SOFTWARE DEFINED RADIO FOR SIGFOX TECHNOLOGY

Jakub Přibyl
Master Degree Programme (2), FEEC BUT
E-mail: xpriby14@stud.feec.vutbr.cz

Supervised by: Radek Fujdiak
E-mail: fujdiak@feec.vutbr.cz

Abstract: This article deals with LPWAN technology Sigfox and its radio communication between end device and base station. The goal is to use SDR device to capture uplink frame sent by end device, demodulate and decode this frame. This is done with use of DVB-T tuner NooElec NESDR Mini 2 and CubicSDR and renard-phy software.

Keywords: LPWAN, SDR, Sigfox

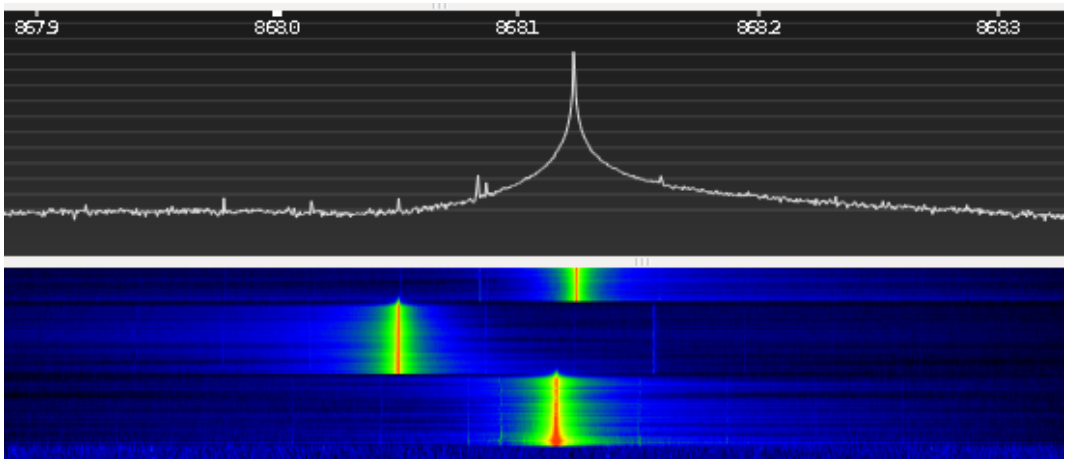
1 ÚVOD

Internet věcí je velmi aktuální a stále se rozvíjející odvětví, které se zabývá přenosem dat pomocí bezdrátových technologií. Jednotlivé technologie se pak odlišují podle dosahu, množství přenesených dat a rychlostí. Cílem IoT je propojit zařízení, které jsou schopny usnadnit lidem život a lidé je budou schopny ovládat [1]. Tato práce je především zaměřená na technologii LPWAN (Nízkoenergetické sítě na velkou vzdálenost) a konkrétně na úzkopásmovou technologii Sigfox. Důvodem vybrání technologie je to, že je nešifrovaná a její komunikace probíhá nad šumem [2]. Díky tomu je zachycení přenosu možné realizovat jen pomocí DVB tuneru a vhodně zvoleného SW.

Cílem práce je prozkoumat možnosti softwarově definovaného rádia Sigfox, provést demodulaci a dekódování posílaných zpráv. Výsledkem práce je vybrání vhodného HW i SW pro zachytávání, zprovoznění komunikace mezi zařízením a Sigfox sítí, zachycení rádiové komunikace a dekódování zachycené zprávy. Ta je porovnána se zprávou, která je poslána do cloudu.

2 TECHNOLOGIE SIGFOX

Sigfox je proprietární LPWAN technologie vyvinuta francouzskou společnosti Sigfox S.A. v Toulouse. Zaměřuje se především na poskytování levné konektivity na velké vzdálenosti s omezenou velikostí přenášených dat. Funguje v nelicencovaných ISM pásmech pod 1 GHz, konkrétně v 868 MHz pro Evropu. Výhodou 868 MHz pásma je minimální rušení, ale také podléhá regulacím, co se týče posílání zpráv. Je tedy možné poslat maximálně 140 uplink zpráv o velikosti 12 B a pro downlink 4 zprávy o velikosti 8 B. Přenos uplink zpráv je omezen na 100 b/s a využívá DBPSK klíčování. Přenos downlink zprávy má rychlost 600 b/s a využívá GFSK klíčování. Jednou z největších výhod technologie je velká životnost baterie a pokrytí obrovských vzdáleností. Přenos není šifrován, jelikož je šifrování více energeticky náročné. Sigfox tímto způsobem nabízí možnost každé firmě implementovat svoje šifrování. Bezpečnost mezi základnovými stanicemi a Sigfox cloudem je zajištěna pomocí VPN připojení a autentizačních klíčů [2]. Každé zařízení má svoje unikátní ID, které se přenáší v každé zprávě. Kromě ID je během výroby přiřazen také symetrický autentizační klíč a PAC, který slouží k registraci zařízení např. do cloudu. Aby se předešlo replay útoku, je ve zprávách přiřazeno sekvenční číslo (SEQ). Jedná se o jednoduchý čítač, který se zvýší o 1, pokud je zpráva poslána do cloudu [3].



Obrázek 1: Zachycená komunikace všech tří rámců uplink zprávy technologie Sigfox.

Rámce jsou posílány celkem tři v krátkém časovém rozmezí (viz obr. 1). Všechny tři rámce nesou stejnou zprávu na jiných frekvencích v rozmezí 868,034 MHz až 868,226 MHz a v jiném čase. Díky tomu je snížena šance kolizí a větší šance na doručení zprávy. Přenos je nesynchronizovaný a nedochází k žádné výměně synchronizačních rámců. Maximální velikost rámce je velikosti 26 B. V rámci je zahrnuta preambule, synchronizační rámec (typ přenášeného rámce), ID zařízení, samotná data (payload), autentikační část a FCS, který slouží pro detekci chyb. Velikost jednotlivých částí rámce lze vidět v tab. 1 [4].

4 B	**2 B**	**4 B**	**0 až 12 B**	**různé**	**2 B**
Preambule	Synchr. rámec	ID koncového zařízení	Data	Autent.	FCS

Tabulka 1: Složení uplink rámce.

3 REALIZACE ZACHYTÁVÁNÍ

Pro realizování zachytávání posílání od koncového zařízení je potřeba vybrat vhodný HW i SW. V rámci HW je potřeba vybrat koncové zařízení a zařízení, přes které je možné realizovat zachytávání. SW část zahrnuje program pro zachytávání a program pro demodulaci a dekódování rámce. Dále je zpráva dekódována a porovnána se zprávou v cloudu.

3.1 VÝBĚR HW A SW

Jako koncové zařízení byl vybrán Sigfox Sens'it 2.1, který byl poskytnut školou. Jelikož koncové zařízení musí být schváleno sítí Sigfox, je zařízení nejlepší volbou skrz dostupnost. Slouží primárně k demonstrování možností sítě Sigfox a slouží k vývoji. Senzor je určen k měření teploty, detekce otevření dveří apod. Data lze poté zobrazit v Sigfox cloudu. Zařízení vysílá ve frekvenčním pásmu 868 MHz. Pro zachytávání byl vybrán DVB-T NooElec NESDR Mini 2 tuner upravený pro SDR. Tuner má v sobě čip R820T2, který je pro zachytávání v těchto frekvencích jedním z nejlevnějších, ale zároveň nejčastěji používaným. Zařízení je schopné zachytávat frekvence v rozmezí 25 MHz až 1700 MHz. Zobrazovací okno má velikost 3,2 MHz v reálném čase, což je dostačující pro zobrazení celého spektra v pásmu 868 MHz. Airspy mini používá stejný čip, ale díky dalším komponentům má o něco větší zobrazovací okno. Cena je však mnohem vyšší než u NESDR Mini 2 a proto je

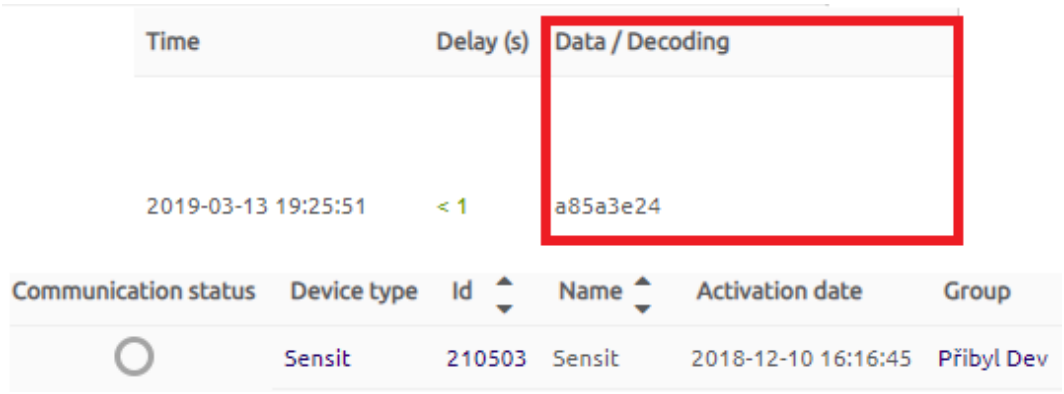
vhodnější pro tyto účely právě NESDR Mini 2. Pokud by bylo vyžadováno vysílání, je nutné si vybrat alternativu v podobě např. LimeSDR mini nebo HackRF. Ty mají zároveň mnohem větší zobrazovací okno a používají jiné čipy. Cílem této práce však není vysílání, proto je použit NESDR Mini 2. Všechny parametry porovnaných zařízení jsou možné vidět v tabulce 2. Software pro zachytávání byl zvolen CubicSDR, který je schopen ukládat zachytávání v souborech .wav, což je poté možné využít v programu, který je využit pro demodulaci a dekódování renard-phy. Oba programy pracují na virtuálním stroji s OS Linux, konkrétně verze Ubuntu 18.04.2 LTS.

	NESDR Mini 2 [5]	**Airspy mini [6]**	**LimeSDR mini [7]**	**HackRF [7]**
Frekvence	25 - 1700 MHz	24 - 1700 MHz	10 MHz - 3,5 GHz	1 MHz - 6 GHz
RF frekvence	3,2 MHz	6 MHz	30,72 MHz	20 MHz
TX výkon	N/A	N/A	až 10 dBm	až 15 dBm
Použité čipy	R820T2	R820T2	LMS7002M	RFFC5071
Vysílač	Ne	Ne	Full-duplex	Half-duplex
Cena	21 dolarů	100 dolarů	159 dolarů	300 dolarů

Tabulka 2: Porovnání zařízení pro zachytávání.

3.2 Zachycení a dekódování rámce

Rámce byly zachyceny pomocí NESDR Mini 2 v programu CubicSDR (viz obr. 1). Přenos je nutné zachytit jako I/Q signál, aby bylo možné využít program renard-phy pro demodulaci a dekódování. I/Q signál je označován jako signál, jehož okamžitá hodnota signálu lze vyjádřit komplexním číslem v daný okamžik. I a Q zastupují reálnou a imaginární část (in-phase a quadrature). IQ signál je tvořen dvěmi sinusoidami o stejné frekvenci, které mají oproti sobě fázový posuv 90 stupňů. V této realizaci je CubicSDR schopen zachytávat I/Q signál a uložit jej jako soubor s koncovkou .wav jen pro šířku pásma 48 kHz, což má za následek, že při přenosu je ve většině případů zachycen pouze jeden rámec.



Obrázek 2: Zpráva v Sigfox cloudu.

Z cloudu (viz obr. 2) je možné vidět, že byla obdržena zpráva a85a3e24 na zařízení, které má ID 210503. Ve zprávě jsou obsaženy údaje o módu (tlačítko, časový rámec), časovém rámci, typu (tlačítko, měření teploty, senzor dveří apod.) a stavu baterie. Z této zprávy lze zjistit, že se jedná o stisknutí tlačítka a stav baterie je 4 V. Po uložení souboru se zachyceným rámcem je potřeba rámec dekódovat. Je využit program renard-phy, ze kterého lze zjistit údaje z obr. 3. Renard-phy je schopen zobrazit kromě samotného payloadu a ID zařízení také vyčíst sekvenční číslo, ktere vidět v cloudu nelze. V cloudu také nelze vidět zpráva pouze po demodulaci před provedením samotného dekódování.

```
[Frame 0]: Content: 59805db4246f9c0d661aebf80924c79
[Frame 0]: Decoding with renard:
Downlink request: no
Sequence Number : 7cf
Device ID       : 00210503
Payload         : a85a3e24
CRC             : OK
MAC             : didn't perform check, provide secret key to check MAC
```

Obrázek 3: Výstup programu renard-phy.

4 ZÁVĚR

Cílem této práce bylo zachytnout, demodulovat a dekódovat Sigfox zprávu, která byla poslána z koncového zařízení. To bylo dosaženo pomocí vybraného zařízení NooElec NESDR Mini 2 a vybráním vhodného softwaru CubicSDR a renard-phy. Práce bude dále pokračovat se zaměřením na zachycení všech tří rámců a jejich dekódování. Dále se bude testovat zachycení downlink rámce a zachycení registrace zařízení do sítě.

REFERENCE

[1] HANES, D.; SALGUEIRO, G.; GROSSETETE, P.;BARTON, R.; HENRY, J. *IoT fundamentals: networking technologies, protocols, and use cases for the Internet of things.* Indianapolis, IN: Cisco press, 2017, xxxi, 543 pages, ISBN 978-1-58714-456-1.

[2] Sigfox. *Sigfox technology overview* [online]. Dostupné z: <https://www.sigfox.com/en/sigfox-iot-technology-overview>

[3] Sigfox *Sigfox Secure Sigfox Ready devices* [online]. Dostupné z: <http://www.aerea.nl/wp-content/uploads/2018/06/Secure-Sigfox-Ready-devices-recommendation-guide-II.pdf>

[4] POOLE, I.; *SigFox for M2M & IoT.* Electronics notes [online]. Dostupné z: <https://www.electronics-notes.com/articles/connectivity/sigfox/what-is-sigfox-basics-m2m-iot.php)

[5] Nooelec *NESDR series product page* [online]. Dostupné z: <https://support.nooelec.com/hc/en-us/articles/360005805834-NESDR-Series>

[6] Airspy *Airspy Mini – The Ultimate Performance in a Dongle Form Factor* [online]. Dostupné z: <https://airspy.com/airspy-mini/>

[7] Crowd Supply *LimeSDR Mini by Lime Microsystems.* [online]. Dostupné z: <https://www.crowdsupply.com/lime-micro/limesdr-mini>

[8] Great Scott Gadgets *HackRF One* Dostupné z: <https://greatscottgadgets.com/hackrf/one/>

[9] SLÁDEK, O. *Analyzátor RFID signálů jako SW radio na bázi USB DVB-T přijímače.* Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2015. 44 s.