SOFTWARE DEFINED RADIO FOR LORAWAN

Ondřej Pospíšil
Master Degree Programme (2), FEEC BUT
E-mail: xpospi89@stud.feec.vutbr.cz

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

Abstract: Paper deals with LoRaWAN communication listening with the usage of software defined radio. The main focus is on capturing unencrypted physical layer communication (LoRa). The process and requirements of capturing by GNU Radio software is described. Furthermore, an example of decryption is presented. Lastly, the requirements for capturing and deciphering of a LoRaWAN MAC layer message are described.

Keywords: LoRaWAN, LoRa, SDR, GNU Radio

1 ÚVOD

LoRaWAN (Long Range Wide Area Network) patří mezi technologie rozsáhlých sítí s nízkou spotřebou energie (Low Power Wide Area Network) [1]. Tyto technologie jsou nyní hojně využívány v rámci senzorických měření v IoT (Internet of Things) [2]. LoRaWAN se skládá z fyzické vrstvy na které neprobíhá šifrovaný provoz a z vrstvy MAC, která definuje šifrovaný provoz protokolu LoRaWAN [3]. Tento článek se zaměřuje na tvorbu SDR (softwarově definovaného radia) pro fyzickou vrstvu LoRa (Long Range), zachycení paketu a dekódování na této vrstvě. Zachycení je realizováno pomocí softwarově definovaného radia a to především pomocí softwaru GNU Radio.

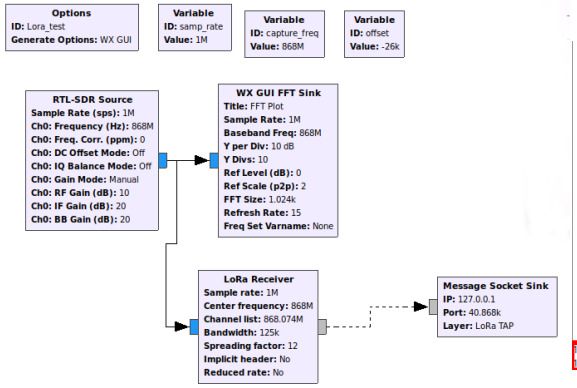
2 ODPOSLECH PŘENOSU

V rámci práce byl zachytáván přenos fyzické vrstvy LoRa. Pro testování byla vytvořena vlastní infrastruktura pro síť LoRaWAN. Byla zkonstruována vlastní brána na desce ic880a [4], pro vysílání bylo použito zařízení The Things UNO a byl vytvořen i experimentální síťový server na open source řešení LoRa server [5]. Vysílání bylo zachytáváno pomocí zařízení RTL-SDR a LimeSDR mini. K zachycení a dekódování byl použit software GNU Radio.

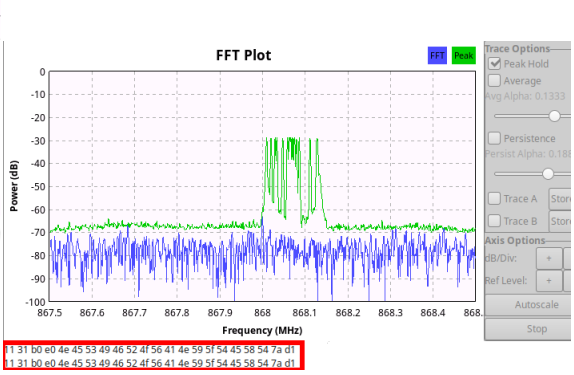
V GNU Radiu byly sestaveny bloky pro zachycení komunikace fyzické vrstvy LoRa, sestavení jednotlivých bloků lze vidět na obrázku 1. Nejdříve byl použit blok RTL-SDR, který slouží jako zdroj signálu zařízení RTL-SDR, blok umožňuje převést signál ze zařízení do GNU Radia. Tento blok byl propojen se dvěma dalšími bloky WX GUI FFT Sink a LoRa Rceiver. První jmenovaný blok se chová jako spektrální analyzér, který aplikuje krátkodobou Fourrierovu transformaci. V tomto bloku byla nastavena vzorkovací frekvence na 1 MHz a frekvence základního pásma na 868 MHz. Jedná se o blok, který zprostředkovává grafické rozhraní. Druhý blok umožňuje příjem a dekódování LoRa signálu, tento blok pochází z knihovny gr-lora od autora rpp0 [6]. Blok byl nastaven pro zachytávání a dekódování na frekvenci 868,100 MHz spreading factor byl zvolen na hodnotě 12. Posledním blokem je Message Socket Sink tento blok vytvoří zprávu z příchozích dat a posílá je na adresu 127.0.0.1 (loopback) a díky tomu je poté možné zachytit zprávu pomocí Wiresharku.

Na obrázku 2 lze vidět zachycení vysílání LoRa pomocí bloku WX GUI FFT Sink, který je grafickým rozhraním pro zachycení signálu v GNU Radiu. Na obrázku je také zobrazen výpis z konzole GNU Radia, který obsahuje dekódovanou zprávu pomocí bloku LoRa Receiver.

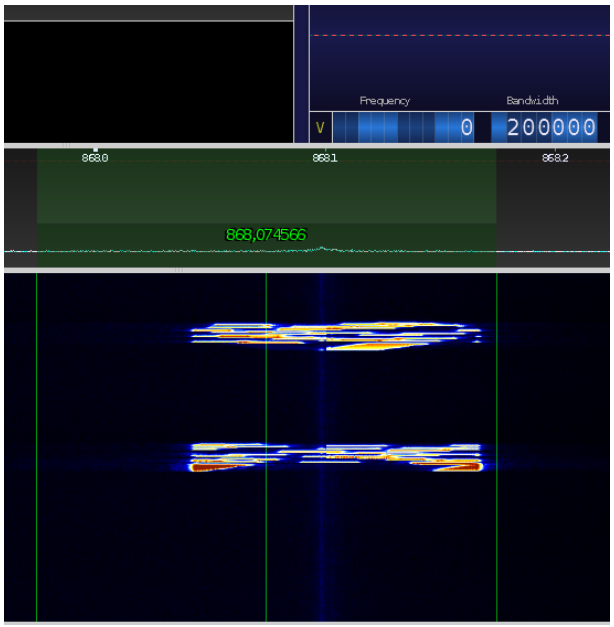
Na obrázku 3 lze vidět zachycení signálu LoRa v rámci softwaru CubicSDR kde lze vidět rozprostření modulace LoRa založené na modulaci Chirp Spread Spectrum při nastavení zařízení na Spreading Factor 12, šířka pásma při vysílání byla nastavena na 125 kHz.



Obrázek 1: Bloky v GNU Radiu pro zachycení komunikace LoRa.



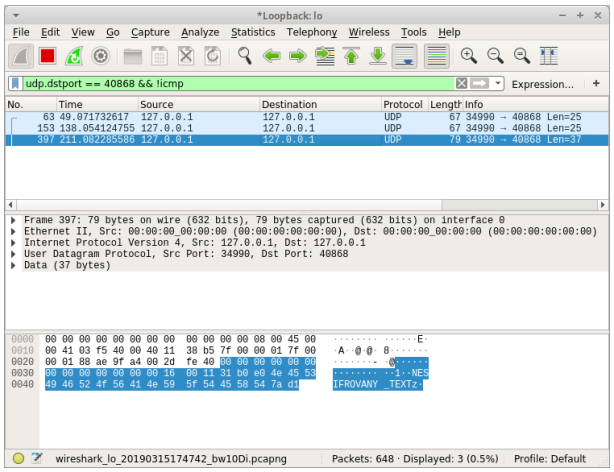
Obrázek 2: Ukázka zachycení v grafickém rozhraní GNU Radia a výpis z konzole GNU Radia.



Obrázek 3: Zachycení signálu LoRa pomocí softwaru CubicSDR.

3 DEKÓDOVÁNÍ FYZICKÉ VRSTVY

Po zachycení signálu byl text dekódován pomocí Wiresharku, jak lze vidět na obrázku 4. Pokud je signál vysílán pouze pomocí modulace LoRa a není do vysílání začleněna vyšší MAC vrstva tak jsou data posílána nešifrovaně, pouze v hexadecimálním tvaru. Na obrázku 5 lze vidět popis paketu při vysílání pomocí modulace LoRa. Paket byl zachycen pomocí GNU Radia a pomocí bloku LoRa Receiver byl obsah dekódován na hexadecimální posloupnost. Na obrázku lze vidět rozdělení podle bajtů a ukázku nezašifrovaného přenosu. Zachycena byla tato hexadecimální posloupnost: 11 31 b0 e0 4e 45 53 49 46 52 4f 56 41 4e 59 5f 54 45 58 54 7a d1.



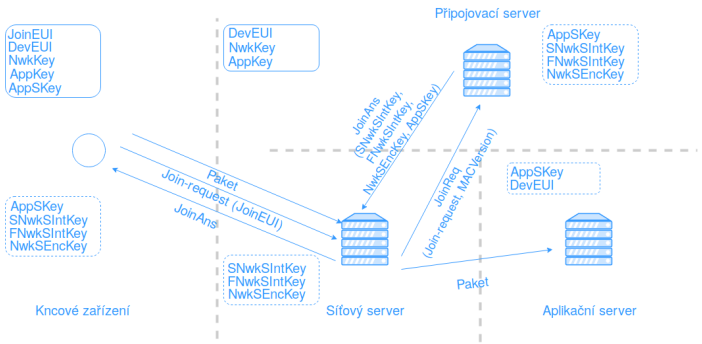
Obrázek 4: Zachycení zprávy v programu Wireshark.

Obrázek 5: Rozdělení zachycené zprávy v rámci formátu LoRa vrstvy.

4 NÁVRH PRO MAC VRSTVU LORAWAN

Pro dekódování protokolu LoRaWAN je nutné mít k dispozici klíče jako NwkKey a AppKey a také relační klíče z těchto klíčů odvozené. Pomocí reverzního inženýrství je třeba zjistit jak jsou klíče šifrovány a jak toto šifrování prolomit. Klíče jsou šifrovány pomocí AES-128 zahrnující metody AES128 Cipher-based Message Authentication Code (CMAC), AES128 Counter with CBC-MAC (CCM), AES128 Electronic Codebook (ECB). Je tedy nutné zachytit jednotlivé klíče a pokusit se prolomit šifrování na MAC vrstvě.

Na obrázku 6 lze vidět uložené informace (klíče a identifikátory) na jednotlivých prvcích sítě LoRaWAN 1.1 a také zprávy, které jsou přenášeny při registraci zařízení pomocí OTAA (Over-the-Air Activation) do sítě a informace (především klíče), které tyto zprávy nesou. Na každém zařízení při této registraci musí být uloženy klíče NwkKey a AppKey z těchto klíčů jsou poté postupně odvozeny další klíče.



Obrázek 6: Přenos informací při aktivaci pomocí OTAA.

5 ZÁVĚR

Článek se zabýval zachytáváním a dekódováním signálu vysílaného pomocí modulace LoRa, která pracuje jako fyzická vrstva u protokolu LoRaWAN. Zachycení a dekódování bylo realizováno pomocí GNU Radia ve kterém byli vytvořeny bloky pro toto odchycení. Dále byl pro dekódování použit program Wireshark. Byla zachycena zpráva vyslaná na frekvenci 868,100 MHz tato zpráva byla dekódována a jde tedy vidět, že komunikaci na fyzické vrstvě lze odposlouchávat.

Dále by měla být do toho procesu zapojena i vyšší MAC vrstva protokolu LoRaWAN, aby jej bylo možno dešifrovat je potřeba použít klíče, které jsou tajné a jsou taktéž přenášeny šifrovaně.

REFERENCE

[1] *LoRa Aliance*[online]. Fermont: LoRa Alliance™ [cit. 2019-03-14]. Dostupné z: https://lora-alliance.org/

[2] Mekki, K.; Bajic, E.; Chaxel, F.: *Comparative study of LPWAN techno-logies for large-scale IoT deployment.* ICT Express, 2018.

[3] *LoRaWAN™ Specification v1.1* [online]. Beaverton, OR 97003, USA: LoRa Alliance, 2017 [cit. 2019-03-14]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf

[4] WiMOD iC880A. In: *WiMOD iC880A DATASHEET* [online]. 47475 KAMP-LINTFORT GERMANY: IMST, 2014 [cit. 2019-03-27]. Dostupné z: https://webshop.ideetron.nl/Files/3/1000/1211/Attachments/Product/IB4c6A1J5Uh6Ej5D3i6cQ88q1P2D1404.pdf

[5] *LoRaServer* [online]. GitHub, 2016 [cit. 2019-03-27]. Dostupné z: https://www.loraserver.io

[6] Gr-lora. *GitHub* [online]. rpp0, 2016 [cit. 2019-03-27]. Dostupné z: https://github.com/rpp0/gr-lora