OVĚŘENÍ BEZPEČNOSTI LORAWAN SÍTĚ POMOCÍ SIMULOVANÝCH SCÉNÁŘŮ

EVALUATION OF THE SECURITY OF A LORAWAN NETWORK USING SIMULATED SCENARIOS

Ondřej Pospíšil, Radek Fujdiak
Fakulta elektrotechniky a komunikačních technologií VUT v Brně
Technická 12, Brno
E-mail: {xpospi89, fujdiak}@vutbr.cz

ABSTRAKT

LoRaWAN je komunikační protokol, který poskytuje komunikaci na velkou vzdálenost s malou spotřebou energie. Protokol se díky svým vlastnostem stal velice populární v oblasti Internetu věcí (IoT). V této souvislosti má bezpečnost tohoto protokolu velký význam, vzhledem k současné všudypřítomnosti IoT. Článek se zabývá odposlechem, zachycením a dešifrováním komunikace protokolu LoRaWAN na fyzické vrstvě a na podvrstvě Media Access Control (MAC) linkové vrstvy. Článek je zaměřen na bezpečnostní mezeru v rámci zpětné kompatibility protokolu LoRaWAN. Aktuálně se používá protokol LoRaWAN ve verzi 1.1.x, který řeší většinu bezpečnostních mezer z předchozího protokolu 1.0.x. V práci bylo pro odposlech zpráv použito softwarově definované rádio. V článku byla ověřena bezpečnost v rámci zpětné kompatibility, a to použitím útoku přehráním zprávy a zasláním falešné zprávy na server.

ABSTRACT

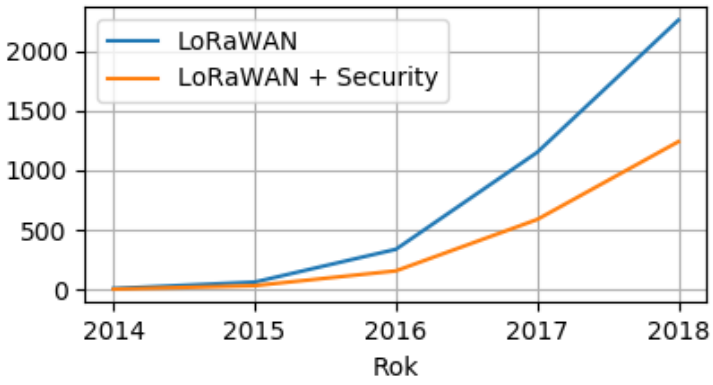
LoRaWAN is a communication protocol that provides long-distance communication with low power consumption. Due to its features, the protocol has become very popular in the Internet of Things (IoT). In this context, the security of this protocol is of great importance, given the current ubiquity of IoT. This article deals with eavesdropping, interception, and unauthorized decryption of LoRaWAN communication on the physical layer and MAC layer with particular focus on the security gap in LoRaWAN backward compatibility. The LoRaWAN version 1.1.x is currently in use, which addresses most of the security gaps from the previous 1.0.x protocol. For eavesdropping messages was used software defined radio. The article has verified backward compatibility security by using a replay attack and sending a fake message to the server.

Klíčová slova: LoRa, LoRaWAN, Softwarově definované rádio, LPWAN, Šifrování, Bezdrátová komunikace, IoT, Cybersecurity

Keywords: LoRa, LoRaWAN, Software defined radio, Security, LPWAN, Wireless communication, IoT, Cybersecurity

ÚVOD

V současnosti je svět obklopen internetem věcí (IoT) v rámci něj jsou často skloňovány sítě typu Low Power Wide Area Networks (LPWAN). Do této kategorie sítí patří i technologie LoRaWAN, ta se využívá především pro senzorická měření v různých oblastech [1]. Tím, že se využití IoT kolem nás zvyšuje, je třeba dbát také na zabezpečení jednotlivých technologií. I při senzorickém měření, může mít správně vedený útok silný dopad. Článek se zabývá útokem přehrání zprávy a také změnou přenášené zprávy. Právě při změně zprávy může být hodnota senzorického měření přepsána a například v energetickém odvětví tyto falešné hodnoty můžou vést například k finančním ztrátám. Z obr. 1 lze vidět, že se zvyšuje zájem akademické i průmyslové sféry nejen o problematiku LoRaWAN sítí, ale také o bezpečnost těchto sítí.



Obr 1: *Výsledek hledání pomocí klíčových slov „LoRaWAN“ a „LoRaWAN + Security“ slov ve vyhledávači Google Scholar [zdroj: autor].*

V první sekci článku je stručně obecně popsána technologie LoRaWAN, jsou zde popsány některé prvky bezpečnosti, které jsou důležité pro porozumění následné ukázky experimentálních útoků v testovací síti. Je zde také popsána aktivační procedura Over-The-Air Activation (OTAA), která je stěžejním prvkem jednotlivých útoků v tomto článku. Článek také poukazuje na některé bezpečnostní rizika, které jsou důležité v rámci zpětné kompatibility sítě. Další část se zabývá experimentálním prostředím, kde jsou popsány jednotlivé prvky a jejich konfigurace v experimentální síti LoRaWAN. V následující části jsou popsány scénáře testování útoků na tuto síť. Jako poslední je v článku popsáno dešifrování jednotlivých vrstev a následná simulace těchto scénářů.

LORAWAN

LoRaWAN patří mezi sítové technologie, které spadají do kategorie geograficky rozsáhlých sítí s nízkou spotřebou energie koncových zařízení. Tato kategorie sítí se nazývá Low Power Wide Area Networks (LPWAN). LPWAN technologie lze využít v sítích Internetu věcí (IoT) a to například v oblastech chytrých měst, logistice, chytrých energetických sítích, nositelné elektroniky, chytrých odečtů dat, průmyslové monitorování, zemědělství a v dalších oblastech [2]. LPWAN sítě nejsou vhodné pro všechna IoT zařízení, ale jsou vhodným řešením v oblastech, kde je kladen důraz na výdrž baterie a kde je tolerance ke zpoždění přenosu (není potřeba real-time přenosu) a hlavně tam, kde jsou požadavky na nízké náklady vybudování sítě [2, 3]. LoRaWAN je otevřeným standardem LoRa Aliance od roku 2015 [4]. Existují i další LPWAN technologie, z nejznámějších je potřeba zmínit technologie NarrowBand-IoT (NB-IoT) a Sigfox. Každá z těchto technologií má své klady i zápory. Hlavní výhodou LoRaWAN oproti ostatním je možnost vytvoření vlastní soukromé sítě bez zásahu třetí strany. Nevýhodou je menší plošné pokrytí bránami z globálního pohledu.

LoRaWAN se skládá z fyzické vrstvy, na které pracuje proprietární modulace Long Range LoRa), pomocí této modulace jsou přenášeny data. Dále využívá LoRaWAN podvrstvy Media Acces Control (MAC), která umožňuje koncovým zařízením komunikovat s nízkou spotřebou energie, mimo to podvrstva umožňuje škálovatelnost a mobilitu sítě.

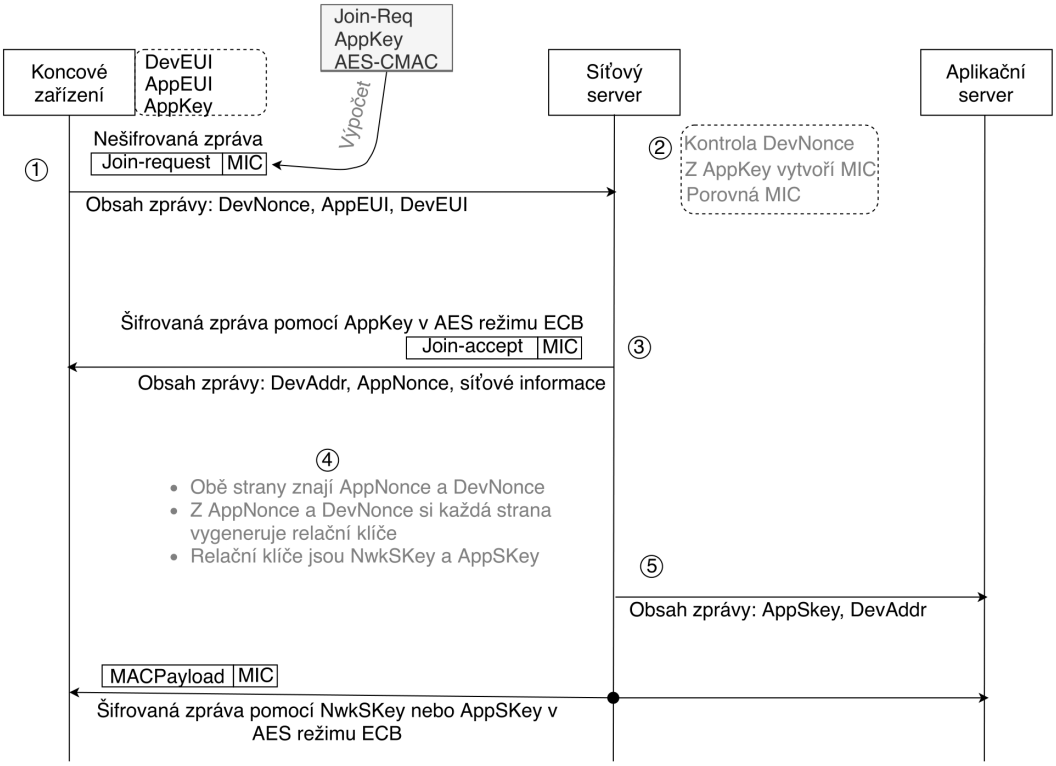
V současnosti je LoRaWAN v provozu ve dvou různých verzích protokolu a to ve starší verzi 1.0.x [4] a nové verzi 1.1.x [5]. Verze 1.1.x řeší velké množství bezpečnostních rizik ze starší verze 1.0.x. Pokud v síti budou zařízení, která stále pracují na verzi 1.0.x síť se v rámci zpětné kompatibility přizpůsobí staršímu protokolu [6]. Síť bude tedy stále náchylná i na útoky z verze 1.0.x. Tento článek se bude dále věnovat pouze protokolu ve verzi 1.0.x vzhledem k stále možným rizikům útoků v rámci zpětné kompatibility.

Síťová architektura LoRaWAN ve verzi 1.0.x se skládá z koncových zařízení které komunikují s jedno nebo s více bránami, zařízení si předávají data s bránami pomocí modulace LoRa. Brána funguje jako prostředník, který v obou směrech přenáší zprávy mezi těmito koncovými prvky a centrálním síťovým serverem. Síťový server může být s bránou propojen drátově (např. ethernet) nebo bezdrátově (např. Wi-Fi, 4G). Síťový server může provozovat také aplikační server anebo k němu může být připojen další samostatný aplikační server, který provozuje aplikace pro IoT.

Článek se věnuje především ověřením bezpečnosti v rámci zpětné kompatibility LoRaWAN a to pomocí zachycení zpráv při registraci zařízen do sítě. Proto zde budou stručně popsány relační klíče a postup registrační procedury, všechny klíče jsou 128 bitové a šifrované pomocí Advanced Encryption Standard (AES) [7]:

- **AppKey:** Kořenový klíč, který je uložen na koncovém zařízení, musí být definován před registrací zařízení. Slouží k odvození relačních klíčů (AppSKey, NwkSKey).
- **NwkKey:** Jedná se o síťový relační klíč, specifický pro každé zařízení. Klíč používá síťový server i koncové zařízení pro výpočet MIC (Message Integrity Code), používá se i pro šifrování FRMPayloadu (užitečných dat) ale pouze při přenosu MAC příkazů.
- **AppSKey:** Jedná se o aplikační relační klíč, specifický pro každé zařízení. Používá jej koncové zařízení a aplikační server k šifrování a dešifrování FRMPayloadu ve kterém jsou přenášena aplikační data.

V rámci LoRaWAN existují dvě možnosti aktivace koncového zařízení. Jsou to Over-The-Air Activation (OTAA) a Activation By Personalization (ABP), která je doporučena jen pro testovací prostředí. V článku je testována zranitelnost pomocí zachycení aktivační procedury OTAA, proto zde bude tato procedura popsána a ukázána. V připojovací proceduře dochází k výměně dvou zpráv se serverem a zařízením, jsou to zprávy typu join-request a join-accept [4]. Na obr. 2 lze vidět, jak probíhá aktivace pomocí OTAA. Na koncovém zařízení musí být uloženy údaje `DevEUI`, `AppEUI` a `AppKey`. Následně koncové zařízení posílá zprávu typu join-req ve které jsou obsaženy hodnoty `DevNonce`, `AppEUI` a `DevEUI`. Nad zprávou je vygenerován MIC (Message Integrity Code) pomocí šifrování AES (CMAC). Zpráva není nijak šifrována. Poté síťový server zkontroluje hodnotu `DevNonce`. Následně je ověřen MIC. Poté síťový server vygeneruje `DevAddr`, `AppNonce` a `NetID` a vytvoří zprávu typu join-accept. Pro tuto zprávu je opět vygenerován MIC a celá zpráva je zašifrována pomocí klíče `AppKey` a AES šifry v režimu Electronic Codebook (ECB) a zpráva je odeslána na koncové zařízení. Na síťovém serveru a koncovém zařízení jsou uloženy stejné informace. Z hodnot `AppNonce` a `DevNonce` vygenerovány hodnoty `NwkSKey` a `AppSKey`.



Obr 2: *Přenos zpráv v rámci aktivace OTAA [zdroj: autor].*

BEZPEČNOSTNÍ RIZIKA

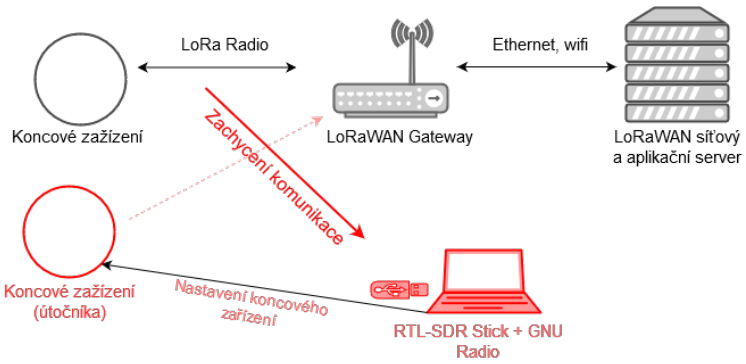
V současnosti jsou bezpečnostní rizika v rámci zpětné kompatibility podle výzkumu [6] tyto:

- **Přehrávání zpráv a jejich odposlech:** Ve verzi 1.0.x není síť chráněna oproti opětovnému použití čítače rámců. To znamená, že je útočníkovi umožněno odposlechnout a poté přehrát zprávu, která přijde v pořádku na server. Díky tomu je také útočník schopen zachytit a sledovat více zpráv, které jsou vytvořeny pomocí stejných relačních klíčů, které mají stejnou hodnotu čítače rámců. Díky tomu může útočník zamezit odesílání nových zpráv na server. Útočník může odposlouchávat také všechny zprávy, jelikož může obnovit text z šifrované zprávy [8, 9, 10]. Tento útok bude popsán v rámci článku.
- **Vytvoření falešné relace:** Je možné vytvořit falešnou relaci, kterou plně ovládá útočník, a tedy posílá svá falešná data a čítač pracuje naprosto správně, to znamená, že uživatel si tohoto útoku nemusí ani všimnout. Díky datům získaným z připojovací procedury je útočník schopen vytvořit vlastní falešnou zprávu obsahující přesně data, která útočník vyžaduje [6, 11]. Tento útok bude popsán v rámci článku.
- **Acknowledged (ACK) spoofing a Bit flipping:** Při ACK spoofingu je schopen útočník pracovat s nedostatkem asociací mezi uznáním a potvrzením dat. Útočník může zachytit potvrzovací zprávu ACK a poté s ní libovolně pracovat a potvrzovat další zprávy. Bit flipping je útok možný díky nedostatečné ochraně integrity aplikačních dat, jde o to, že transportní vrstva mezi síťovým a aplikačním serverem nemusí být plně zabezpečena a zde může útočník pracovat. Díky tomu může útočník provést úpravu přenášených dat jednotlivých aplikací. V tomto případě je ohrožena především důvěryhodnost přenášených dat [6, 9, 10].
- **Odepření služby (DoS) na koncovém zařízení:** Tohoto útoku je možné dosáhnout dvěma způsoby a to přehráním potvrzovací zprávy nebo přehráním zprávy požadavku. První způsob

probíhá tak, že útočník odpoví na žádost o připojení od koncového zařízení před síťovým serverem. Koncové zařízení odešle útočníkovi relační klíč. Koncové zařízení a síťový server skončí každý s jinými odvozenými klíči a ztratí schopnost komunikovat. Druhý způsob probíhá tak, že útočník přehraje zprávu žádosti a na síťovém serveru se vytvoří nová relace. Tím je útočník schopen rozhodit komunikaci koncového zařízení se síťovým serverem. Pokud síťový server udržuje více nepotvrzených relací, tak přehráním více relací může být server přinucen zahodit relační kontext koncového zařízení bez čekání na jakékoli potvrzení [6, 9, 10].

EXPERIMENTÁLNÍ PROSTŘEDÍ

Pro experimentální simulaci útoků v LoRaWAN síti byla sestavena privátní testovací síť. Schéma této sítě lze vidět na obr. 3. Jednotlivé prvky a jejich konfigurace budou popsány následně v textu. Síť pracuje v rámci protokolu LoRaWAN ve verzi 1.0.2. V práci byl také vytvořen vlastní LoRaWAN server na open source řešení Chirp stack [12] v rámci tohoto serveru byl spuštěn síťový i aplikační server na jednom místě.



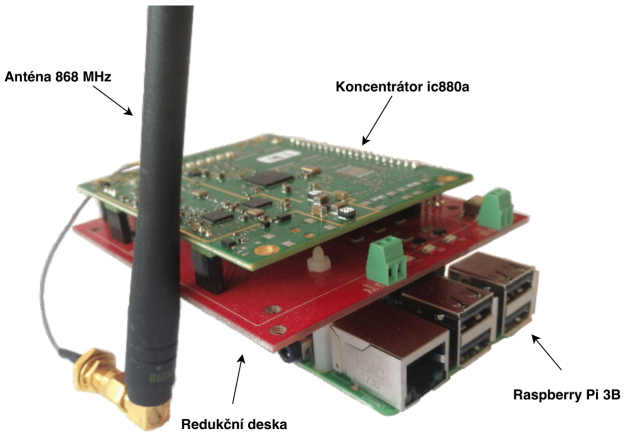
Obr. 3: *Schéma sítě pro experimentální měření [zdroj: autor].*

KONCOVÁ ZAŘÍZENÍ

Jako koncová zařízení byla zvolena dvě zařízení LoRa modul RHF PS01509 [13] a zařízení postavené na modulu Murata [14]. První koncové zařízení RHF bylo použito jako zařízení, které je běžnou součástí sítě a komunikuje s bránou, je to zařízení, jehož komunikace byla odposlouchávána. Druhé zařízení Murata, bylo zvoleno jako útočné zařízení a to vzhledem k tomu, že zařízení pracuje s balíčkem ,,The I-CUBE-LRWAN“ [15], který umožňuje plné ovládnutí vysílací části zařízení. Tomuto zařízení byly zasílány příkazy z počítače.

BRÁNA

V práci byla zkonstruována brána, která je prostředníkem mezi komunikací koncového zařízení a síťového serveru. . Základem brány byl jednodeskový počítač Raspberry Pi 3 B [16], k němu byla připojena speciální deska LoRaWAN koncentrátoru ic880a [17]. Tento koncentrátor pracuje na frekvenci 869 MHz. Proto byla použita anténa pracující na frekvenci 868 MHz. Pro snadnější a bezpečnější práci byla mezi tyto komponenty připojena redukční deska [18]. Na bránu byl nahrán software potřebný pro přenos samotných paketů, který je kompatibilní s Chirp stack serverem [12]. Bránu lze vidět na obr. 4.



Obr. 4: *Brána LoRaWAN postavena na Raspberry Pi 3 a koncentrátoru ic880a [zdroj: autor].*

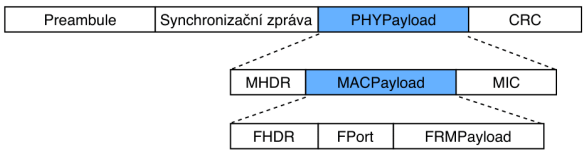
PROSTŘEDÍ POČÍTAČE

Počítač byl připraven pro práci se softwarově definovaným rádiem (SDR), a to pomocí svobodného toolkitu GNU Radio. GNU Radio bylo zvoleno z důvodu většího množství již předpřipravených knihoven pro modulaci LoRa. Pro zachycení komunikace LoRaWAN byla využita open source implementace fyzické vrstvy LoRa Gr-lora [19]. Jako hardware pro SDR bylo zvoleno zařízení RTL-SDR USB [20], jde o nejlevnější řešení a zároveň dostačující na zachytávání LoRaWAN komunikace, zařízení pracuje od 24 MHz až po 1 766 MHz. K zařízení byla připojena všesměrová anténa se ziskem 3 dBi. Zařízení RTL-SDR USB pracuje pouze jako přijímač, ne jako vysílač, což je dostačující.

SCÉNÁŘE TESTOVÁNÍ

V článku je dále ukázáno testování dvou možných scénářů útoků na LoRaWAN síť. Prvním útokem je přehrání zprávy. Tento útok probíhá tak, že útočník zachytí vysílanou zprávu z koncového zařízení a odešle ji ze svého zařízení na bránu. Jsou zde dvě možnosti, pokud je na serveru zapnut čítač rámců, musí být brána rádiově rušena, pokud není může být odeslána a server ji příjme. Tímto způsobem lze realizovat i útok odepření služby (DoS).

Druhý scénář probíhá tak, že útočník zachytí zprávu, dešifruje jí, poté pozmění, znovu zašifruje a odešle na bránu a poté zprávu přijme server. Útočník může ve zprávě upravit všechny informace to znamená, že i když je na serveru spuštěn čítač rámců, není problém pro útočníka změnit číslo odesílané zprávy a tím vyřadit z provozu původní zařízení. Vzhledem k tomu, že jde o zásah do zprávy je zde ukázána struktura zprávy LoRaWAN na obr. 5.



Obr. 5: *Struktura zprávy LoRaWAN [zdroj: autor].*

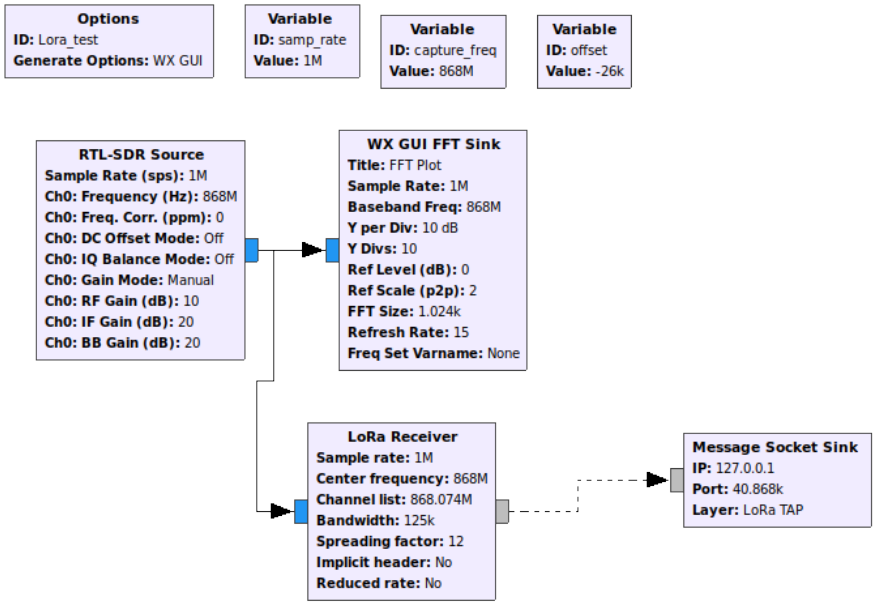
Jediná část celého `PHYPayloadu`, která je šifrována je část `FRMPayload`. Je šifrována aplikačním relačním klíčem `AppSKey` a to pokud nese aplikační data, nebo síťovým relačním klíčem `NwkSKey` pokud nese MAC příkazy. Z toho vyplývá, že pro dešifrování aplikačního datového rámce je nutné znát aplikační relační klíč.

Následně v textu bude ukázáno, jak bylo provedeno dešifrování zprávy LoRaWAN a poté jak byly zrealizovány jednotlivé scénáře v experimentální síti LoRaWAN.

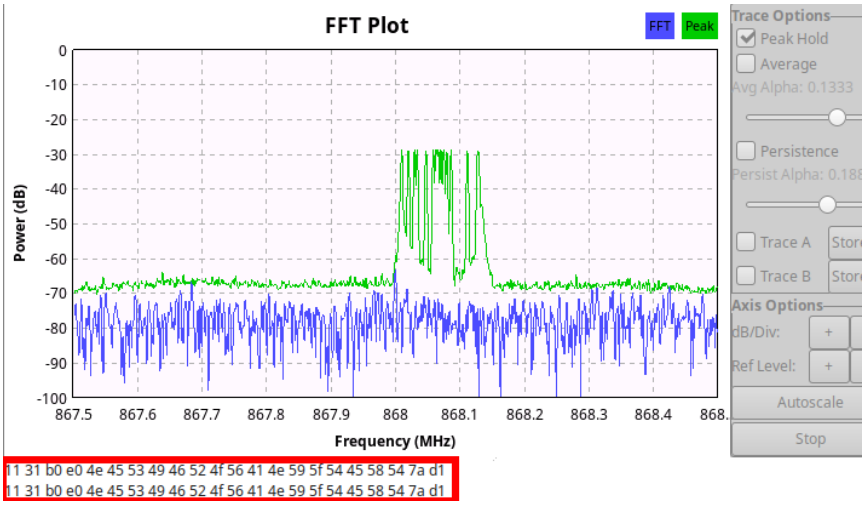
EXPERIMENTÁLNÍ VÝSLEDKY MĚŘENÍ

DEŠIFROVÁNÍ FYZICKÉ VRSTVY LORA

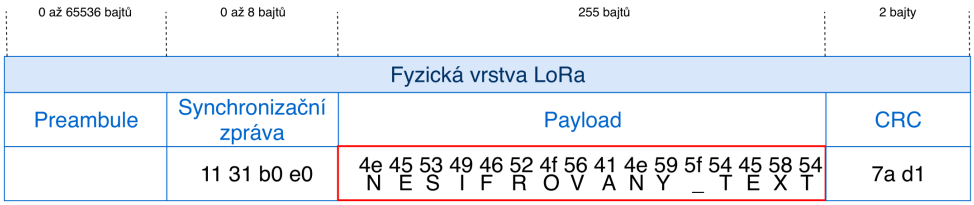
Aby bylo možné realizovat popsané scénáře tak bylo nejdříve nutné odposlechnout pouze fyzickou vrstvu LoRa, aby bylo ověřeno, zda přijaté pakety pomocí GNU radia jsou správné a nejsou přijata zavádějící data. V GNU radiu byly sestaveny bloky pro příjem fyzické vrstvy LoRa pomocí knihovny Gr-lora [20]. Na obr. 6 lze vidět propojení bloků. Jako přijímač bylo ke GNU Radiu připojeno zařízení RTL-SDR USB [18]. Pomocí tohoto zařízení byla zachytávána komunikace z koncového zařízení. Jako koncové zařízení byl zvolen modul RHF PS01509. Z tohoto modulu byla vysílána nešifrována zpráva ,,NESIFROVANY_TEXT“ v hexadecimálním tvaru. Zpráva byla zachycena pomocí GNU Radia to lze vidět na obr. 7. Červeně je označena hexadecimální posloupnost, ve které se nachází požadovaná zpráva. Na obr. 8 lze vidět převod zachycené zprávy z hexadecimálního tvaru.



Obr. 6: *Propojení bloků pro odposlech fyzické vrstvy LoRa v GNU Radiu [zdroj: autor].*



Obr. 7: *Zachycení zprávy v GNU Radiu [zdroj: autor].*

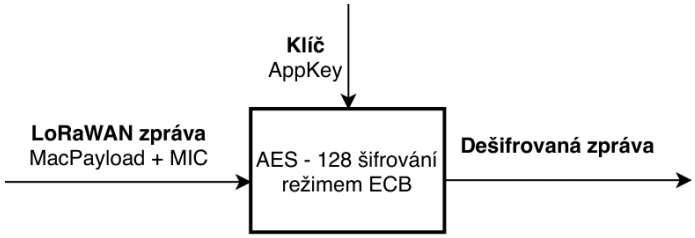


Obr. 8: *Převod zachycené zprávy z hexadecimálního tvaru [zdroj: autor].*

DEŠIFROVÁNÍ LORAWAN MAC

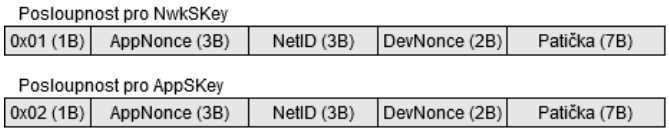
Po zachycení fyzické vrstvy, bylo možné přejít k zachycení a dešifrování vyšší vrstvy MAC. Vysílání a zachytávání datového pole probíhalo stejně jako v předešlém případě s tím rozdílem, že nyní bylo datové pole šifrováno. Jednalo se tedy o reálnou komunikaci. Jak bylo popsáno dříve, celé dešifrování je prováděno na protokolu LoRaWAN verze 1.0.2. Dříve v článku již byla popsána struktura zprávy. Část `PHYPayload` je obsažena ve zprávě a jediná její část, která je šifrována je část `FRMPayload`. `FRMPayload` je šifrován aplikačním relačním klíčem `AppSKey` a to pokud nese aplikační data, nebo síťovým relačním klíčem `NwkSKey` pokud nese MAC příkazy. Z toho vyplývá, že pro dešifrování aplikačního datového rámce je nutné znát aplikační relační klíč. Pro dešifrování a generování relačních klíčů je nutné nejdříve získat `AppKey`. Tento klíč je uložen v paměti koncového zařízení a je také viditelný na síťovém serveru. `AppKey` lze získat z koncového zařízení, na kterém není tento klíč nijak šifrován. Aby bylo možné odvodit relační klíče, je nutné odchytit celou aktivační proceduru OTAA.

Nejdříve byla v GNU Radiu zachycena zpráva typu join-request, tato zpráva není šifrována. Z této zprávy zjistíme hodnotu `DevNonce` (2 poslední bajty zprávy typu join-request). Následně byla zachycena zpráva typu join-accept. Z této zprávy je nutné získat hodnotu `AppNonce` (hodnoty `DevNonce` a `AppNonce` jsou nutné k vygenerování relačních klíčů `NwkSKey` a `AppSKey`). Zprávu typu join-accept je šifrována pomocí AES-128 v režimu ECB, to znamená, že zpráva byla šifrována klíčem o délce 128 bitů. Klíčem pro AES šifru je zde `AppKey`. Ve zprávě je zašifrována pouze část `MACPayload` společně s MIC. Ostatní části zprávy jako synchronizační zpráva, CRC, MHDR je nutné odstranit pro správné dešifrování této zprávy. Na obr. 9 je ukázáno, jak probíhalo dešifrování.



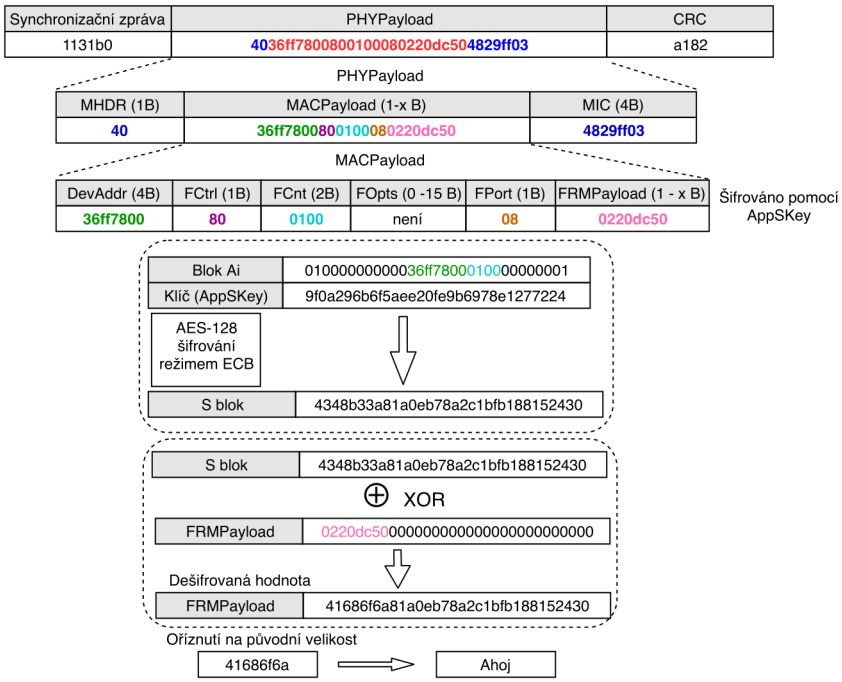
Obr. 9: *Dešifrování zprávy LoRaWAN [zdroj: autor].*

Díky dešifrování této zprávy byla získána hodnota `AppNonce`, ta je, jak bylo zmíněno dříve, nutná ke generování relační klíčů. Klíče se generují pomocí hodnot `DevNonce`, `AppNonce` a `NetID` (tato hodnota je také známa po dešifrování zprávy typu join-accept). K těmto hodnotám se ještě doplní patička nul o velikosti 7 bajtů, aby byla velikost rovna 16 bajtům. Z těchto informací bude nejdříve sestavena hodnota, která je následně zašifrována pomocí aplikačního klíče `AppKey` standardem AES-128 v režimu ECB. Pro každý relační klíč je složena rozdílná hodnota (rozdíl je pouze v prvním bajtu). Pro aplikační relační klíč je první hodnota hexadecimální 0x02 a pro síťový relační klíč je první hodnota 0x01. Na obr. 10 je tato posloupnost ukázána.



Obr. 10: *Posloupnost pro vygenerování relačních klíčů [zdroj: autor].*

Díky zachycení aktivační procedury a následnému vytvoření relačních klíčů, je možné dešifrovat jakoukoli zprávu LoRaWAN v rámci relace. Dešifrování zpráv probíhalo ve zkratce následně. Nejdříve je opět zachycen fyzický přenos paketu pomocí SDR. Tento paket má šifrovanou pouze část `FRMPayload` zbytek je nešifrován. Postupně jsou bajty paketu rozděleny na části, až zbude pouze `FRMPayload`, který nese aplikační data. Dešifrovat `FRMPayload` už je více náročné oproti zprávě typu join-accept. Nejprve je důležité zjistit jakým klíčem je zpráva šifrována, jak bylo zmíněno dříve, jsou dvě možnosti šifrování buď to klíčem `AppSKey` nebo `NwkSKey`. Tuto skutečnost zjistíme díky hodnotě `FPort`. Následně je důležité vygenerovat sekvenci bloků A_i, zde je počet bloků závislý na velikosti `FRMPayloadu`. I když `FRMPayload` má různé velikosti, tak jeden blok A_i může mít pouze 16 bitů. Podle délky `FRMPayloadu` je poté vygenerován přesný počet A_i bloků. A_i blok je sestaven z šesti nulových bajtů poté následuje adresa zařízení v reverzním tvaru, čtyři bajty hodnoty `FCnt`, jeden bajt nul a jeden bajt roven počtu všech bloků. Celý blok A_i je následně šifrován opět pomocí AES-128 v režimu ECB jako klíč je použit `AppSKey`, když je více bloků A_i tak jsou šifrovány po jednom a skládány za sebe, jakožto posloupnost Si bloků. Nakonec probíhá operace Exkluzivní disjunkce (XOR) mezi blokem S (tedy všechny bloky A_i) a `FRMPayloadem`, který je doplněn nulami o stejnou velikost jako má blok `S`. Ukázka dešifrování je na obr. 11, kde byla koncovým zařízením vysílána zpráva ,,Ahoj‘‘, zpráva byla zachycena pomocí SDR a úspěšně dešifrována.



Obr. 11: *Dešifrování zprávy LoRaWAN [zdroj: autor].*

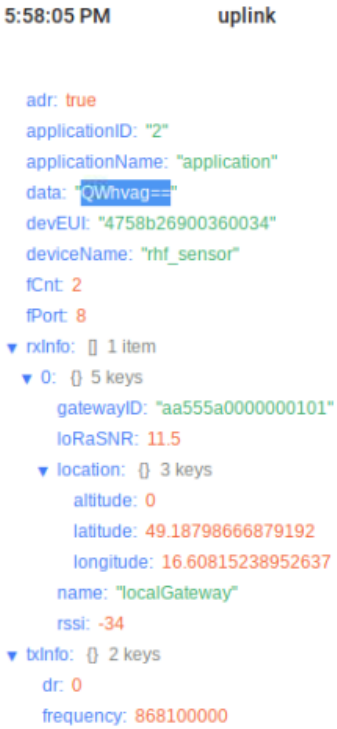
PŘEHRÁNÍ ZPRÁVY

Nejdříve byl proveden útok přehráním zprávy, z koncového zařízení RHF byla vysílána zpráva, tato zpráva byla zachycena pomocí SDR, pro přehrání zprávy bylo použito zařízení Murata, díky balíčku „*The I-CUBE-LRWAN*“ bylo možné plně ovládnout vysílání zařízení. Zařízení bylo přinuceno vysílat

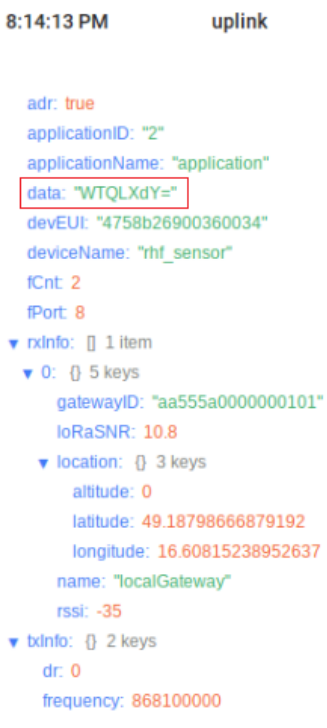
přesnou posloupnost a díky tomu byla zpráva odeslaná ve stejném stavu, jako byla zachycena. Útok přehrání zprávy může být proveden dvěma způsoby. Pokud není na serveru používán čítač příchozích zpráv (`FCnt`), tak není třeba rádio rušení brány a tento útok může posloužit i jako DoS útok. Pokud je čítač na serveru používán, je třeba bránu rádiově rušit a poté lze zprávu na server odeslat pouze jednou. V práci byla experimentálně ověřena možnost, kdy není čítač `FCnt` na serveru v provozu. Nejdříve byla zpráva úspěšně zachycena pomocí SDR, poté byla zkopírována a zaslána pomocí dalšího koncového zařízení Murata na server. Jak lze vidět na obr. 12, tak zpráva byla serverem úspěšně přijata.

ÚPRAVA ZPRÁVY

Po útoku opakováním zprávy byl proveden další útok a to podstrčení falešné zprávy serveru. Byla opět vysílána stejná zpráva jako v předchozím případě. Zachycení zprávy probíhalo stejně jako v případě útoku opakování zprávy, ale následně bylo třeba celou zpráv dešifrovat tak, jak bylo popsáno dříve v článku a poté změnit aplikační datový rámec a znovu celou zprávu zašifrovat a nakonec tuto posloupnost odeslat na síťový server. U tohoto útoku bylo nutné zachytit aktivační proceduru, aby bylo možné odvodit relační klíče potřebné k dešifrování a následnému zašifrování zprávy. Zpráva musela být tedy, jak již bylo popsáno, postupně parsována a dešifrována. Důležitou částí bylo při šifrování zohlednit výpočet MIC, aby server tuto zprávu přijal, musel nad ní být vypočten nový MIC. Šifrování MIC probíhalo pomocí AES-128 v režimu CMAC. Poté co byla sestavena nová falešná zpráva, tak bylo opět využito koncové zařízení Murata a byl upraven jeho kód pro vysílání této posloupnosti. Na obr. 13 lze vidět, jak byla upravená zpráva vůči zprávě z předchozího útoku úspěšně přijata serverem. Pokud známe relační klíče, tak serveru v podstatě lze podvrhnout jakoukoli zprávu, lze si upravit bajtovou posloupnost přesně podle své potřeby.



Obr. 12: *Přijetí zprávy, která nebyla autorizována na server [zdroj: autor].*



Obr. 13: *Přijetí upravené zprávy na server [zdroj: autor].*

ZÁVĚR

Článek se věnoval vytvoření experimentálního prostředí pro testování dvou scénářů útoků na LoRaWAN síť a to útoku přehrání zprávy a poté úpravě zprávy a následnému zaslání na server. V první části článku byl obecný popis protokolu LoRaWAN, a byly zde také popsány některé bezpečnostní prvky protokolu, které byly nezbytné pro následný popis provedených útoků. Následně byla v první části také popsána aktivační procedura OTAA, která je stěžejním prvkem pro testované scénáře. Poté byla v článku popsána konstrukce jednotlivých prvků experimentálního prostředí LoRaWAN. Nakonec bylo v článku popsáno, jak se postupovalo při simulování jednotlivých scénářů. Nejprve zde bylo popsáno dešifrování fyzické vrstvy LoRa a následně vyšší vrstvy MAC protokolu LoRaWAN. Bylo zde ukázáno jak pomocí zachycení aktivační procedury OTAA dešifrovat obsah zprávy. Nakonec byly simulovány dva scénáře útoků na experimentální síť LoRaWAN. Prvním simulace útoku byla přehrání zprávy, kdy byla zachycená zpráva poslána znovu na server jiným zařízením, kdy na serveru nebyl aktivní čítač rámců `FCnt`, to znamená, že tímto způsobem by bylo možné realizovat i útok DoS. Druhá simulace útoku byla o změně obsahu zachycené zprávy, následným zašifrováním nové zprávy a odesláním na server. Při tomto útok lze i změnit hodnot čítače rámců, takže i tímto způsobem lze server zmást a posílat falešné zprávy s vlastními hodnotami. Obě simulace útoků proběhly úspěšně. Útoky byly testovány na verzi 1.0.x, ale v rámci zpětné kompatibility je hrozba těchto útoků stále aktuální a musí se s ní počítat.

LITERATURA

[1] FAROOQ, Muhammad Omer a Dirk PESCH. Analyzing LoRa: A use case perspective. In: *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* [online]. IEEE, 2018, 2018-, s. 355–360 [cit. 2020-03-11]. DOI: 10.1109/WF-IoT.2018.8355224.

[2] MEKKI, Kais, Eddy BAJIC, Frédéric CHAXEL a Fernand MEYER. A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express* [online]. Elsevier, 2019, 5(1), 1-7 [cit. 2020-03-11]. DOI: 10.1016/j.icte.2017.12.005. ISSN 2405–9595.

[3] RAZA, Usman, Parag KULKARNI a Mahesh SOORIYABANDARA. Low Power Wide Area Networks: An Overview. *IEEE Communications Surveys & Tutorials* [online]. IEEE, 2017, 19(2), 855–873 [cit. 2020-03-11]. DOI: 10.1109/COMST.2017.2652320.

[4] SORNIN, Nicolas, Miguel LUIS, Thomas EIRICH, Thorsten KRAMP a Olivier HERSENT. LoRaWAN™ Specification: Version: V1.0. In: *LoRa Alliance* [online]. 2400 Camino Ramon, Suite 375, San Ramon, CA 94583: LoRa Alliance, 2015, s. 1–82 [cit. 2019-05-08]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-05/lorawan1_0_2-20161012_1398_1.pdf/

[5] SORNIN, Nicolas a Alper YEGIN. LoRaWAN™ 1.1 Specification. In: *LoRaWAN Specification* [online]. Beaverton, OR 97007: LoRa Alliance, 2017, s. 1–101 [cit. 2020-01-02]. Dostupné z: https://lora-alliance.org/sites/default/files/2018-04/lorawantm_specification_-v1.1.pdf

[6] DÖNMEZ, Tahsin C.M a Ethiopia NIGUSSIE. Security of LoRaWAN v1.1 in Backward Compatibility Scenarios. *Procedia Computer Science* [online]. Elsevier B.V, 2018, 134, 51–58 [cit. 2020-03-11]. DOI: 10.1016/j.procs.2018.07.143. ISSN 1877-0509.

[7] ADVANCED ENCRYPTION STANDARD (AES). In: *Processing Standards Publication 197* [online]. Federal Information, 2001 [cit. 2020-03-11]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[8] NA, Seungjae, Dongyeop HWANG, Woonseob SHIN a Ki-hyung KIM. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In: *2017 International Conference on Information Networking (ICOIN)* [online]. IEEE, 2017, s. 718–720 [cit. 2020-03-11]. DOI: 10.1109/ICOIN.2017.7899580. ISSN 19767684.

[9] TOMASIN, Stefano, Simone ZULIAN a Lorenzo VANGELISTA. Security Analysis of LoRaWAN Join Procedure for Internet of Things Networks. In: *2017 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)* [online]. IEEE, 2017, s. 1–6 [cit. 2020-03-11]. DOI: 10.1109/WCNCW.2017.7919091.

[10] BUTUN, Ismail, Nuno PEREIRA a Mikael GIDLUND. Analysis of LoRaWAN v1.1 security: research paper. In: *SMARTOBJECTS '18: Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects* [online]. Association for Computing Machinery, 2018, s. 1–6 [cit. 2020-03-11]. DOI: 10.1145/3213299.3213304.

[11] NAOUI, Sarra, Mohamed Elhoucine ELHDHILI a Leila Azouz SAIDANE. Enhancing the security of the IoT LoraWAN architecture. In: *2016 International Conference on Performance Evaluation and Modeling in Wired and Wireless Networks (PEMWN)* [online]. IEEE, 2016, s. 1–7 [cit. 2020-03-11]. DOI: 10.1109/PEMWN.2016.7842904.

[12] BROCAAR, Orne. ChirpStack Network Server. *Github* [online]. Amsterdam: brocaar, 2016 [cit. 2020-03-11]. Dostupné z: https://github.com/brocaar/chirpstack-network-server

[13] *RHF-PS01509: Lorawanclass a/cat command specification* [online]. RisingHF, 2017 [cit. 2019-05-12]. Dostupné z: http://wiki.ai-thinker.com/_media/lora/docs/rhf-ps01509_lorawan_at_command_specification_v3.2.pdf

[14] Sub-GModule Data Sheet. In: *BP-ABZ-C* [online]. Murata (China) Investment Co., s. 1–16 [cit. 2020-01-02]. Dostupné z: https://wireless.murata.com/pub/RFM/data/type_abz.pdf

[15] STM32 LoRa® software expansion for STM32Cube. In: *I-CUBE-LRWAN* [online]. STMicroelectronics, 2019, s. 1–4 [cit. 2020-01-02]. Dostupné z: https://www.st.com/resource/en/data_brief/i-cube-lrwan.pdf

[16] *Raspberry Pi 3 Model B+* [online]. In: . Raspberry Pi Foundation, 2016 [cit. 2020-03-11]. Dostupné z: https://static.raspberrypi.org/files/product-briefs/Raspberry-Pi-Model-Bplus-Product-Brief.pdf

[17] WiMOD iC880A. In: *Datasheet* [online]. 47475 Kamp-Lintfort Germany: IMST, 2016, s. 1–29 [cit. 2020-03-11]. Dostupné z: https://cdn.sos.sk/productdata/61/a5/9d83830f/ic880a-spi.pdf

[18] IC880A LoRaWAN Gateway Backplane v2.0. *Coredump Shop Electronics* [online]. Coredump Rapperswil, 2015 [cit. 2019-05-15]. Dostupné z: https://shop.coredump.ch/product/ic880a-lorawan-gateway-backplane/

[19] ROBYNS, Pieter. Gr-lora. *GitHub* [online]. rpp0, 2016 [cit. 2019-03-29]. Dostupné z: https://github.com/rpp0/gr-lora

[20] *R820T High Performance Low Power Advanced Digital TV Silicon Tuner Datasheet* [online]. In: . Chung Hsing Road, Chutung, HsinChu 310, Taiwan: Rafael Microelectronics, 2011, s. 1–26 [cit. 2020-04-02]. Dostupné z: https://rtl-sdr.com/wp-content/uploads/2013/04/R820T_datasheet-Non_R-20111130_unlocked.pdf