené softvérovo definovaným rádiom,
- `type` – typ NFC komunikácie, využíva enumeráciu `NfcType`.

4.1.2 Dátová trieda `NfcRecord`

Dátová trieda reprezentujúca zanalyzovanú komunikáciu. Okrem dát prevzatých z `NfcRawRecord` obsahuje všetky informácie, ktoré boli získané v priebehu analýzy (ktorá je popísana v ďalších častiach práce). Menovite sa jedná o premenné:

- **`raw_samples`** – dáta tak, ako ich zachytilo softvérovo definované rádio,
- **`digital_samples`** – digitalizované dáta zachytené pomocou softvérovo definovaného rádia,
- **`type`** – typ NFC komunikácie, využíva enumeráciu `NfcType`,
- **`messages`** – jednotlivé vysielané správy, ktoré analýza objavila. Využíva dátovu triedu `NfcMessage` opisovanú v ďalšej časti,
- **`uids`** – jednotlivé časti UID pasívnych zariadení, ktoré boli vyextrahované z objavených správ.

4.1.3 Dátová trieda `NfcMessage`

Táto trieda reprezentuje jednotlivé vysielané správy, ktoré dokázala analýza objaviť. Obsahuje všetky dôležité informácie o danej správe spolu s jej obsahom. Obsahuje premenné:

- **`start`** – štartovacia pozícia správy v rámci vzoriek `raw_samples`, respektíve `digital_samples` z nadradenej triedy `NfcRecord`,
- **`end`** – koncová pozícia v rámci `raw_samples`, respektíve `digital_samples` z nadradenej triedy `NfcRecord`,
- **`coded_bits`** – zakódované bity správy,
- **`decoded_bits`** – dekódované bity správy,
- **`raw_frame`** – dekódované bity správy reprezentované ako príslušny NFC rámec,
- **`text`** – textový názov rámca v prípade, že je možné ho identifikovať,
- **`device_type`** – typ NFC a zariadenia, využíva `NfcMessageType`.

4.2 Obsluha RTL-SDR

Nasledujúca časť obsahuje dokumentáciu implementácie obsluhy SDR. Pre obsluhu softvérovo definovaného rádia RTL-SDR sa využíva knižnica `pyrtlsdr`. Jedná sa o knižnicu priamo určenú pre prácu s daným softvérovo definovaným rádiom. Umožňuje jeho inicializáciu a nastavenie, rovnako ako zachytávanie vzoriek.

4.2.1 Nastavenie SDR

RTL-SDR sa inicializuje vždy pri zavolaní metódy `capture` z triedy `NfcSdr`. Týmto spôsobom nie je rádio zbytočne zaťažované mimo nevyhnutný čas. Taktiež tento postup umožňuje aktualizáciu nastavenia po zmene premenných na to určených v triede `NfcSdr`.

Nastavenie vzorkovacej frekvencie závisí od daného typu NFC. Pre každý typ je definovaná hodnota `multiplier`. Samotná hodnota sa následne vypočíta ako *106 000* * `multiplier`. Pre NFC typu A je táto hodnota nastavená na hodnotu *12*. Keďže tento typ prenáša dáta rýchlosťou 106 000 bitov za sekundu, výsledná vzorkovacia frekvencia zaručí 12 vzoriek pre každý bit prenesenej informácie.

4.2.2 Zachytávanie komunikácie

Samotné zachytávanie komunikácie pomocou SDR prebieha po jeho inicializácii a nastavení. Užívateľ pri volaní metódy `capture` zadá požadovaný čas, po ktorý sa má komunikácia zachytávať. Podľa času a vypočítanej vzorkovacej frekvencie sa vypočíta počet cyklov zaznamenania 1000 vzoriek pre dosiahnutie požadovaného časového intervalu.

Knižnica *pyrtlsdr* umožňuje asynchronné zachytávanie malého počtu vzoriek. Týmto spôsobom nedochádza k žiadnej strate vzoriek pri ich zachytávaní. Vzorky sú zachytávané v podobe *I/Q vzorkovania*. Jedná sa o formu reprezentácie signálu v trojdimenzionálnom priestore pomocou iracionálnych čísel. Pre ďalšie použitie sú tieto vzorky spracované vzorcom $\sqrt{real^2 + imag^2}$. Pomocou tohto vzorca získame maximálnu hodnotu amplitúdy pre danú vzorku, ktorá je pre nás najdôležitejšia.

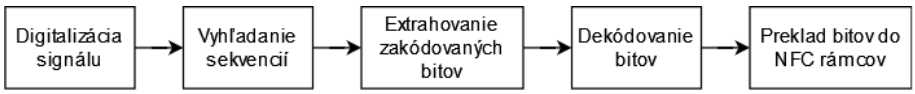
Pre zrýchlenie celého procesu práce so vzorkami prebieha v rámci zachytávania komunikácie aj prvý krok analýzy – digitalizácia signálu vysielaného aktívnymi zariadeniami. Týmto spôsobom sa taktiež znižuje riziko chybovosti, keďže sa vždy digitalizuje malý počet vzoriek. Princíp digitalizácie je popísaný v ďalšej časti práce.

Na záver sa takto spracované vzorky zo všetkých cyklov uložia ako inštancia dátovej triedy `NfcRawRecord` spolu s informáciou o type zachytávaného NFC. Táto inštancia sa ukladá do premennej `raw_records` triedy `NfcSdr`.

4.3 Analýza komunikácie

V nasledujúcej časti dokumentujem implementáciu analýzy vzoriek zachytených pomocou SDR. Pre implementáciu bol použitý programovací jazyk Python. Väčšina matematických úkonov a úkonov nad veľkým počtom vzoriek je implementovaných pomocou knižnice *numpy*. Táto knižnica niekoľkonásobne urýchľuje prácu nad veľkým počtom vzoriek v porovnaní s bežnými spôsobmi pri práci s programovacím jazykom Python.

Analýza vzoriek sa primárne sústredí na vyhľadanie a analýzu signálu vysielaného aktívnymi zariadeniami. Signál vysielaný pasívnymi zariadeniami sa analyzuje v závislosti na výsledkoch analýzy signálu vysielaného aktívnymi zariadeniami. Oba typy analýzy sa primárne skladajú z piatich krokov, ktorých postupnosť možno vidieť na obrázku nižšie.



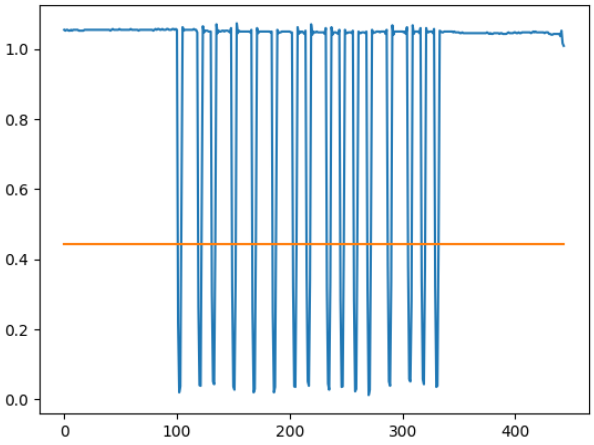
Obr. 4.1: Postup analýzy zachytených vzoriek. Foto autor

Výsledky analýzy sa ukladajú ako inštancia dátovej triedy `NfcRecord` do premennej `analyzed_records` triedy `NfcSdr`.

4.3.1 Digitalizácia signálu

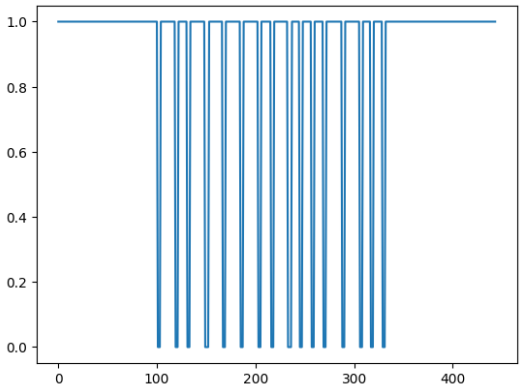
Digitalizáciu signálu možno popísať ako transformáciu zachytených vzoriek z pôvodných hodnôt do hodnôt 0/1. Keďže je vysielaný signál jednoznačne rozpoznateľný podľa poklesu amplitúdy v zachytených vzorkách, je možné určiť *rozhodovaciu hodnotu*, podľa ktorej sa takáto transformácia následne vykoná.

Pri digitalizácií signálu vysielaného aktívnymi zariadeniami sa pre rozhodovaciu hodnotu využíva maximálna hodnota z nespracovaných vzoriek, na ktoré sa má digitalizácia aplikovať. Tá je následne násobená hodnotou `reader_coefficient` z triedy `NfcSdr`. Predvolená hodnota je rovná *1/3*. Na obrázku nižšie možno vidieť takúto hodnotu porovnanú s nespracovanými vzorkami.



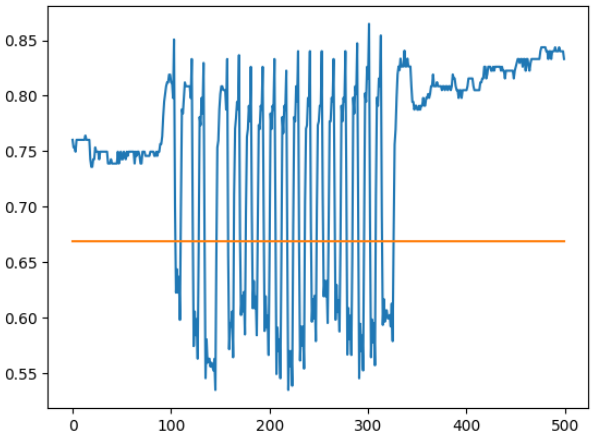
Obr. 4.2: Rozhodovacia hodnota spolu so signálom aktívneho zariadenia. Foto autor

Po výpočte tejto hodnoty sa následne každá hodnota nespracovanej komunikácie s touto hodnotou porovná a nastaví na 0/1 podľa toho, či je *rozhodovacia hodnota* väčšia (prípadne rovnaká) alebo nižšia. Výsledok takejto transformácie možno vidieť na nasledujúcom obrázku.



Obr. 4.3: Digitalizované vzorky. Foto autor

Podobný princíp sa využíva aj pri analýze signálu vysielaného pasívnym zariadením. V priebehu digitalizácie takéhoto signálu sa využíva minimálna hodnota z nespracovaných vzoriek. Táto hodnota je následne násobená hodnotou `card_coefficient` z triedy `NfcSdr`. Predvolená hodnota je rovná `1.2`. Výslednú *rozhodovaciu hodnotu* v porovnaní s nespracovanými vzorkami je možné vidieť na nasledujúcom obrázku.



Obr. 4.4: Rozhodovacia hodnota spolu so signálom pasívneho zariadenia. Foto autor

Každá hodnota z nespracovaných vzoriek sa s touto hodnotou porovnáva a nastavuje na 0/1 podľa toho, či je *rozhodovacia hodnota* menšia (prípadne rovnaká) alebo väčšia.

4.3.2 Vyhľadávanie sekvencií aktívnych zariadení

Po digitalizácii vzoriek možno vyhľadať tie sekvencie, ktoré nás v rámci analýzy zaujímajú. Kompletné zachytené vzorky obsahuju množstvo "hluchých" sekvencií, počas ktorých nevysielali žiadne NFC zariadenia.

Počas analýzy signálu vysielaného aktívnym zariadením je začiatok sekvencie vysielanej takýmto zariadením jasne detekovateľný ako prvý pokles z hodnoty 1 na hodnotu 0 v digitalizovaných vzorkách. Implementácia prehlási takúto sekvenciu za ukončenú v momente, kedy objaví 30 po sebe idúcich hodnôt 1 v digitalizovaných sekvenciách. Tento postup sa aplikuje na celé digitalizované vzorky, čím sa vyextrahujú dvojice pozícií pre všetky sekvencie vysielané aktívnym zariadením.

V prípade vyhľadávania sekvencií vysielaných pasívnym zariadením je postup podobný. Začiatok takejto sekvencie je jasne detekovateľný v digitalizovaných vzorkách ako zmena z hodnoty 0 na hodnotu 1. Zároveň sa prehľadávajú len tie rozsahy vzoriek, ktoré sa nachádzajú medzi už nájdenými sekvenciami aktívnych zariadení. Pasívne zariadenia totiž vysielajú signál len ako reakciu na signál vyslaný aktívnym zariadením. Je preto zbytočné prehľadávať celé digitalizované vzorky. Zároveň je v rámci jedného rozsahu vzoriek vyhľadávaná maximálne jedna sekvencia vysielaná pasívnym zariadením.

4.3.3 Extrahovanie zakódovaných bitov

Ako bolo diskutované už v predchádzajúcich častiach, pre NFC typu A sa komunikácia zachytáva so vzorkovaciou frekvenciou *106 000 * 12*. NFC technológia typu A prenáša dáta rýchlosťou 106 000 bitov za sekundu, čo znamená, že vo vyhľa-daných sekvenciách predstavuje každých 12 vzoriek 1 bit informácie. Pri extrahovaní zakódovaných bitov z týchto sekvencií sa znižuje počet vzoriek podľa aplikovaného kódovania.

Aktívne zariadenia využívajú pre kódovanie upravený Millerov kód. Toto kódovanie možno prezentovať ako rozdelenie každého bitu na 4 časti. Implementácia teda z digitalizovaných vzoriek postupne vyberá jednu vzorku z každej postupnosti 4 vzoriek.

Pasívne zariadenia využívajú pre kódovanie Manchester kód. Toto kódovanie možno prezentovať ako rozdelenie každého bitu na dve časti. Implementácia postupne priemeruje každých 6 bitov, túto hodnotu zaokrúhľuje a ukladá.

Zatiaľ čo pred extrahovaním zakódovaných bitov môže figurovať aj v digitalizovaných vzorkách nejaká forma šumu, extrahované bity by už mali byť pre opakovaný signál toho istého príkazu vždy totožné. Implementované

riešenie tento fakt využíva pri analýze signálu aktívnych zariadení. Súbor `frames.py` obsahuje slovník základných príkazov, ktoré aktívne zariadenia vysielajú, identifikované práve zakódovanými bitmi. Implementácia sa pokúsi extrahované bity v tomto slovníku nájsť. V prípade nájdenia zhody ďalšie kroky nevykonáva a len skopíruje informácie o danom príkaze z daného záznamu v slovníku.

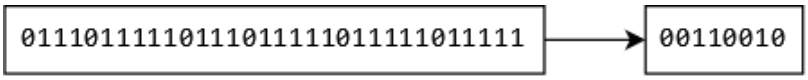
Užívateľ môže do slovníka pridať ďalšie príkazy. Slovník momentálne obsahuje príkazy *REQA*, *WUPA* a príkaz *SEL*, žiadajúci zaslanie prvej a druhej časti UID pasívneho zariadenia.

4.3.4 Dekódovanie bitov

Následným krokom analýzy je dekódovanie extrahovaných zakódovaných bitov. To prebieha podľa pravidiel diskutovaných v predchádzajúcich častiach práce.

Pre signál aktívnych zariadení sa využívajú pravidlá upraveného Millerovho kódu, pre signál pasívnych zariadení pravidlá Manchester kódu.

Výsledkom tohto kroku sú jednotlivé bity NFC rámcov. V prípade aktívnych zariadení sa zredukuje počet bitov na štvrtinu, v prípade pasívnych zariadení na polovicu.

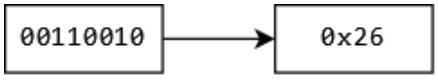


Obr. 4.5: Príklad dekódovania bitov – príkaz *REQA*. Foto autor

4.3.5 Preklad bitov

Posledným krokom samotného spracovania vzoriek je preklad dekódovaných bitov do NFC rámcov v čitateľnej forme. Implementácia podľa počtu bitov rozhodne o tom, či sa jedná o rámec v krátkom alebo štandardnom tvare a podľa toho postupne preloží bity do dvojíc bajtov. V prípade štandardných rámcov preskakuje kontrolné bity.

Výsledkom je NFC rámec v čitateľnej podobe.



Obr. 4.6: Príklad prekladu bitov do NFC rámca – príkaz *REQA*. Foto autor

4.3.6 Vyhľadávanie UID pasívnych zariadení

Implementované riešenie na záver analýzy vyhľadá v získaných NFC rámcoch UID pasívnych zariadení. Z predchádzajúcich častí práce je známy formát príkazov *SEL*, ktoré obsahujú jednotlivé časti UID. Nástroj vyhľadá dané rámce v dlhšej forme, ktorá indikuje, že tieto sú doplnené o hodnotu častí UID. Tú z rámcov vyextrahuje a následne uloží.

4.3.7 Analýza sekvencií pasívnych zariadení

Užívateľ má možnosť vypnúť celkovú analýzu sekvencií pasívnych zariadení. V prípade, že je táto analýza zapnutá, riešenie pridáva analýzu signálu vysielaného pasívnymi zariadeniami za analýzu každej sekvencie aktívneho zariadenia.

Pasívne zariadenie vysiela signál jedine ako odpoveď na signál už predtým vyslaný aktívnym zariadením. Po analýze každej sekvencie aktívneho zariadenia nastáva postupne digitalizácia signálu pasívneho zariadenia od konca práve zanalyzovanej sekvencie aktívneho zariadenia po začiatok ďalšej takej sekvencie. Po digitalizácii nasledujú všetky ostatné kroky analýzy popísané v predchádzajúcich častiach práce.

V prípade, že sa užívateľ rozhodne analýzu sekvencií pasívnych zariadení vypnúť, implementované riešenie postupne zanalyzuje len nájdené sekvencie aktívnych zariadení.

4.4 Užívateľská aplikácia

V nasledujúcej časti tejto práce popisujem implementáciu užívateľskej aplikácie. Postupne dokumentujem jej fungovanie, nastavenie a inštaláciu.

Užívateľská aplikácia je implementovaná formou webovej aplikácie. Tá je spúšťaná na minipočítači Raspberry Pi. Prístupná je pomocou bezdrôtovej Wi-Fi siete, ktorú vytvára Raspberry Pi. Aplikácia je naprogramovaná v programovacom jazyku Python s využitím frameworku Flask.

4.4.1 Raspberry Pi

Pri implementácii som kládol dôraz na správne fungovanie finálneho riešenia na minipočítačoch Raspberry Pi. Z toho dôvodu som pre vývoj webovej aplikácie vybral framework Flask, ktorý umožňuje takéto aplikácie vytvárať bez zaťažovania prostriedkov zariadenia, na ktorom je finálna aplikácia spúšťaná.

Užívateľská aplikácia taktiež využíva schopnosť Raspberry Pi vytvárať bezdrôtové Wi-Fi siete. Vďaka tomu je webová časť užívateľskej aplikácie dostupná užívateľovi, ktorý sa so svojim zariadením pripája na túto Wi-Fi sieť.

4.4.2 hostapd

Pre softvérové riadenie a nastavenie bezdrôtovej Wi-Fi siete, ktorá je spomenutá v predchádzajúcich častiach práce, využíva implementované riešenie softvérového démona *hostapd*. Jedná sa o softvérové riešenie, ktoré umožňuje plne využiť potencionál Raspberry Pi vytvárať takéto bezdrôtové siete.

Pre túto prácu bola najdôležitejšia možnosť vytvárať zaheslované Wi-Fi siete. Vďaka tomu môže užívateľ pristupovať k webovej časti aplikácie bezpečne. Taktiež umožňuje užívateľovi zmeniť heslo, prípadne aj názov vytváranej Wi-Fi siete.

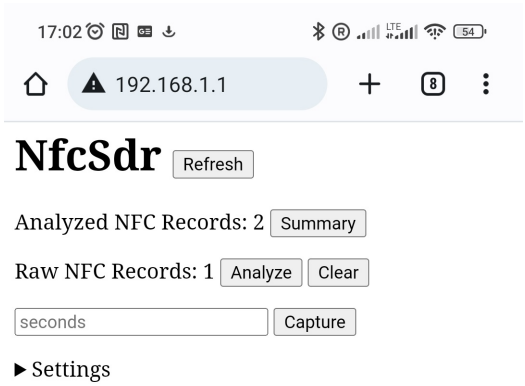
V rámci implementácie užívateľskej časti som naprogramoval aj skript, ktorý umožňuje zmeniť vyššie uvedené nastavenia bez nutnosti úpravy konfiguračných súborov samotného hostapd. Tento skript spolu s inštalačným skriptom je popísaný v ďalších častiach práce.

4.4.3 Webová aplikácia

Najdôležitejšou súčasťou užívateľskej aplikácie je jej webová časť. Jedná sa o prostredie, ktorým užívateľ pristupuje k celému riešeniu. Je prístupná po zadaní IP adresy `192.168.1.1` do webového prehliadača. Umožňuje ovládanie celého riešenia popisovaného v predchádzajúcich častiach práce.

Webová aplikácia je naprogramovaná v jazyku Python s využitím frameworku Flask. Hlavná logika celej webovej aplikácie a funkcionalita jednotlivých podstránok aplikácie je naprogramovaná v súbore `webserver.py`. Vzhľad jednotlivých podstránok je definovaný pomocou *HTML* súborov, ktoré sa nachádzajú v priečinku `templates`. Framework Flask umožňuje využívať tieto súbory ako šablóny, do ktorých vkladá požadované dáta.

V rámci šablón, ktoré webová aplikácia využíva, je nadefinovaný aj responzívny dizajn. Tento dizajn umožňuje užívateľovi jednodnoducho využívať aplikáciu aj na mobilných zariadeniach.



Obr. 4.7: Hlavná stránka webovej aplikácie na mobilnom zariadení. Foto autor

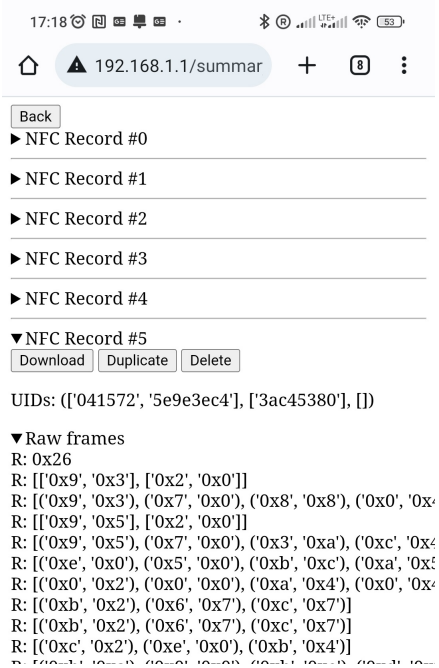
Hlavná stránka webovej aplikácie obsahuje všetky pre užívateľa relevantné funkcie a informácie. Užívateľ je schopný zachytávať NFC signál po zadaní časového intervalu a stlačení tlačidla *Capture*. Po jeho stlačení začne aplikácia zachytávať signál. Po úspešnom zachytení požadovaného časového intervalu je o tomto užívateľ informovaný a presmerovaný späť na hlavnú stránku.

Užívateľ môže pred začiatkom analýzy zachytávať ľubovoľný počet komunikácií. Tie sa postupne ukladajú, čím sa zvyšuje počítadlo *Raw NFC Records*. Užívateľ je následne schopný buď všetky tieto vzorky vymazať kliknutím na tlačidlo *Clear* alebo spustiť ich analýzu pomocou tlačidla *Analyze*.

O úspešnom ukončení analýzy je užívateľ informovaný a následne presmerovaný späť na hlavnú stránku. Zistené informácie sú dostupné na samostatnej stránke, na ktorú sa užívateľ dostane pomocou tlačidla *Summary* umiestneného vedľa počtu analyzovaných vzoriek označených na hlavnej stránke ako *Analyzed NFC Records*.

4.4.4 Správa zachytených dát

Webová aplikácia umožňuje zobraziť najdôležitejšie informácie získané analýzou zachytených vzoriek. Pre každú analýzu vytvorí aplikácia vlastný odstavec, ktorý môže užívateľ rozkliknúť. Webová aplikácia umožňuje zobrazenie zachytených NFC rámcov a extrahovaných UID pasívnych zariadení.



Obr. 4.8: Výsledky analýzy vo webovej aplikácií. Foto autor

Na predchádzajúcom obrázku sú zobrazené výsledky analýzy, ktorá objavila 3 časti UID pasívnych zariadení – 2 prvé časti a 1 druhú časť. Okrem toho je možné si zobraziť všetky preložené NFC rámce.

Každú analýzu môže užívateľ vymazať pomocou tlačidla *Delete*. V prípade, že chce analýzu vzoriek uskutočniť opakovane (napríklad s iným nastavením vzťahujúcim sa na analýzu signálu pasívnych zariadení), dokáže vzorky duplikovať pomocou tlačídla *Duplicate*. Toto tlačidlo duplikuje všetky dáta nutné pre opätovnú analýzu, ktorá je opäť uskutočniteľná na hlavnej stránke.

Pomocou tlačidla *Download* dokáže užívateľ stiahnuť kompletnú analýzu danej komunikácie. Týmto spôsobom získa kompletné výsledky analýzy spoločne so všetkými dátami, ktoré k daným výsledkom viedli.

4.4.5 Formát stiahnutých dát

Webová aplikácia umožňuje užívateľovi stiahnuť výsledky ľubovoľnej analýzy, ktorá bola v rámci aplikácie uskutočnená. Jedná sa o archív obsahujúci 3 súbory:

- `raw_samples.npy` – pôvodné dáta tak, ako ich zachytilo softvérovo definované rádio,
- `digital_samples.npy` – dáta z `raw_samples.npy` po procese digitalizácie,
- `data.json` - dáta získané analýzou.

Výsledky získané analýzou sú štrukturovane uložené v súbore `data.json`. Obsahujú typ NFC, extrahované časti UID pasívnych zariadení a všetky informácie o zachytených správach, ktoré obsahuje aj trieda `NfcMessage`.

4.4.6 Konfigurácia aplikácie

Na hlavnej stránke webovej aplikácie dokáže užívateľ v sekcii *Settings* zmeniť fungovanie SDR prostredníctvom zmeny premenných triedy `NfcSdr`. Po rozkliknutí sekcie *Settings* sa objaví zoznam premenných, ktorých hodnoty možno zmeniť. Zmeny sa ukladajú stlačením tlačidla *Save*.

4.5 Pomocné skripty

V rámci realizácie navrhnutého riešenia som tiež vytvoril sadu skriptov, ktoré umožňujú jeho jednoduchú inštaláciu a konfiguráciu vytváranej Wi-Fi siete. Jedná sa o bash skripty, ktoré sú určené pre spúšťanie na zariadení, ktoré je určené na spúšťanie finálneho riešenia. V tejto časti práce popisujem implementáciu týchto skriptov a ich použitie.

4.5.1 Inštalačný skript

Skript `install.sh` umožňuje jednoduchú inštaláciu celého finálneho riešenia. Postupne nainštaluje všetky knižnice potrebné pre jeho správne fungovanie. Taktiež automaticky aplikuje sieťové nastavenia pre správne fungovanie vytváranej bezdrôtovej Wi-Fi siete. Skript od užívateľa následne vyžiada názov vytváranej Wi-Fi siete a heslo pre jej zabezpečenie. Na záver nastaví automatické spúšťanie užívateľskej aplikácie. Pre správne fungovanie je nevyhnutný reštart zariadenia, na ktorom je riešenie inštalované. Túto skutočnosť skript oznámi a po krátkom časovom intervale zariadenie reštartuje.

4.5.2 Konfiguračný skript

Pomocou skriptu `configure-wifi.sh` môže užívateľ jednoducho zmeniť konfiguráciu vytváranej Wi-Fi siete. Po jeho spustení vyzve skript užívateľa o zadanie nového názvu a následne hesla pre zabezpečenie siete. Samozrejmosťou je aj zachovanie pôvodných hodnôt. Po potvrdení zmien skript upraví konfiguračný súbor softvérového démona hostapd a po krátkom časovom intervale prebehne jeho reštart, čím sa zmeny konfigurácie aplikujú.

Kapitola 5

Testovanie

V poslednej kapitole tejto práce popisujem proces testovania implementovaného riešenia. Postupne dokumentujem testovacie prostredie, v ktorom testovanie prebiehalo, aj jeho samotný proces.

5.1 Testovacie prostredie

Pre testovanie som použil minipočítač Raspberry Pi 3B+. K minipočítaču bolo pripojené softvérovo definované rádio RTL-SDR V3 pomocou USB. V priebehu testovania som použil oba typy antén, ktorých fungovanie som opisoval v analytickej časti tejto práce.

Ako operačný systém som pre účely testovania zvolil oficiálny operačný systém pre platformu Raspberry Pi, ktorý sa nazýva *Raspberry Pi OS* a je nadstavbou operačného systému *Debian*. Keďže sa jedná o oficiálny operačný systém pre platformu RPi, považujem správne fungovanie konečného riešenia na tomto operačnom systéme za veľmi dôležité.

Pred začatím testovania som nainštaloval čistú kópiu operačného systému. Jediné úpravy, ktoré na operačnom systéme pred začiatkom testovania prebehli, boli aktualizácia celého systému pomocou príkazov `apt update` a `apt upgrade` a nakopírovanie zdrojových kódov finálneho riešenia.

5.2 Inštalácia

Ako prvý test som vybral test inštalačného skriptu `install.sh` popísaného v predchádzajúcej kapitole. Po spustení tohto skriptu s najvyššími právami (`sudo bash install.sh`) skript správne nainštaloval a nastavil všetky dôležité komponenty. Následne vyzval na zadanie informácií pre konfiguráciu bezdrôtovej Wi-Fi siete. Nasledovalo aplikovanie tejto konfigurácie a nastavenie automatického spúšťania užívateľskej aplikácie.

Finálne riešenie spolu so softvérovým démonom hostapd sa po dokončení behu inštalačného skriptu a reštartu zariadenia automaticky spustili. Na mobilnom zariadení sa v zozname dostupných Wi-Fi sietí objavila bezdrôtová sieť s názvom zadaným v priebehu inštalácie.

5.3 Pripojenie k bezdrôtovej sieti

Druhým testom bolo pripojenie ku vytvorenej bezdrôtovej sieti. Po zvolení tejto siete na mobilnom zariadení sa správne zobrazila požiadavka na zadanie hesla. Po zadaní rovnakého hesla ako bolo heslo zadané počas inštalácie sa zariadenie k bezdrôtovej sieti úspešne pripojilo. Spustenie príkazu `ping 192.168.1.1` potvrdilo pripojenie zariadenia k rovnakej sieti ako je pripojený minipočítač Raspberry Pi, na ktorom bolo riešenie spustené.

5.4 Zmena konfigurácie bezdrôtovej siete

Ako tretí test som vybral zmenu konfigurácie bezdrôtovej siete. Po spustení skriptu `configure-wifi.sh`, popisovaného v predchádzajúcej časti práce, si skript správne vyžiadal názov a heslo bezdrôtovej siete. Následne skript správne oznámil nutnosť odpojenia užívateľského zariadenia zo siete z dôvodu reštartu softvérového démona hostapd. Tak sa aj udialo, pričom opätovné pripojenie nenastalo.

Pokus o opätovné pripojenie k vytvorenej Wi-Fi sieti s pôvodným heslom (ktoré bolo zadané pri inštalácii) skončil neúspešne, čím sa potvrdila zmena hesla. Po zadaní nového hesla (ktoré bolo zadané na začiatku tohto testu) sa zariadenie úspešne pripojilo. Opätovný pokus s príkazom `ping` potvrdil pripojenie k správnej sieti.

5.5 Dosiahnuteľnosť webovej aplikácie

Nasledujúcim testom bola dosiahnuteľnosť samotnej webovej aplikácie. Po opätovnom pripojení k bezdrôtovej sieti a zadaní IP adresy `192.168.1.1` do webového prehliadača sa webová aplikácia úspešne načítala. Všetky komponenty webovej aplikácie boli funkčné.

5.6 Zachytávanie komunikácie

Na začiatok testovania webovej aplikácie som zvolil test zachytávania komunikácie. Po zadaní časového intervalu do kolónky na hlavnej stránke a stlačení tlačidla *Capture* mi webová aplikácia správne oznámila začatie zachytávania komunikácie. Po ubehnutí časového intervalu webová aplikácia oznámila úspešné ukončenie zachytávania. Na hlavnej stránke sa správne zvýšilo

počítadlo *Raw NFC Records*, pričom sa objavili tlačidlá pre spustenie analýzy a vyčistenie nezanalyzovaných vzoriek.

5.7 Analýza komunikácie

Po zachytení komunikácie som sa rozhodol v rámci ďalšieho testu otestovať funkčnosť analýzy komunikácie. Po stlačení tlačidla *Analyze* webová aplikácia oznámila začatie analýzy. Po krátkom časovom intervale webová aplikácia oznámila úspešný koniec analýzy. Na hlavnej stránke sa počítadlo *Raw NFC Records* správne vynulovalo a počítadlo *Analyzed NFC Records* správne zvýšilo o 1. Zároveň sa objavilo tlačidlo *Summary*.

5.8 Analýza viacero zachytených vzoriek

Po analýze jednej komunikácie som otestoval funkčnosť s väčším počtom vzoriek. Po zachytení väčšieho počtu vzoriek som pomocou tlačidla *Analyze* spustil ich analýzu. Webová aplikácia oznámila úspešné ukončenie analýzy, pričom sa počítadlá na hlavnej stránke správne upravili. Na stránke s výsledkami analýz sa vytvoril správny počet nových výsledkov, čím sa potvrdilo správne fungovanie webovej aplikácie aj s väčším počtom vzoriek.

5.9 Nepripojené SDR

Ďalším testom bol pokus o zachytávanie komunikácie bez pripojeného SDR k minipočítaču Raspberry Pi. Po fyzickom odpojení RTL-SDR od RPi som znova zadal časový interval do kolónky a stlačil tlačidlo *Capture*. Webová aplikácia vypísala chybu, avšak neprestala fungovať. Po opätovnom načítaní hlavnej stránky boli všetky komponenty funkčné.

5.10 Zmena nastavení SDR

Po opätovnom pripojení RTL-SDR k RPi nastal test zmeny nastavení SDR. Na hlavnej stránke som po rozkliknutí sekcie *Settings* zmenil parameter *Center Frequency* a vypol analýzu signálu pasívnych zariadení. Webová aplikácia po stlačení tlačidla *Save* správne ohlásila úspešné uloženie nastavení.

Následne som zachytil malý časový interval komunikácie, počas ktorej nastala interakcia NFC karty s NFC čítačkou. Po stlačení tlačidla *Analyze* úspešne prebehla analýza. Analýza správne obsahovala len rámce vysielané čítačkou, čím sa potvrdila funkčnosť zmeny nastavení SDR na hlavnej stránke.

5.11 Nesprávne zadané hodnoty

V rámci ďalšieho testu som postupne otestoval všetky kolónky na hlavnej stránke zadaním nesprávnych alebo žiadnych hodnôt. Aplikácia správne oznámila chybu po potvrdení zadaných hodnôt a žiadnu z týchto hodnôt neuložila, čím bolo potvrdené jej správne fungovanie.

5.12 Rôzna doba zachytávania komunikácie

Ako ďalší test som sa rozhodol otestovať fungovanie zachytávania komunikácie vo webovej aplikácii. Opakovane som zachytil rôzne časové intervaly a následne spustil ich analýzu. Po úspešnej analýze som prezretím NFC rámcov zistil rôzny počet NFC rámcov, čím sa potvrdilo správne fungovanie.

5.13 Vyčistenie nezanalyzovaných vzoriek

V rámci nasledujúceho testu som zachytil niekoľko vzoriek. Po stlačení tlačidla *Clear* sa správne vynulovalo počítadlo *Raw NFC Records*, čím sa potvrdila správna funkčnosť daného tlačidla.

5.14 Stiahnutie analýzy

Ďalším testom bolo stiahnutie dokončenej analýzy. Po stlačení tlačidla *Download* sa správne stiahol archív. Archív správne obsahoval 3 súbory, popisované v predošlej kapitole práce. Najväčšie 2 súbory obsahovali pôvodné a digitalizované vzorky, tretí obsahoval výsledky analýzy. Porovnaním stiahnutých dát s dátami zobrazenými vo webovej aplikácií sa potvrdilo správne fungovanie.

5.15 Vymazanie výsledkov analýzy

Nasledujúcim testom bolo vymazanie analýzy komunikácie. Po stlačení *Delete* webová aplikácia správne oznámila jej vymazanie. Počet výsledkov sa znížil o jedna. Pri pokuse o stiahnutie výsledku analýzy na rovnakej pozícii ako bol vymazaný výsledok sa stiahol nový archív, čím sa potvrdilo aj zmazanie príslušného archívu.

5.16 Duplikovanie analyzovaných vzoriek

Ako posledný test som zvolil test tlačidla *Duplicate* na stránke s výsledkami analýz. Po jeho stlačení webová aplikácia správne oznámila úspešnú duplikáciu. Na hlavnej stránke sa správne zvýšilo počítadlo *Raw NFC Records*.

Po opätovnej analýze sa potvrdilo správne fungovanie tohto tlačidla. Analýza bola rovnaká ako pôvodná, z ktorej boli vzorky duplikované.

Záver

Cieľom práce bolo navrhnúť a implementovať prenosné riešenie pre odpočúvanie NFC pomocou softvérovo definovaného rádia. Pred samotným návrhom bola nutná analýza existujúcich riešení, technológie SDR, technológie NFC a jej možných bezpečnostných zraniteľností, ktoré by mohli byť odpočúvaním zneužité.

Analýzou existujúcich riešení som zistil, že neexistuje žiadne riešenie, ktoré by na odpočúvanie komunikácie pomocou NFC využívalo softvérovo definované rádio. Taktiež som zistil, že takéto riešenie by bolo prístupnejšie vďaka viacúčelovosti softvérovo definovaného rádia. Následnou analýzou technológie NFC som zistil princíp komunikácie medzi zariadeniami. Taktiež som zistil, že počas nadväzovania komunikácie medzi NFC sa prenášajú medzi zariadeniami informácie, ktoré by mohli byť po ich zachytení zneužité. Ďalšou analýzou som dospel k možnému spôsobu, ktorým sa dá technológia NFC odpočúvať. Zo získaných informácií som vytvoril návrh riešenia, ktoré využíva softvérovo definované rádio na odpočúvanie takejto komunikácie.

Výsledkom je prenosné zariadenie, ktoré umožňuje pomocou softvérovo definovaného rádia RTL-SDR odpočúvať, zachytávať a analyzovať NFC. Riešenie je implementované s dôrazom na použitie s platformou Raspberry Pi. Súčasťou je užívateľská aplikácia v podobe webovej aplikácie, ku ktorej užívateľ pristupuje po pripojení k bezdrôtovej Wi-Fi sieti vytváranej zariadením, na ktorom je aplikácia spúšťaná. Celú implementáciu som zdokumentoval a následne riadne otestoval, čím som dokázal jej správne fungovanie.

Výsledné riešenie je možné ešte vylepšiť. V rámci práce som zistil, že zachytávať signál vysielaný pasívnymi zariadeniami (NFC karty, tagy, atď.) môže byť veľmi zložité. Medzi možné vylepšenia radím ďalšie preskúmanie a implementáciu spôsobov, ktorými by sa signál dokázal zachytávať a analyzovať spoľahlivejšie. Zaujímavé by bolo aj rozšírenie funkcionality webovej časti užívateľskej aplikácie.

Literatúra

[1] Proxmark: *Introduction to the Proxmark Platform* [online]. [cit. 2023-02-07]. Dostupné z: `https://proxmark.com/` https://github.com/RfidResearchGroup/proxmark3

[2] RFID Research Group: *Proxmark3 a RFID / NFC project* [online]. [cit. 2023-02-07]. Dostupné z: `https://github.com/RfidResearchGroup/proxmark3/`

[3] HydraBus: *HydraNFC Shield v1.0 Specifications* [online]. [cit. 2023-02-07]. Dostupné z: `https://hydrabus.com/hydranfc-1-0-specifications/?v=928568b84963`

[4] HydraBus: *HydraNFC Shield v1 and HydraNFC Antenna* [online]. [cit. 2023-02-07]. Dostupné z: `https://github.com/hydrabus/hydranfc/`

[5] LAB401: *HydraNFC* [online]. [cit. 2023-02-07]. Dostupné z: `https://lab401.com/products/hydranfc`

[6] LAB401: *HydraBus* [online]. [cit. 2023-02-07]. Dostupné z: `https://lab401.com/products/hydrabus`

[7] PERSON Chris: *The ChameleonMini is a skeleton key for RFID* [online]. [cit. 2023-02-07]. Dostupné z: `https://www.theverge.com/23411372/chameleon-mini-rfid-nfc-attack-proxmark3-keyless-card-reader`

[8] Kasper & Oswald: *ChameleonMini* [online]. [cit. 2023-02-07]. Dostupné z: `https://kasper-oswald.de/gb/chameleonmini/`

[9] Chair for Embedded Security: *Chameleon-Mini* [online]. [cit. 2023-02-07]. Dostupné z: `https://github.com/emsec/ChameleonMini`

[10] Teledyne LeCroy: *ComProbe® NFC Protocol Analyzer: NFC-A, NFC-B and NFC-F* [online]. [cit. 2023-02-07]. Dostupné z: https://fte.com/products/nfc.aspx

[11] RTL-SDR: *About RTL-SDR* [online]. [cit. 2023-02-07]. Dostupné z: https://www.rtl-sdr.com/about-rtl-sdr/

[12] VICES Per: *What is a Software Defined Radio?* [online]. [cit. 2023-02-07]. Dostupné z: https://www.everythingrf.com/community/what-is-a-software-defined-radio

[13] VENKATESAN Adithya: *How Things Work: NFC can be active or passive* [online]. [cit. 2023-02-09]. Dostupné z: http://thetartan.org/2014/9/15/scitech/howthingswork

[14] RF Wireless World: *How NFC works* [online]. [cit. 2023-02-09]. Dostupné z: https://www.rfwireless-world.com/Tutorials/NFC-Near-Field-Communication-tutorial.html

[15] MINIHOLD Roland: *Near Field Communication (NFC) Technology and Measurements* [online]. [cit. 2023-02-09]. Dostupné z: https://scdn.rohde-schwarz.com/ur/pws/dl_downloads/dl_application/application_notes/1ma182/1MA182_5E_NFC_WHITE_PAPER.pdf

[16] Electronics Notes: *NFC Physical Layer: modulation & RF signal* [online]. [cit. 2023-04-02]. Dostupné z: https://www.electronics-notes.com/articles/connectivity/nfc-near-field-communication/physical-layer-rf-signal-modulation.php

[17] PARIKH Shreya: *Security of NFC* [online]. [cit. 2023-03-31]. Dostupné z: https://www.ijert.org/research/security-of-nfc-IJERTCONV5IS01039.pdf

[18] ISO/IEC14443-3: *Initialization and anticollision* [online]. [cit. 2023-04-02]. Dostupné z: http://www.emutag.com/iso/14443-3.pdf

[19] RF Wireless World: *NFC A vs NFC B vs NFC F-Difference between NFC-A,NFC-B,NFC-F* [online]. [cit. 2023-04-02]. Dostupné z: https://www.rfwireless-world.com/Terminology/NFC-A-vs-NFC-B-vs-NFC-F.html

[20] POUNDER Les: *How to Turn a Raspberry Pi Into a Wi-Fi Access Point* [online]. [cit. 2023-04-14]. Dostupné z: https://www.tomshardware.com/how-to/raspberry-pi-access-point

[21] KUISMA Mikael: *I/Q Data for Dummies* [online]. [cit. 2023-04-15]. Dostupné z: http://whiteboard.ping.se/SDR/IQ

Dodatok A

Zoznam použitých skratiek

NFC Near Field Communication

SDR Softvérovo definované rádio

ASK Amplitude-shift keying

UID Universal Identificator

MAC Media Access Control

LSB Least significant bit

MSB Most significant bit

RPi Raspberry Pi

RFID Radio Frequency Identification

USB Universal Serial Bus

Dodatok B

Obsah priloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `src`
  - `impl` ..... zdrojové kódy implementácie
  - `thesis` ..... zdrojová forma práce vo formáte LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce vo formáte PDF
  - `thesis.ps` ..... text práce vo formáte PS