SECURE COMMUNICATION IN MODERN RADIO NETWORKS

Martin Frei

Grammar school (3), Gymnázium Matyáše Lercha

E-mail: marting1177@gmail.com

Supervised by: Radek Fujdiak

E-mail: fujdiak@feec.vutbr.cz

Abstract: The goal of this research is to create fast, secure and low energy E2E encryption that would supplement the absence of such cryptosystem in the currently expanding Sigfox network and, at the same time, utilize the already existing network security as best as possible.

Keywords: Internet of Things; Encryption; Design and implementation of encryption; LPWAN; Sigfox; Vernam cipher;

1 ÚVOD

Sigfox je relativně novou rozrůstající se sítí v ČR, která je vytvořena podle konceptu IoT. Aktuálně pokrývá 92 % našeho území [1]. Síť pracuje na technologii velmi úzkého pásma, což zajišťuje velký dosah ve vnitřním i ve venkovním prostředí.

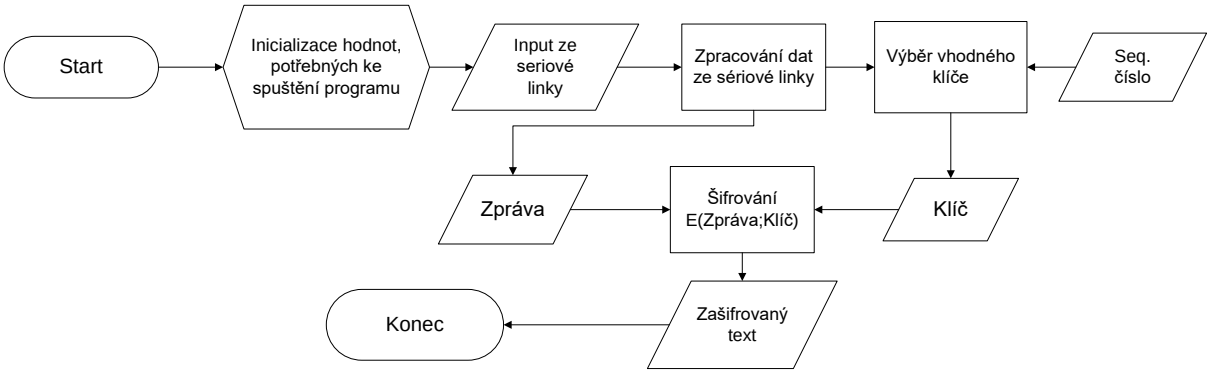
Cílem článku je analyzovat použitelná šifrování a provést výběr a implementaci vhodného kryptosystému typu konec-konec (E2E z angl. End to End) do této sítě a tím vyřešit stávající absenci ochrany důvěrnosti v síti [2]. Budeme se zabývat distribucí klíčů, výběrem šifry. Následně provedeme rozsáhlá měření, která nám zaručí, že jsme vybrali správně.

2 VÝBĚR ŠIFRY

Při výběru vhodné šifry pro Sigfox nás bude nejvíce ovlivňovat délka zprávy (maximálně 12 B), již implementované zabezpečení, energetická náročnost, rychlost šifrování. Ze základu je možné vybírat ze 2 základních druhů šifer, a to šifry symetrické a asymetrické. Asymetrické šifrování je pro naše účely příliš výpočetně a energeticky náročné, proto bude vybrána jedna ze symetrických šifer. Při výběru byly podrobně rozebrána šifra OTP a AES CBC, po jejich důkladném zhodnocení, byla zvolena šifra OTP, u které je matematicky dokázána její nerozluštitelnost [4]. Šifru kombinujeme s již vloženým zabezpečením sítě. HMAC a CRC8 je používán pro kontrolu integrity zpráv [2].

3 IMPLEMENTACE ŠIFRY

Šifra byla implementována do vývojového kitu Arduino s přídavným modulem pro SD kartu a LPWAN modulem, který zajišťuje komunikaci se sítí Sigfox. Na obrázku 1 můžeme vidět, že šifrovací algoritmus je velmi jednoduchý a energeticky nenáročný. Inicializace hodnot obsahuje kontrolu zapojení modulů a spouštění sériových linek, dále program zpracovává input ze sériové linky, poté se vybere vhodný klíč a zpráva se zašifruje. Samotná operace šifrování je velmi málo energeticky náročná, probíhá pomocí operace exkluzivní disjunkce (XOR) zprávy s vybraným klíčem z SD karty.

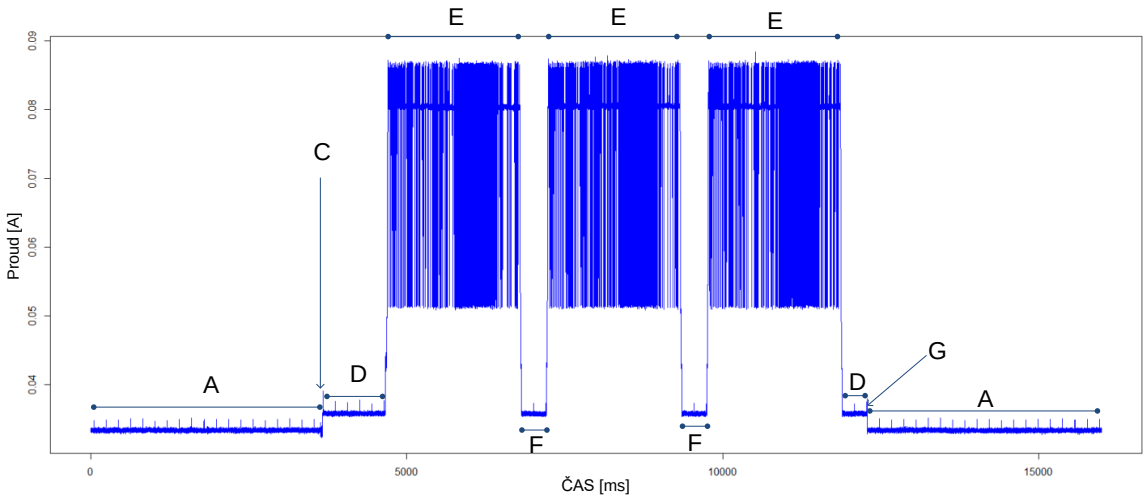


Obrázek 1 blokové schéma šifrovacího algoritmu, dešifrování vice versa.

Databáze klíčů je vytvořena v textovém souboru uloženém na SD kartě. Klíče jsou uložené po 12 B řádcích, každý řádek reprezentuje sekvenční číslo zprávy, pokud přeteče maximální hodnota sekvenčního čísla (4096), číslování započne znovu od nuly. Komunikaci s SD kartou zajišťuje základní knihovna pro Arduino (SD.h). Výdrž modulu na baterii se pohybuje kolem 3–10 let, pokud by bylo zařízení používáno 10 let a chtěli bychom odeslat maximální počet povolených 144 zpráv za den, potřebovali bychom 144*365*10= 525600 klíčů. Pro uložení tohoto počtu klíčů je potřeba 6,3072 MB paměti. Na straně serveru budou nahrány stejné klíče, díky kterým se payload bude dešifrovat. Pro generování náhodných klíčů je vhodné využít hardwarový generátor, např. ChaosKey.

4 MĚŘENÍ

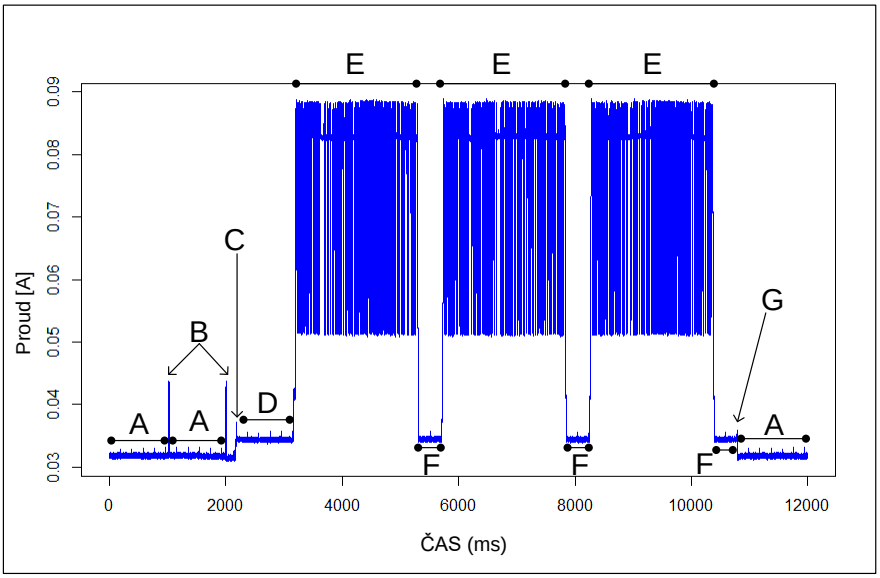
Měření v zařízení bez implementovaného šifrování (obrázek 2) probíhalo 2,5 min. a bylo při něm odesláno 30 zpráv s 15 s prodlevou mezi jednotlivými zprávami. Interval snímání odběru byl 0,08 ms. Odběr v zařízení není nijak razantní, pouze při odesílání zpráv vzroste na hodnoty nad 0,07 A.



Obrázek 2 graf odběru proudu v zařízení bez implementovaného šifrování, popisky grafu vysvětleny níže.

Zařízení s implementovaným šifrováním (obrázek 3) probíhalo 2,5 min., bylo při něm odesláno 30 zpráv s prodlevou 15 s mezi nimi. Interval snímání odběru byl nastaven na 0,02 ms. Celý proces před odesláním zprávy (i s šifrováním) trvá, dle grafu cca 1000 ms, jeho průměrný odběr činní 0,0347 A. V porovnání s odesláním zprávy jde o minimální navýšení. Můžeme zde vidět 3 špičky, první z nich je způsobena použitím SD modulu pro načtení klíče (0,044 A), druhá je vytvořena šifrováním zprávy samotné (0,044 A), poslední je odběr při vytváření režie zprávy (0,03636 A).

Tyto 3 špičky jsou zanedbatelné, pokud je přirovnáme k odběru LPWAN modulu (0,07818 A). Z grafu je tedy zřejmé, že naše šifra je energeticky velmi úsporná a je možno ji používat i na zařízeních umístěných v odlehlých oblastech, kde je výdrž baterie klíčovou vlastností.



Obrázek 3 měření odběru energie v zařízení s implementovaným šifrováním, popisky grafu vysvětleny níže.

Popisky ke grafům:

A....0,03342 A, B....0,04400 A, C....0,03636 A, D....0,03533 A, E....0,07818 A, F....0,03533 A, G....0,03580 A.

5 ZÁVĚR

Cílem této práce bylo navrhnout a implementovat kryptosystém, který by vyřešil dosavadní absenci mechanismu pro zaručení důvěrnosti zpráv v síti Sigfox. Proto byla provedena důkladná analýza možných kryptosystémů, které by dokázaly co nejlépe využít již existující bezpečnostní prvky sítě. Výběrem šifry OTP bylo zajištěno rychlé, bezpečné, a hlavně nízkoenergetické E2E šifrování pro uživatele Sigfox, které může být nadále rozšířeno a uvedeno do praxe. Energetická náročnost našeho šifrování je potvrzena měřeními, která jsou uvedena výše. Bezpečnost šifry OTP je pomocí kombinace s prvky sítě Sigfox pro zaručení integrity více než uspokojivá a je rozebírána v pracích [3,4,5].

REFERENCE

[1] SIMPLECELL. Connecting things. *Simplecell* [online]. [cit. 2018-02-28]. Dostupné z: https://simplecell.eu/

[2] Sigfox. *Sigfox technical overview* [online]. May 2017, , 26 [cit. 2018-02-28]. Dostupné z: https://www.disk91.com/wp-content/uploads/2017/05/4967675830228422064.pdf

[3] KOUŘIL, Daniel a Luděk ŠULÁK. Zdokonalení autentizace použitím jednorázových hesel [online]. Plzeň: IMPROMAT CZ, 2006 [cit. 2018-03-11]. ISBN 80-86583-11-2. ISSN 1211-8737. Dostupné z: https://europen.cz/Anot/29/HLAVNI.pdf#page=47

[4] SINGH, Simon. Kniha kódů a šifer [online]. 2003 [cit. 2018-03-11]. ISBN 80-86569-18-7.

[5] HÁLA, Vojtěch. Kvantová kryptografie. Aldebaran Bulletin [online]. 2005, 4. Duben, 3(14), 3. ISSN 1214-1674. Dostupné z: http://aldebaran.cz/bulletin/2005_14_kry.php