EFFICIENT SECURITY OF MODERN LOW-POWER WIRELESS COMMUNICATION TECHNOLOGIES

Vojtěch Blažek
Bachelor Degree Programme (3), FEEC BUT
E-mail: xblaze32@stud.feec.vutbr.cz

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

Abstract: This thesis deals with communication security in Sigfox networks. That includes studying the network's parameters and capabilities and then analysing the appropriate cryptosystems. The thesis contains a description of cryptography as such and a description of cryptosystems that could be implemented in end devices. From the selected cryptosystems, three of the most appropriate are selected based on the required properties, which are put into practice on the Arduino-based development kit and then experimental measurements are made to determine the basic features of the device.

Keywords: Internet of Things, Sigfox, Security Proposal, Encryption, One-Time Pad

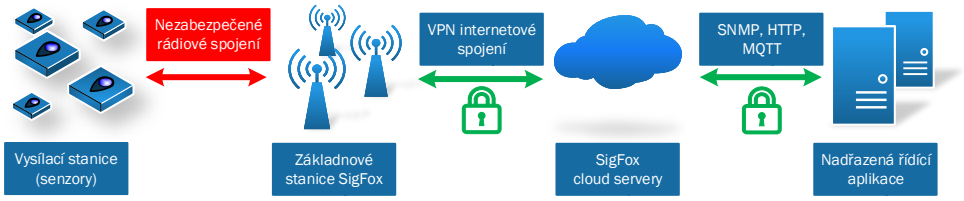
1 ÚVOD

Zabezpečování dat a chránění jejich obsahu před zneužitím je v dnešní době potřeba ve všech typech komunikací. Všechna data by měla být do jisté míry chráněna a šifrována, protože nikdy nevíte kdo a jak je chce zneužít. Tato práce je věnována návrhu zabezpečení komunikace bezdrátových nízkoenergetických moderních technologií. Především se tedy zabývá výběrem vhodných kryptografických algoritmů, implementací nejvhodnějších šifer do koncového zařízení a následným upravováním programového řešení a vývojového kitu za účelem zabezpečení zařízení proti prolomení a snížení odběru zařízení. Výsledné implementace podstoupí základní měření.

2 POPIS TECHNOLOGIE SIGFOX

Pro naše použití jsme si z možných LPWAN technologií vybrali technologii Sigfox. Sigfox je komunikační bezdrátový systém pro energeticky nenáročný přenos malého množství dat na vzdálenosti až několika kilometrů. Typickými oblastmi použití jsou odečty vody, elektřiny, plynu dále parkovací senzory, Industry 4.0, zabezpečovací zařízení atd. Sigfox je založen na topologii hvězda a pro komunikaci se používají rámce o celkové velikosti 26 bajtů, ze kterých je 0 až 12 bajtů určeno pro uživatelská data (Payload). Posílání zpráv je omezeno denně na 140 vysílacích zpráv a 4 zpětné zprávy. To vytváří omezení u použití, kde je zapotřebí odesílat data častěji [1].

SigFox používá některé mechanismy a nástroje k zabezpečení posílaných dat, ale neposkytuje bezpečnou komunikaci mezi koncovým zařízením a základnovými stanicemi (znázorněno na Obrázku 1). Data jsou dále zranitelná na Sigfox serverech, kde k nim do jisté míry mají přístup zaměstnanci Sigfox poskytovatele. Uživatelé by tedy měli vždy provádět dodatečné šifrování v rámci payloadu 12 bajtů. Teprve s využitím vlastního šifrování dat dostáváme opravdu bezpečnou end-to-end komunikaci [2].



Obrázek 1: Znázornění zabezpečení Sigfox komunikace (převzato z [2]).

3 NÁVRH ZABEZPEČENÍ

Výběr správné šifry je klíčový pro správné fungování zabezpečení na daném zařízení. Jelikož koncová zařízení Sigfox sítě by měla být co nejvíce energeticky úsporná, tak hlavním parametrem při výběru šifry je rychlost výpočtu. Při výběru vhodných šifer jsme uvažovali šifry zmíněné v Tabulce 1 a One-time pad šifru (zkráceně OTP). Tato šifra se od ostatních zmíněných šifer odlišuje tím, že používá jen operaci exkluzivního součtu XOR a díky tomu je také rychlejší než ostatní [3]. V této tabulce také naleznete hodnoty kolika hodinových cyklů procesoru je potřeba k zašifrování jednoho bajtu a k přípravě klíče společně s inicializačním vektorem (zkráceně IV).

Tabulka 1: Shrnutí výběru uvažovaných šifer (převzato z [4])

Název šifry	Počet bitů klíče	Cyklů na bajt	Cyklů na 12 bajtů	Cyklů k přípravě klíče a IV	Cyklů k přípravě a zašifrování 12 bajtů
ChaCha20	256	5,16	61,92	252	313,92
Salsa20	256	2,48	29,76	372	401,76
AES CTR	128	0,57	6,84	598	604,84
Sosemanuk	128	1,48	17,76	1049	1066,76
Panama	256	1,36	16,32	1803	1819,32
Poznámka: Vychází z Crypto++ Benchmark. Měřeno na procesoru Intel Core-i5 Skylake 2,7 GHz.					

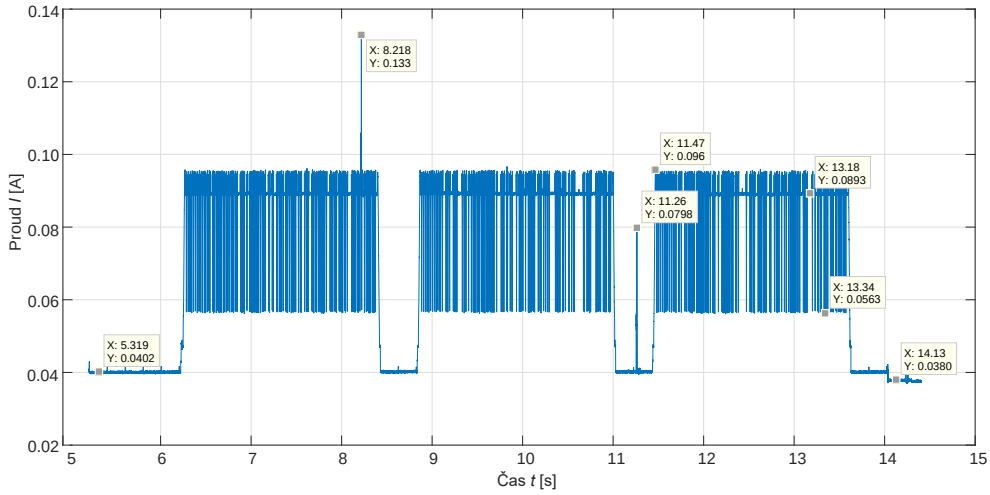
Pro další použití a implementaci jsme se rozhodli použít šifry ChaCha20, AES CTR a OTP. Jak z posledního sloupce tabulky vyplývá, tak šifra ChaCha20 je velice rychlá pro šifrování dvanácti bajtových zpráv, a proto ji budeme implementovat. Šifru AES jsme vybrali, protože má také dobrou rychlost šifrování a je obecně známá a široce nasazovaná. Proto bude sloužit jako dobrý příklad při srovnání s ostatními vybranými šiframi. Primárně se budeme zaměřovat na implementaci šifry OTP, protože je rychlejší a jednodušší než všechny ostatní uvažované šifry.

ONE-TIME PAD

Vernamova šifra, také známa jako One-Time Pad, je jednoduchý avšak účinný šifrovací algoritmus. Její princip spočívá v posunu každého znaku zprávy o určitý počet míst v abecedě. Každý znak se posouvá o náhodný počet míst, což určuje zcela náhodný klíč, který by měl znát jen odesílatel a příjemce. Prakticky dojde k náhradě náhodnými znaky a na tomto faktu je založen důkaz o nerozluštitelnosti této šifry. Jelikož šifra používá unikátní klíč pro každou zprávu, je velice důležité zajistit bezpečný přenos tajného klíče k příjemci. To se však nemusí dělat v případě použití synchronizovaných generátorů klíčů nebo předem vygenerované databáze klíčů [5]. Aby šifra fungovala musí splňovat určité podmínky. Jednou z podmínek je, že se klíč smí použít pouze jednou. Toto pravidlo je v binární variantě šifry velice důležité, protože pro operaci exkluzivní disjunkce (XOR, z anglického exclusive disjunction, značíme $\otimes$) platí: $(A \otimes X) \otimes (B \otimes X) = A \otimes B$ [5].

4 MĚŘENÍ ENERGETICKÉ NÁROČNOSTI

Cílem tohoto měření bylo zjistit jak hodně je provedené hardwarové řešení energeticky náročné a případně zjistit, která část algoritmu je nejvíce energeticky náročná. To by nám mělo pomoci při pozdější optimalizaci kódu. Měření bylo provedeno za pomoci přístroje N6705B Power Analyzer. Výsledkem měření je graf odebíraného proudu v závislosti na čase, který můžete vidět na Obrázku 2. Dalším výsledkem je hodnota celkového odběru na jednu zprávu. Tato hodnota se rovná výsledku integrálu $\int_{5,2}^{14,4} Idt = 0,6619$ A. Výsledek je vyšší, než jaký jsme očekávali. Tomu tak je z důvodu neoptimalizování programu, odesílání zprávy třikrát po sobě (bezpečnostní opatření technologie Sigfox) a také faktu, že Arduino UNO obsahuje mnoho aktivních vedlejších částí.



Obrázek 2: Graf změřeného odběru v závislosti na čase.

5 ZÁVĚR

Cílem této práce bylo navrhnout zabezpečení komunikace bezdrátové nízko-energetické komunikační sítě Sigfox. To bylo dosaženo postupným získáváním znalostí o komunikační síti a o vhodných šifrách. Další důležitou částí bylo vybrat tři nejvhodnější šifry a vhodně je implementovat. Vybrali jsme šifry OTP, ChaCha20 a AES CTR. Vše bylo zrealizováno na vývojové desce Arduino UNO, ke které byl připojen Sigfox modul s anténou a SD modul s paměťovou kartou, na které byli uloženy klíče potřebné pro šifrování. Práce bude dále pokračovat se zaměřením na snížení energetické náročnosti a zabezpečení zařízení proti prolomení.

REFERENCE

[1] VOJÁČEK, A. *SIGFOX - princip, struktura, protokol, použití* [online]

[2] KRPÁLEK, J. *Inteligentní řízení veřejného osvětlení v koncepci IoT* [online]. ČVUT v Praze. 2017

[3] TORNEA, O.; BORDA, M. E.; PILECZKI, V.; MALUTAN, R. *DNA Vernam cipher*[online], E-Health and Bioengineering Conference. 2011

[4] DAI, W. *Crypto++ 6.0.0 Benchmarks* [online]. Dostupné z: https://www.cryptopp.com/benchmarks.html

[5] ŠILHAVÝ, P. *Datová komunikace*, VUT v Brně, první vydání. 2012. ISBN: 978-80-214-4455-3