VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2018

Bc. Patrik Škunda

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNÁ AUTENTIZACE A KLÍČOVÝ MANAGEMENT V INTERNETU VĚCÍ
SECURE AUTHENTICATION AND KEY MANAGEMENT IN THE INTERNET OF THINGS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Patrik Škunda**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Lukáš Malina, Ph.D.**
SUPERVISOR

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Telekomunikační a informační technika**
Ústav telekomunikací

Student: Bc. Patrik Škunda ***ID:*** 164419
Ročník: 2 ***Akademický rok:*** 2017/18

NÁZEV TÉMATU:

Bezpečná autentizace a klíčový management v Internetu věcí

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s kryptografickými metodami, které jsou vhodné pro Internet věcí (IoT) a pro aplikaci na výpočetně a paměťově omezených zařízení. Zhodnoťte a analyzujte vybrané bezpečnostní schémata, jejich efektivitu a jejich praktickou aplikovatelnost do systémů IoT. Zaměřte se na moderní šifry a soudobé knihovny pro omezené zařízení a omezené přenosové technologie typy LPWAN a proveďte jejich výkonostní a paměťové zhodnocení. Na základě podrobné analýzy knihoven, šifer a schémat, navrhněte vhodné bezpečnostní řešení, které bude poskytovat nejen autentizaci entit v IoT, ale i autentičnost a integritu přenášených dat. Pro různé vstupní parametry (počet uzlů, délka dat, výpočetní výkonost uzlu) simulujte a zhodnoťte použitelnost řešení.

DOPORUČENÁ LITERATURA:

[1] WANG, Mingjun, YAN, Zheng. Security in D2D communications: a review. Trustcom/BigDataSE/ISPA, 2015 IEEE. Vol. 1. IEEE, 2015.

[2] STALLINGS, William. Cryptography and Network Security. 4th edition. [s.l.] : [s.n.], 2006. 592 s. ISBN 0131873164.

Termín zadání: 5.2.2018 ***Termín odevzdání:*** 21.5.2018

Vedoucí práce: Ing. Lukáš Malina, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Táto práca sa zaoberá problematikou bezpečnej autentizácie a kľúčového managementu v internetu vecí. Popisuje základné protokoly využívajúce sa v IoT, ďalej kryptografické primitíva, komunikačné technológie v IoT a koncové prvky. Súčasťou je aj meranie výkonnosti kryptografických primitív na Raspberry Pi a výber vhodnej LPWAN technológie pre simuláciu. Záver práce je venovaný simulácií LoRaWAN siete.

KĽÚČOVÉ SLOVÁ

Internet vecí, Kryptografické primitíva, Autentizácia, Kľúčový manažment, Obmedzené zariadenie, LoRaWAN, Simulácia

ABSTRACT

This thesis deals with issues of secure authentication and key management in the Internet of Things. It describes basic protocols used in IoT, cryptographic primitives, communication technologies in IoT and end elements. It also includes a measuring the performance of cryptographic primitives on Raspberry Pi and selecting the appropriate LPWAN simulation technology. The conclusion of the work is devoted to the simulation of a LoRaWAN network.

KEYWORDS

Internet of things, Cryptographic primitives, Authentication, Key management, Constrained device, LoRaWAN, Simulation

ŠKUNDA, Patrik. *Bezpečná autentizácia a kľúčový management v internetu vecí*. Brno, 2017, 83 s. Diplomová práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: prof. Ing. Lukáš Malina, Ph.D.

VYHLÁSENIE

Vyhlasujem, že som svoju diplomovoú prácu na tému „Bezpečná autentizácia a kľúčový management v internetu vecí“ vypracoval(a) samostatne pod vedením vedúceho diplomovej práce, využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor(ka) uvedenej diplomovej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto diplomovej práce som neporušil(a) autorské práva tretích osôb, najmä som nezasiahol(-la) nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý(-á) následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákoníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora(-ky)

POĎAKOVANIE

Rád bych poďakoval vedúcemu diplomovej práce pánovi Ing. Lukášovi Malinovi, Ph.D. za odborné vedenie, konzultácie, trpezlivosť a podnetné návrhy k práci. Zároveň by som chcel poďakovať rodine a priateľom, ktorí ma nesmierne podporovali a verili mi.

Brno ....

podpis autora(-ky)

Faculty of Electrical Engineering
and Communication
Brno University of Technology
Purkynova 118, CZ-61200 Brno
Czech Republic
http://www.six.feec.vutbr.cz

POĎAKOVANIE

Výzkum popsaný v tejto diplomovej práci bol realizovaný v laboratóriách podporených projektom SIX; registračné číslo CZ.1.05/2.1.00/03.0072, operačný program Výzkum a vývoj pro inovace.

Brno ....

podpis autora(-ky)

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OP Výzkum a vývoj
pro inovace

Tato práce vznikla jako součást klíčové aktivity KA6 - Individuální výuka a zapojení studentů bakalářských a magisterských studijních programů do výzkumu v rámci projektu OP VVV Vytvoření double-degree doktorského studijního programu Elektronika a informační technologie a vytvoření doktorského studijního programu Informační bezpečnost, reg. č. CZ.02.2.69/0.0/0.0/16_018/0002575.

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Projekt je spolufinancován Evropskou unií.

OBSAH

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ÚVOD

Internet vecí sa v poslednej dobe dostáva viac do pozornosti vďaka pokroku bezdrôtovej technológie. Základná myšlienka je bezdrôtová vzájomná komunikácia jednotlivých systémov a zariadení medzi sebou a ich možnosť ich ovládať, vzdialene sledovať, zbierať a predávať si rôzne informácie. V blízkej budúcnosti sa odhaduje exponenciálny rast počtu týchto zariadení. S takýmto nárastom sa bude zvyšovať aj riziko na ich možné zneužitie alebo ovládnutie, preto je nutné sa zaoberať aj ich bezpečnosťou.

Táto práca sa zameriava na bezpečnú autentizáciu a kľúčový management v internetu vecí. Na začiatku prvej kapitoly je popísaný úvod do internetu vecí, nasleduje popis jednotlivých protokolov používaných v internete vecí, a popis koncových prvkov. Následne je práca zameraná na popis možných útokov v internete vecí a popis kryptografických šifier, ktoré sa využívajú na šifrovanie. V druhej kapitole je rozobratý celkový prehľad bezpečnostných schém v internetu vecí, ktoré sú následne porovnávané. Ďalej sú rozobrané požiadavky na ustanovenie kľúča v internetu vecí. V závere druhej kapitoly sme sa zamerali na bezpečnostné porovnanie jednotlivých kryptografických primitív. Tretia kapitola sa zaoberá porovnaním kryptografických primitív z hľadiska ich výkonnosti na obmedzenom zariadení Raspberry Pi. Kapitola obsahuje taktiež popis metódy merania a popis obmedzeného zariadenia Raspberry Pi. Realizované testovacie merania na kryptografických primitívach sú sumarizované v jednotlivých tabuľkách a následne vyhodnotené a graficky spracované. Nasledujúca kapitola je zameraná na analýzu vhodnosti technológií. Sú tu zhrnuté predpoklady a výber vhodnej technológie pre simuláciu. Záver kapitoly patrí bližšej technickej analýze LoRa. Piata kapitola ponúka prehľad využitia sieťového simulátora NS-3 v IoT. Posledná kapitola sa zameriava už na samotnú simuláciu, ktorá zahŕňa tri scenáre využitia technológie LoRa. Prvý sa zameriava na nízky počet senzorov (do 50), druhý scénar obsahuje rádovo stovky senzorov a tretí rádovo tisícky.

1 KRYPTOGRAFICKÉ METÓDY

Cieľom tejto kapitoly je oboznámiť čitateľa s významom IoT a základnými kryptografickými metódami, ktoré môžu byť nasadené v IoT. Popisuje kryptografické metódy, protokoly, koncové prvky a možné hrozby, potencionálne útoky na dátovú komunikáciu v internetu vecí (i na samotné zariadenie).

1.1 IoT

Anglický názov Internet of Things v skratke IoT je v preklade Internet vecí. Pod týmto pojmom si môžeme predstaviť veci, ktoré sú explicitne identifikovateľné a komunikujú navzájom so sebou. Prvý krát sa toto slovné spojenie objavilo na prezentácií pána Kevina Ashtona v roku 1999 [3].

V dnešnej dobe sa stretávame s týmito vecami každý deň, či už sú to rôzne zariadenia stojace v domácnosti, nosené na tele, vedecké prístroje alebo priemyselné stroje a ďalšie embedded zariadenia, poprípade senzory na sledovanie teploty a vlhkosti. Môžeme sa stretnúť aj s rôznymi senzormi v dopravných prostriedkoch, ktoré napomáhajú záchranným zložkám pri nehode ich v momente lokalizovať a určiť vážnosť dopravných nehôd, napríklad OnStar systém v automobiloch značky Opel. Naše domácnosti sa môžu premeniť na inteligentné a my ich budeme môcť ovládať s malým úsilím odkiaľkoľvek alebo si pred nastaviť správanie našej domácnosti. Kávu si budeme môcť uvariť pomocou mobilného telefónu pred tým ako prídeme z práce domov. Na základe gps signálu z nášho mobilného telefónu pred príchodom domov nám vykurovací systém vykúri alebo vychladí miestnosti na ideálnu nami požadovanú teplotu [30].

Je to koncept s obrovským potenciálom do budúcnosti, ktorý nielen ovplyvní spôsob ako žijeme ale aj to ako pracujeme. Hlavným účelom IoT je zjednodušenie života, šetrenie času a prostriedkov. CEO Erricsonu vyslovil ohromujúcu predpoveď, ktorá tvrdí, že na svete by malo byť do roku 2020 pripojených takmer 50 biliónov zariadení. S neustálim rastom počtu týchto zariadení vzrastá aj možné riziko ich zneužitia, preto je dôležité klásť veľký dôraz na ich bezpečnosť [28].

1.2 IoT Protokoly

1.2.1 CoAP

Protokol CoAP (Constrained Application Protocol) je binárnou verziou protokolu HTTP. Bol navrhnutý na prenos informácií medzi obmedzenými zariadeniami, ktoré sú využívané v IoT. Pakety protokolu CoAP sú omnoho menšie ako protokolu

HTTP. Na komunikáciu využíva protokol UDP a výmena správ medzi zariadeniami je realizovaná asynchrónne. Neposkytuje garanciu doručenia datagramov, či budú datagramy doručené v správnom poradí, alebo ochranu pred duplicitným doručením. Je založený na modely žiadosť-odpoveď a poskytuje tak jednoduchý model interakcie medzi uzlami. Koncept je postavený na tzv. modeli REST (Representational State Transfer). Môžeme ho nájsť v senzorových sieťach inteligentných budovách, spotrebičoch a je dizajnovaný pre komunikáciu M2M (Machine-to-Machine) [38].

1.2.2 DTLS

Datagram Transport Layer Security (DTLS) predstavuje protokol, ktorý zabezpečuje komunikáciu pre datagramové protokoly (napr. UDP). Už ako jeho názov napovedá je založený a postavený na protokole TLS. DTLS je špeciálne navrhnutý tak, aby zmeny v programovaní a používaní oproti TLS boli čo najmenšie. DTLS protokol je navrhnutý k ochrane dát medzi komunikujúcimi aplikáciami. Datagramový prenos nepotrebuje a ani neuskutočňuje spoľahlivé doručovanie dát. DTLS túto vlastnosť dodržiava. Aplikácie, ako sú streamovanie médií, IP telefónia a online hry, používajú datagramový prenos na komunikáciu vďaka citlivosti na oneskorení prenášaných dát. Správanie týchto aplikácii je bezo zmeny nakoľko DTLS nekompenzuje stratu alebo znovu odosielanie dát.

Základnou myšlienkou pri konštruovaní DTLS je vytvoriť TLS nad UDP. Dôvod prečo nemôže byť rovno použité TLS je, že pakety sa môžu strácať. TLS nemá žiadne vnútorné mechanizmy na spracovanie tejto nespoľahlivosti, čo znamená, že nemožno použiť implementáciu TLS na datagramovú prevádzku. Účelom DTLS je vytvoriť čo najmenší počet zmien potrebných na to, aby TLS vyriešilo tento problém. V čo najväčšej možnej miere je snaha aby DTLS bol čo najviac identický s TLS.

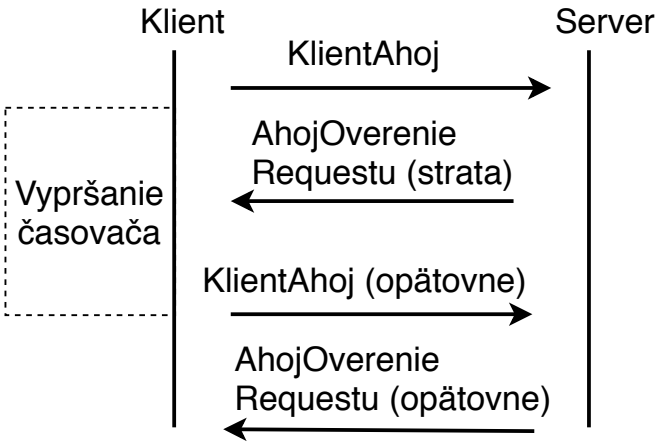
TLS vytvára nespoľahlivosť na dvoch úrovniach: Vrstva pre šifrovanie komunikácie - nedovoľuje dešifrovať jednotlivé pakety. Pretože kryptografický kontext je previazaný medzi záznamami a MAC - Message Authentication Code, ktorý vloží do správy poradové číslo a vykonáva ochranu proti opakovaniu sa a zmene poradia paketov. Vrstva Handshake musí čakať ak sa nejaký paket stratil pretože, to závisí na ich spoľahlivom prenose. Sú na to dva dôvody:

- Keďže handshake je synchronizovaný kryptografický nástroj, vyžaduje aby správy boli prenášané a prijímané v danom poradí. V inom prípade sa to považuje za chybu.
- Môže byť aj problém s fragmentáciou, pretože handshake správy môžu byť väčšie ako prenášané datagramové správy.

Prvý problém, a to väzby medzi paketmi môže byť vyriešený metódou, ktorá je použitá v Secure Internet Protocol (IPsec) pridaním explicitného stavu pre každý

jeden záznam.

K vyriešeniu problému so stratou paketou DTLS používa jednoduchý prenosový časovač. Obrázok 1.1 ukazuje základný koncept prenosu. Klient očakáva od servera správu HelloVerifyRequest. Ak táto správa nepríde, potom klient pošle opakovanú správu ClientHello a server mu následne zase pošle správu HelloVerifyRequest tú istú čo predtým.



Obr. 1.1: Základný koncept DTLS časovača

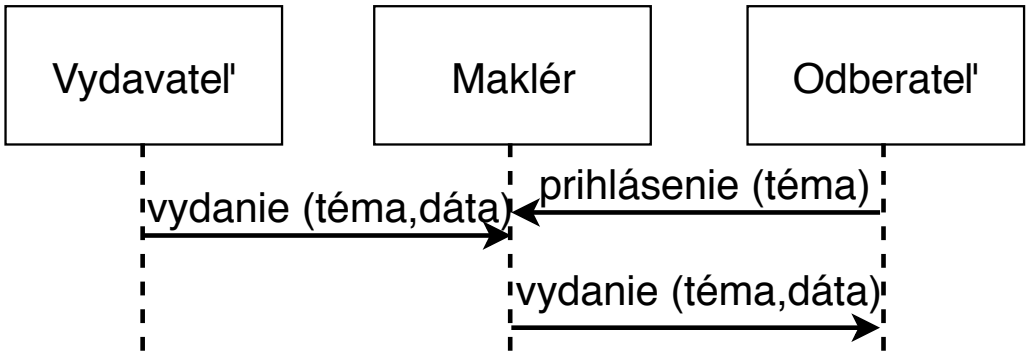
Prehodenie poradia paketov je riešené pridaním špecifického poradového čísla, podľa ktorého sa určuje, či prijatá je nasledujúca v poradí. Ak je ďalšia v poradí tak sa spracuje, ak nie je z daného poradia tak sa zaradí do frontu a čaká, kým sa prijme nasledujúca správa respektívne počet správ, aby sedelo poradové číslo segmentu.

Handshake správy môžu byť pomerne veľké, avšak UDP datagramy sú obyčajne limitované na 1500 bajtov. DTLS to kompenzuje tým, že každá handshake správa bude rozdelená do niekoľkých UDP segmentov. Každá handshake správa potom obsahuje časť offsetu a časť dĺžky, čo umožňuje prijímateľovi znovu poskladať celú správu ak prijal všetky segmenty [45].

1.2.3 MQTT

Message Queue Telemetry Transport (MQTT) je jedným z využívaných aplikačných protokolov v internete vecí. Funguje na princípe zverejnenia a odoberania (publish subscribe). Pre prenos správ je využívaný tzv. broker, ktorý riadi ich prenos správ. Na obrázku 1.2 je znázornená jednoduchá komunikácia, kedy sa odoberateľ (Subscriber) prihlási do určitej skupiny. Následne, keď vydavateľ (Publisher) zverejní dáta patriace do tejto skupiny, tak broker tieto dáta prepošle všetkým odoberateľom.

V súčasnosti existuje aj niekoľko ďalších variant tohto protokolu, ktoré sú lepšie prispôsobené na prácu s hardvérovo obmedzenými zariadeniami. V práci MQTTS



Obr. 1.2: Komunikácia prostredníctvom brokera

– A Publish/Subscribe Protocol For Wireless Sensor Networks autori uvádzajú základné črty protokolu MQTT-S:

- Optimalizácia pre hardvérovo obmedzené zariadenia napájané batériou.
- Prispôsobenie sieťovým podmienkam v senzorových sieťach – malá šírka pásma, vysoká chybovosť doručovania správ a krátke pole dát.
- Nezávislé od prenosovej technológie. Je možné využiť akúkoľvek technológiu, ktorá podporuje službu prenosu podľa sieťovej adresy a službu broadcast.
- V porovnaní s MQTT, nevyžaduje spojovo orientovanú komunikáciu a nespolieha sa na segmentáciu správ a ich doručenie v správnom poradí [12].

Štruktúra

Štruktúra hlavičky protokolu MQTT vychádza podľa špecifikácie verzie 3.1 - [14]. Napriek pevnej dĺžke hlavičky, dĺžka samotných správ je variabilná a záleží od typu správy.

- Message Type – určuje o aký typ správy ide. Napríklad správa typu connect (pripojenie klienta na server), publish (prenos aplikačných dát) alebo subscribe (prihlásenie k odberu správ určitej skupiny) .
- DUP flag – označuje sa ako pozitívny, ak sa doručuje duplikát správy.
- QoS level – označujú úroveň kvality služieb.
- RETAIN – používa sa iba pri správe PUBLISH, ak je nastavený na 1 - vydavateľ žiada server aby si udržal správu až kým nebude doručená všetkým odoberateľom. Správy by mali byť uchovávané aj po reštarte servera[24].

1.3 Protokoly na ustanovenie kľúča

IKE protokol

Internetová kľúčová výmena (Internet Key Exchange) je štandardný protokol IPsec (Internet Protocol Security), ktorý slúži na zabezpečenie vyjednávania o virtuálnej privátnej sieti (VPN) a vzdialenom hostiteľovi, alebo prístupu do siete. Špecifikovaný v IETF RFC 2409, IKE definuje automatický spôsob vyjednávania a autentizácie pre bezpečnostné asociácie IPsec (SA). Bezpečnostné združenia sú bezpečnostné politiky definované pre komunikáciu medzi dvoma alebo viacerými subjektmi, vzťah medzi entitami je reprezentovaný kľúčom . Protokol IKE zaisťuje bezpečnosť komunikácie SA bez predkonfigurácie, ktorá by inak bola potrebná[34].

HIP protokol

HIP - (Host Identity Protocol) definuje mechanizmus zabezpečenia podpisu nazývaný Base Exchange(HIP-BEX). Tento mechanizmus vytvára dynamicky bezpečnostné združenia medzi HIP peermi na internete. Na dohodu tajných kľúčov sú potrebné iba 4 správy. Každý partner HIP by mal mať verejný kľuč slúžiaci ako identifikátor hostiteľa (HI), ktorého protistrana je známa a používaná iba jeho oprávneným vlastníkom. Tieto dva kľúče sú užitočné pre overovanie totožnosti a overovanie cieľov. Ako náhle je vytvorená relácia zabezpečenia HIP, koncoví účastníci môžu začať výmenu dát bezpečne pomocou ESP (Encapsulating Security Payload)pod protokolu IPsec protokolu a tajný kľúč je dohodnutý s HIP. Mechanizmus HIP-BEX zahŕňa ťažké asymetrické kryptografické operácie a z tohto dôvodu ho nemožno podporovať v IoT. Preto bolo navrhnutých niekoľko riešení na zjednodušenie a prispôsobenie HIP. Kvôli zníženiu výpočtových nákladov na HIP-BEX bola zavedená kryptografia eliptických kriviek v Diffie-Hellman (ECDH), a vznikol tak HIP Diet Exchange (HIP-DEX). Na výpočet kľúča relácie a na identifikáciu partnera HIP je potrebný iba jeden verejný kľúč. Preto zadržanie kľúča relácie je dostatočné na autentizáciu uzla a na preukázanie jeho legitímnosti [35].

TLS Handshake protokol

Transport Layer Security (TLS) Handshake Protocol je zodpovedný za overenie a výmenu kľúčov nevyhnutnú pre vytvorenie alebo obnovie zabezpečenej relácie. Pri vytváraní zabezpečenej relácie Handshake Protocol spravuje nasledujúce: vyjednávanie šifrovacích balíkov, autentizácia servera a voliteľne klienta, zmena informácií o kľúči relácie.

- **Vyjednávanie šifrovacích balíčkov** - Klient a server vytvoria kontakt a vyberú šifrovú sadu, ktorá sa použije počas výmeny správ.

- **Autentizácia** - V TLS server preukazuje svoju totožnosť klientovi. Klient môže tiež potrebovať dokázať svoju totožnosť na serveri. PKI, použitie párov verejných / súkromných kľúčov, je základom tejto autentifikácie. Presná metóda, ktorá sa používa na overenie totožnosti, je určená dohodnutou šifrovacou sadou.
- **Výmena kľúčov** - Klient a server si vymieňajú náhodné čísla a špeciálne číslo s názvom Pre-Master Secret. Tieto čísla sa kombinujú s ďalšími údajmi, ktoré umožňujú klientovi a serveru vytvárať zdieľané tajomstvo nazývané Master Secret. Master Secret sa používa klientom a serverom na generovanie zápisu MAC tajomstva, čo je kľúč relácie používaný na hashovanie a kľúč na zápis, ktorý je kľúčom relácie používaným na šifrovanie [43].

1.4 Komunikačné technológie v IoT

Internet vecí si vyžaduje širokú škálu nových technológií a zručností, ktoré mnoho organizácií ešte nemá zvládnutých. Technológie a princípy Internetu vecí budú mať veľmi široký dosah na organizácie, ktoré ovplyvňujú obchodné stratégie, riadenia rizík a širokú škálu technických oblastí, ako je architektúra, návrh, prevádzka a zabezpečenie siete. V ďalších pod kapitolách si priblížime jednotlivé bezdrôtové prístupové technológie vhodné na pripojenie zariadení do Internetu vecí. Na koniec sekcie sú vybrané vlastnosti zhrnuté v tabuľke 1.1. Obrázok 1.4 prehľadne zobrazuje závislosť rýchlosti prenosu dát na dosahu technológie. Nasledujúci obrázok 1.5 detailnejšie zhŕňa vlastnosti.

1.4.1 BLE

Bluetooth Low Energy sa masívnejšie objavil v roku 2011. Je to inteligentná nízkoenergetická verzia Bluetooth určená na komunikáciu v krátkych dosahoch do 50 m. Zásadný rozdiel je, že BLE má nízku spotrebu, ale aj nižšiu priepustnosť dát, čo nemusí byť nevýhodou, ak vezmeme do úvahy veľkosť dát od väčšiny senzorov. Pracovné pásmo je 2,4 Ghz a má zadefinovaných 40 kanálov, pričom rozsah je 1 MHz. Zariadenie vybavené BLE by malo byť schopné vydržať niekoľko rokov. Bluetooth verzia 4.2 vďaka funkcii „Internet Protocol Support Profile“ dovolí inteligentným senzorom prístup na internet priamo cez 6LoWPAN konektivitu. Táto IP konektivita umožňuje využívať existujúcu IP infraštruktúru pre správu inteligentných Bluetooth zariadení. Táto verzia oproti 4.0 zahŕňa väčšiu bezpečnosť, priepustnosť a ďalšiu redukciu spotreby energie. Z bezpečnosti je to LE Privacy 1.2 a LE Secure Connections. LE Privacy 1.2 spôsobuje, že adresa MAC v reklamných paketoch sa má nahradiť náhodnou hodnotou, ktorá sa mení v časových intervaloch určených

výrobcom. Takto je skrytá totožnosť zariadenia a skutočná adresa MAC zostáva skrytá [10].

1.4.2 NFC

Technológia NFC slúži k bezdrôtovej komunikácii na veľmi krátke vzdialenosti, zvyčajne menej ako 4 centimetre, bez nutnosti zbytočného nastavovania pripojenia alebo akéhokoľvek fyzického kontaktu. NFC vychádza z technológie RFID. Komunikácia prebieha vždy len medzi dvoma NFC zariadeniami súčasne, na frekvencii 13,56 MHz a rýchlosťou 106 až 424 kb/s. Technológia je postavená na RFID a zároveň kompatibilná so Smart cards. Dodržiava protokoly ISO/IEC 18092 a ISO/IEC 14443 [25].

1.4.3 WiFi

WiFi je súbor štandardov umožňujúci elektrickým zariadeniam pripojiť sa na bezdrôtovú lokálnu siete LAN (WLAN) v súčasnosti založených na špecifikácii IEEE 802.11. Jeho počiatky sa datujú do roku 1991. Wi-Fi využíva nelicencované frekvenčné pásma, je preto ideálna pre budovanie lacných, ale výkonných počítačových sietí bez nutnosti použitia káblov. Týmito bezplatnými pásmami sú 2,4 a 5 GHz, používanejšie je ale nižšie 2,4 GHz pásmo. V danom pásme je problémom, že ho využívajú aj iné bezdrôtové technológie - či už Bluetooth, alebo rôzne proprietárne rozhrania bezdrôtové myší či klávesnice. Toto pásmo tiež býva najmä v hustej mestskej aglomerácii značne rušené okrem iného aj veľkým množstvom Wi-Fi sietí, preto pripojenie môže byť nestabilné, jeho rýchlosť môže značne kolísať. Preto je výhodnejšie využívať doteraz neveľmi zarušené 5 GHz pásmo. Oproti iným technológiám má Wi-Fi taktiež pomerne obmedzený dosah 1.1 a priepustnosť prekážkami. Wi-Fi je vhodná pre IoT zariadenia, ktoré nepotrebujú dlhú výdrž batérie resp. sú stále pod napätím. V roku 2010 bol vytvorený štandard Low-Power Wi-Fi dôležitý pre rozšírenie oblasti Wi-fi sietí pre splnenie požiadaviek IoT. Medzi najlepšie vylepšenia patrí pripojenie veľkého počtu zariadení, veľký rozsah pokrytia a obmedzenie spotreby energie. V mnohých aplikáciach musí prístupový bod pokryť stovky, niekedy až tisíce zariadení, ktoré pravidelne vysielajú pakety. Jednou z hlavných úloh IEEE pre 802.11 bol obmedzený počet staníc, ktoré môžu byť súčasne pripojené. Nový skrátený formát rámcov, pokročilý mechanizmus prístupu ku kanálom, nové energetické mechanizmy sú vylepšenia, ktoré umožňujú nízko nákladovým zariadeniam pripojenie s nelicencovaným pásmom Wi-Fi [1].

1.4.4 ZigBee

Je bezdrátová komunikačná technológia postavená na štandarde IEEE 802.15.4, ktorého sa ujalo medzinárodné spoločenstvo veľkých elektrotechnických firiem, ktoré sa nazvalo ZigBee Alliance a medzi jeho členmi patria aj firmy ako Samsung, Texas Instruments, Philips, AT&T, Cisco, Huawei, Intel. Tento IEEE štandard patrí medzi tých najmladších - bol predstavený ešte len v roku 2004. K jej hlavným prednostiam patrí spoľahlivosť, veľmi nízka spotreba a priaznivá cena. Protokoly ZigBee sú extrémne jednoduché a musia byť spracovateľné aj 8 bitovými kontrolérmi pre najjednoduchšie aplikácie. Navyše sa u zariadení počíta s batériovou energiou a dobou výdrže na úrovni stoviek dní až jednotiek rokov. Celá štruktúra protokolu zaberá len 30 kB pamäte. Signál sa šíri v nelicencovaných pásmach. Globálne pracuje v pásme 2,4 GHz s 16 kanálmi a rýchlosťou až 25 kb/s. V zámorí ďalej využíva pásmo 915 MHz s 10 kanálmi a prenosovou rýchlosťou 40 kb/s, v Európe potom pásmo 868 MHz s jediným kanálom a rýchlosťou redukovanou na 20 kb/s. Na adresovanie jednotlivých zariadení sa používajú binárne kódy s dĺžkou 64 bitov, prípadne v skrátenej (a predpokladá sa, že používanejšej) verzii 16 bitov. 16 bitové adresy umožňujú pripojiť až 65 535 zariadení. Topológia siete ZigBee môže byť principiálne trojdruhová:

- hviezda (star) s centrálnym koordinačným centrom,
- stromová (cluster), ktorá slúži najmä pre predĺženie oznamovacích vzdialeností,
- sieťová (mesh) na zabezpečenie využíva algoritmus f s kľúčom o dĺžke 128 bitov. Je možné použiť zabezpečenie už v MAC vrstve, ak je to vyžadované.

1.4.5 Z-Wave

Z-Wave je bezdrôtová komunikačná technológia s nízkou spotrebou energie určená primárne pre domácu automatizáciu a pre produkty, ako sú ovládače lámp, senzory a mnoho ďalších. Bola optimalizovaná pre spoľahlivé doručenie dát s nízkou latenciou. Používa malé dátové pakety s prenosovou rýchlosťou až 100 kb/s. Využíva typ siete MESH bez nutnosti použitia centrálneho uzla. Je možné ovládať až 232 zariadení.

1.4.6 Sigfox

Sigfox je sieť typu LPWAN zameraná na komunikáciu medzi zariadeniami v rámci internetu vecí. Technológia SigFox bola vyvinutá súkromnou Francúzkou spoločnosťou, ktorá bola založená v roku 2009. Sigfox umožňuje IoT zariadeniam komunikovať lacno, bezpečne a na veľké vzdialenosti pri minimálnej spotrebe energie. Typickými oblasťami stoviek aplikácií siete SIGFOX v Európe sú odpočty vody, elektriny a

plynu, parkovacie senzory, Industry 4.0, SmartCity, zabezpečovacie zariadenia, logistika, sledovanie teplôt pri transporte a uskladňovaní, starostlivosť o seniorov, meranie zrážok a prietokov v záplavových oblastiach. Spoločnosť Sigfox vlastní všetku sieťovú technológiu od serverov až po softvér koncových zariadení, v mnohých prípadoch je samotná spoločnosť Sigfox zároveň aj sieťovým operátorom. V prípade, že chce iný operátor vybudovať sieť Sigfox, musí nevyhnutne spolupracovať so spoločnosťou Sigfox a na jednom území nemôže byť súčasne viac ako jedna sieť. Jednou z výhod tohto prístupu je možnosť pohodlného prechodu zariadenia medzi sieťami. Vďaka transparentnému roamingu zariadenie funguje automaticky vo všetkých Sigfox teritóriách bez ďalších nákladov na užívateľa. Sigfox využíva špeciálnu modulačnú techniku, pomocou ktorej dosahuje veľmi dobrý prenos na veľké vzdialenosti pri nízkych vysielacích výkonoch, čím napomáha k zníženiu celkovej spotreby energie zariadení využívajúcich túto sieť. Sigfox pracuje v ISM pásme 868 MHz. Využíva UNB - Ultra Narrow Band pásmo pre vysielanie iba krátkeho pulzu dát s vysielacím výkonom obmedzeným na 100 mW. Každá správa v dobe prenosu zaberá šírku pásma 100 Hz a je prenášaná rýchlosťou 100 alebo 600 bitov za sekundu. Nevýhodou siete Sigfox je výrazné obmedzenie maximálneho počtu odoslaných správ za deň a veľmi nízka prenosová kapacita v smere prenosu od základňovej stanice ku koncovým bodom siete. Prenos v smere od koncových bodov je však postačujúci pre potreby senzorického bodu, 10 až 1000 bitov za sekundu [37] [39].

1.4.7 LoRA

Technológia Lora, je zaujímavá pre Internet vecí a tiež zariadenia pre vzdialenú signalizáciu a riadenie (Long Range Signaling and Control, LRSC), ktoré budú inštalované na veľkej rozlohe (Wide Area Network) a zároveň si vystačí s malým dátovým tokom, príp. sa od nich ešte očakáva veľmi nízka spotreba (Low Power). Všeobecne sa potom také siete označujú ako LPWAN (Low Power Wide Area Network). Ich ďalšou výhodou je životnosť batérie v zariadeniach, ktorá vystačí na viac rokov fungovanie. LoRa (Long Range) je modulácia patentovaná firmou SEMTECH, ktorá okrem iného využíva kódovanie 4/5, doprednú korekciu chýb a moduláciu Chirp. Protokol LoRaWAN zabezpečuje transparentné zabezpečený prenos dát medzi koncovým zariadením a aplikáciami bežiacich na serveri a späť. O štandardizáciu a rozvoj protokolu LoRaWAN sa stará nezisková organizácia LoRa Alliance, medzi ktorej členov patria desiatky firiem. LoRa bola navrhnutá ako pre európske pásmo 868 MHz, tak pre to americké 913 MHz. Obe pásma majú výhodu a zároveň nevýhodu, že sú voľné a zadarmo. Legislatíva sa pre obe pásma líši, napriek tomu spomínaná technológia dosahuje skvelé výsledky. Brány a koncové zariadenia môžu používať rovnakú frekvenciu pre prenos, ale v rôznych časových úsekoch. Tento koncept je známy ako

TDD. LoraWAN frekvenciu pre Európu sú definované nasledovne:

- LoRaWAN definuje desať kanálov pre Európu. Z toho 8 kanálov sú multidata-rate s rýchlosťou prenosu dát od 250 b/s na 5,5 kb/s.
- Jeden kanál môže pracovať pri vyššej rýchlosti prenosu dát s rýchlosťou 11 kb/s.
- Jeden FSK kanál môže pracovať s rýchlosťou 50 kb/s.

Citlivosť je -136 dB a odolnosť voči rušeniu -16 dB (pod úrovňou šumu), dosah na priamu viditeľnosť 40 km, v mestskej zástavbe okolo 2-4 km. Aby nedošlo k omylu, hardvér a softvér sa pre oba kmitočty líši, avšak aplikačné rozhranie je identické. Keďže LoRa je na rozdiel od Sigfoxu otvorený štandard a zoskupenie hneď niekoľkých firiem a výrobcov, umožňuje individuálnu a flexibilnú kombináciu jednotlivých komponentov a súčastí. Sigfox je naproti tomu kompletné, vopred dané riešenie. LoRa tak ponúka väčšiu voľnosť. V ponuke je hneď niekoľko kompatibilných vysielačov či senzorov od viacerých výrobcov, napríklad senzory od firmy SEMTECH, ktoré obsahujú mimo radu detektorov aj GPS [21] [18].

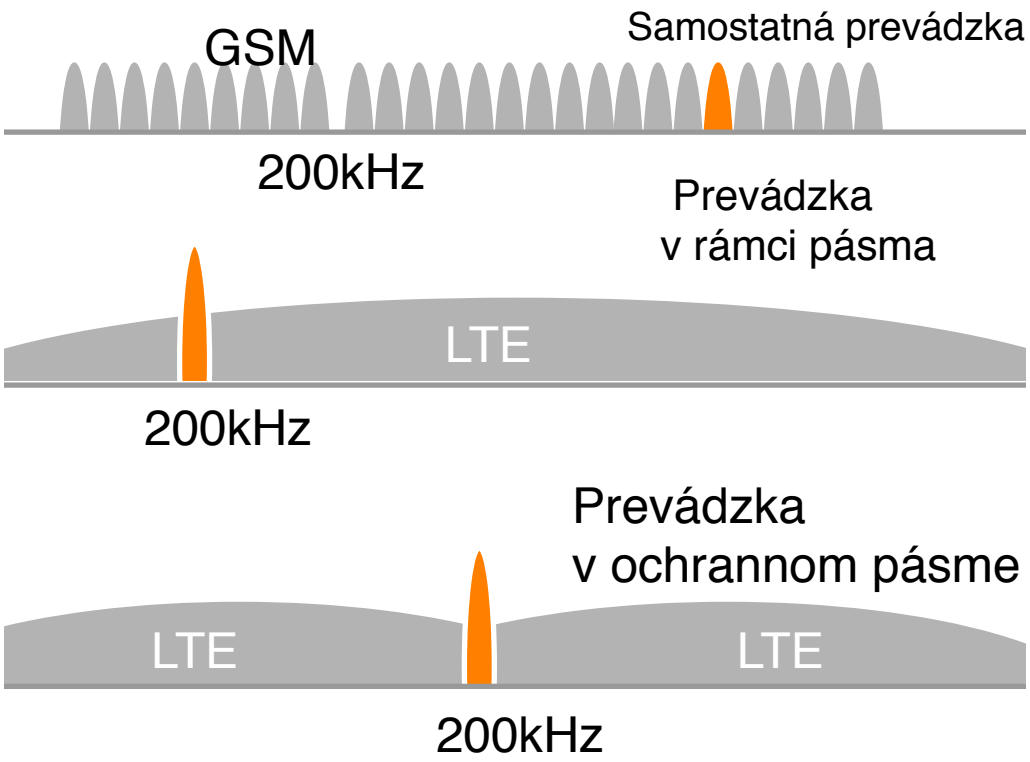
1.4.8 NB-IoT

Narrow Band IoT bezdrôtová úzko-pásmová LPWA technológia špeciálne vyvinutá pre internet vecí. NB-IoT bol špecifikovaný v 13tom vydaní 3GPP v Júny 2016. NB-IoT môže existovať spolu s GSM (globálny systém pre mobilné komunikácie) a LTE (dlhodobý vývoj) v rámci licencovaných frekvenčných pásiem (napr. 700 MHz, 800 MHz a 900 MHz). NB-IoT zaberá šírku frekvenčného pásma 200 KHz, čo zodpovedá jednému zdrojovému bloku v prenosoch GSM a LTE.

Pri tejto voľbe frekvenčného pásma sú možné nasledujúce prevádzkové režimy, ako je znázornené na obrázku 1.3:

- Samostatná prevádzka (Stand-alone operation): možným scenárom je využitie pásiem GSM frekvencií, ktoré sa v súčasnosti používajú.
- Prevádzka v ochrannom pásme (Guard-band operation): využívanie nevyužitých zdrojov blokov v ochrannom pásme dopravcu LTE.
- Prevádzka v rámci pásma (In-band operation): využívanie blokov prostriedkov v rámci nosiča LTE.

NB-IoT umožňuje pripojenie až 100 K koncových zariadení na bunku s možnosťou zvýšenia kapacity pridaním ďalších nosičov NB-IoT. NB-IoT využíva viacnásobný prístup s jedným nosným kmitočtovým rozdelením (FDMA) v uplinku a ortogonálnom FDMA (OFDMA) v zostupnom prepojení a využíva kvadratúrnu modifikáciu kľúčového posunu fázového posunu (QPSK). Rýchlosť prenosu dát je obmedzená na 200 kb/s pre downlink a 20 kb/s pre uplink. Maximálna veľkosť užitočného zaťaženia pre každú správu je 1600 bajtov. Jej dosah je 15 km (164 dB). Ak



Obr. 1.3: Režimy prevádzky pre NB-IoT

priemerné vysielanie nepresiahne 200 bajtov za deň je schopná technológia NB-IoT dosiahnuť životnosť batérie 10 rokov [22].

1.4.9 IQRF

Je to platforma pre bezdrôtovo pripojené zariadenia s nízkou prenosovou rýchlosťou, nízkou spotrebou dát a malým množstvom prenášaných dát. Jej pokrytie signálom dosahuje rádovo desiatky až stovky metrov a využíva sa najviac k prenosu nameraných dát od senzorov, riadení systémov a automatizácií budov. Využíva IQMESH sieťový protokol, ktorý na doručovanie dátových paketov využíva smerovací mechanizmus, ktorý ich preposiela cez ostatné zariadenia v sieti. Zlepšuje tak rozsah, robustnosť a spoľahlivosť a opravuje potencionálne problémy hviezdicovej topológie. Extra nízka spotreba energie je nielen pri uspanom zariadení, rádovo μA, ale taktiež aj pri prijímaní, 15 μA. Do jednotlivých sietí možno pripojiť až 240 zariadení s 240 timi skokmi. Pracuje v bezlicenčnom pásme 868 MHz, 916 MHz alebo 433 MHz. Veľkou výhodou IQRF je kompletné zaobstaranie siete od jednej firmy (od hardwaru až po podporu).

1.4.10 6LoWPAN

6LoWPAN je kombinácia IPv6 a bezdrôtovej osobnej siete s nízkou prenosovou rýchlosťou (LoWPAN). Umožnuje malým zariadeniam s obmedzenou schopnosťou spracovania využiť na bezdrôtový prenos informácii internetový protokol. Uvedený štandard definuje spôsob komprimovania hlavičky IP paketu, segmentuje pakety dlhšie ako jeden rámec štandardu 802.15.4 a zabezpečuje spoluprácu so sieťou internet. Jednoduché zabezpečenie interoperability medzi bezdrôtovou sieťou na báze 6LoWPAN a internetom predurčuje tento štandard na širokú triedu aplikácií, ktorá je dnes populárne označovaná ako Internet vecí [23].

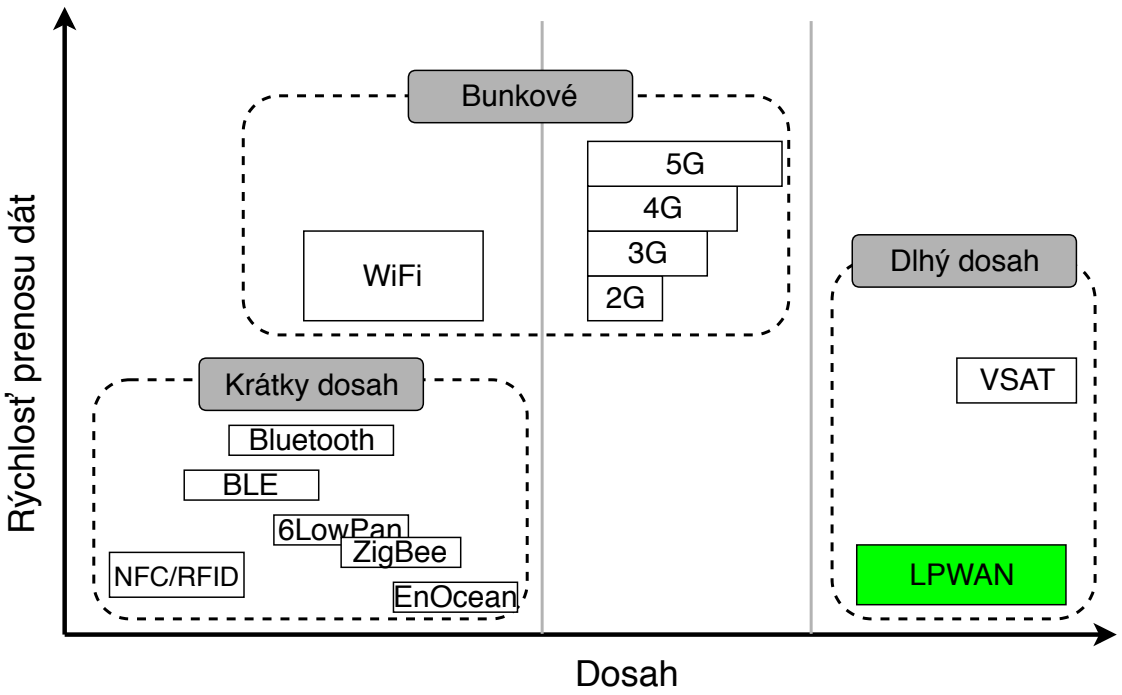
Tab. 1.1: Porovnanie jednotlivých technologií

	Dosah	**Max. rýchlosť prenosu**	**Zabezpečenie**	**Max. počet bitov dat pre 1 správu**
BLE	50 m	1 Mb/s	128-bit AES	20 bytov
NFC	10 cm	106 až 424 kb/s	nie	248 bytov
WiFi	50 m/2,5-19 km	1-250 Mb/s	RC4 / AES	N/A
ZigBee	10–100 m	20-250 kb/s	AES 128 b	82-100 bytov
Z-Wave	100 m	9,6/40/100 kb/s	AES 128 b	9 bytov
Sigfox	50 km/3 km	100 b/s	AES 128 b	12/8 bytov u/d
LoRa	40 km/2-4 km	0,3-50 kb/s	AES 128 b	55-222 bytov
NB-IoT	N/A	50 kb/s	AES 128 b	1600 bytov
6LowPAN	20 m	N/A	AES 128 b	N/A

1.5 Koncové prvky

RFID tag

Radio Frequency IDentification - rádio frekvenčný identifikátor. Je elektronický štítok, ktorý ma za úlohu vymieňať dáta s RFID čítačkou cez rádiové vlny. Skladá sa z antény, ktorá príma a vysiela signál, transceivera umožňuje komunikáciu s čítačkou a transpondéra - obsahuje funkcie, ktoré má samotný štítok plniť. Využívajú sa na identifikáciu a sledovacie účely. Delia sa na aktívne a pasívne. **Pasívny** nemá vlastný zdroj elektrickej energie. Vysielač periodicky vysiela pulzy do okolia. Ak sa v blízkosti objaví pasívny RFID čip, využije prijímaný signál na nabitie svojho napájacieho kondenzátora a odošle odpoveď. **Aktívny** sa používa menej často než pasívny systém RFID. Je zložitejší a drahší, obsahuje zdroj napájania a je schopný sám vysielať svoje identifikácie [31].



Obr. 1.4: Požadovaná rýchlosť prenosu údajov v porovnaní s rozsahom rádiokomunikačných technológií

Technical capabilities	Low Power Wide Area Networks (LPWAN)							Short Range Networks				
	LoRaWAN	Neul	Nwave	SigFox	Weightiess - N	Weightiess - P	Cellular	BLE	WIFI	Tread	ZigBee	Z-Wave
Range (km/m)	2-5 urban; 15 suburban; 45km rural	up to 10km	yes	up to 10km urban; 50km rural	5km	2km	35km GSM; 200km 3G/4G	80m	50m	mesh	100m/ Mesh	30m/ Mesh
Deep Indoor Performance	yes	ISM yes, Whitespace	sub-GHz	yes	yes	yes	no	no	no	no	-	-
Freq: Band	varies, Sub-GHz	yes, depends on base -station	yes	Frequency independent; 868/902MHz	Sub-GHz	Sub-GHz	900/1800/1900/ 2100MHz	2,4GHz	2,4GHz	2,4GHz	915MHz/ 2,4GHz	900MHz
ISM?	yes	yes	no	yes	yes	yes	depends	yes	yes	yes	yes	yes
Fully Bi-Directional	yes, depends on mode	10 . 100kbps	100bps	no	uplink only	yes	yes	yes	yes	-	yes	yes
Data Rate	0,3 - 50 kbps	low	low	10 - 1000bps	30kbps - 100kbps	up to 100kbps adaptive	35-170kbps GSM/ 3 - 10mbps LTE	< 1mbps	600mbps max	-	250kbps	10-100kbps
Power Profile	low	-	yes	low	low	low	Medium	high	high	low	low	low
Authentication	yes	-	yes	yes	yes	yes	high security, back by major telecoms	trused devices problematic	yes	yes	yes	yes
E2E Encryption	yes	-	yes	yes	yes	yes	yes	yes	yes	yes	yes	yes
Over the Air Software Upgrades	yes	-	no	no	no	yes	yes	yes	yes	-	yes	yes
Supports sensors moving between hubs	yes	-	no	no	yes	yes	yes	yes	yes	no	yes, mesh-based	yes, mesh based
Location Aware	yes	-	no	no	no	-	yes	no	yes	-	-	-
Operational Model	Public or private	-	public or private	public	public or private	public or private	public or private	public or private	public or private	private/WIFI/ backbone	public or private	public or private
Standard	LoRaWAN	weightless	weightless	no	Weightiess	Weightiess	GSM, LTE etc.	bluetooth 4.0	IEEE802.11	Thread, based on 6LoWPAN IEEE802.15.4	ZigBee	Z-Wave
Scalability	yes	yes	yes	yes	limited	yes	yes	yes		yes	yes	Limited

Obr. 1.5: Porovnanie IoT technológií LPWAN a sietí krátkeho dosahu

Embedded device

Fráza Embedded system popisuje systém s vlastným výpočtovou jednotkou s možnosťou komunikácie. Je to systém zameraný na poskytovanie jednej alebo málo špecifických funkcií. Embedded zariadeniami môžeme nazývať veľké rozpätie zariadení, napríklad od kalkulačky, PDA, bankomat až po svetelnú signalizáciu a iné. Tieto zariadenia sú dodávané s množstvom špeciálnych procesorov, ktoré sú prispôsobované ich požiadavkám. Na procesory sú kladené nároky ako malé rozmery,pasívne chladenie, nízka spotreba, cena a pod. Pre ich špecifický účel, môžu tvorcovia systému pri návrhu ich optimalizovať pre konkrétnu aplikáciu a tým tak znížiť cenu [13].

System on chip

SoC - Systém na čipe je integrovaný obvod, ktorý integruje všetky komponenty počítača, alebo iného elektronického systému do jedného čipu. Vo všeobecnosti tento čip obsahuje CPU, GPU, severný, niekedy aj južný mostík a komponenty pre konektivitu napríklad pre WiFi alebo GPS. Najväčšími výrobcami takýchto čipov sú Qualcomm, Nvidia, Samsung. V zabezpečenom SoC sú požadované štyri kľúčové funkcie: bezpečné bootovanie, zabezpečená pamäť, kontrola integrity údajov pri spustení a ústredná odpoveď na porušenie bezpečnosti.

Jednočip

Jednočip alebo mikrokontrollér je jednoduchý čip, ktorý umožňuje jednoduchšie výpočetné funkcie a metódy, väčšinou má obmedzenú inštrukčnú sadu. Vykonáva inštrukcie, číta, uchováva informácie, meria čas, poprípade vypína alebo zapína veci a vie mnoho ďalších vecí, záleží na type. Je to integrovaný obvod, ktorý zahŕňa zvyčajne všetko potrebné na to, aby mohol obsiahnuť celú aplikáciu, bez toho aby potreboval ďalšie podporné obvodu. Vyžadujú napájanie vo forme stabilného jednosmerného prúdu. Môžeme ich nájsť v bežných spotrebných veciach ako je mikrovlnná rúra alebo práčka. Je podobný SoC, ale menej sofistikovaný, a často je súčasťou či už SoC alebo embedded systémov [41].

1.6 Hrozby a potencionálne útoky

S veľmi rýchlym budovaním, vývojom internetu vecí je veľmi dôležité si uvedomiť aj veľkú mieru zodpovednosti vyplývajúcej z moci niečo nové vytvárať. Pracujeme so širokým spektrom súkromných informácii, je nutné ich určitým spôsobom chrániť pred rizikami. Medzi najväčšie riziká môžeme zahrnúť útoky na zariadenie s cieľom

znefunkčniť zariadenia, získanie súkromných informácií poprípade získanie finančných prostriedkov. Najväčšou chybou, ktorej sa ľudia často dopúšťajú je popieranie týchto bezpečnostných rizík. Bezpečnosť je tou najdôležitejšou zložkou a hlavným pilierom, na ktorom treba stavať a nebrať to na ľahkú váhu [33].

1.6.1 Typy útokov

Fyzické útoky

Tieto typy útokov manipulujú s hardvérovými komponentami a sú relatívne ťažšie vykonať pretože vyžadujú drahý materiál. Niektoré príklady predstavujú rozbalenie čipu, rekonštrukciu rozvrhnutia, mikro-skúšanie [4].

Útok postranným kanálom

Tieto útoky sú založené na postranných informáciach z kanála, ktoré môžu byť získané zo šifrovacieho zariadenia, čo nie je šifrovaný ani šifrový text, ktorý je výsledkom šifrovacieho procesu. Šifrovacie zariadenia produkujú informácie o časovaní, ktoré sú ľahko merateľné, ožarovanie rôznych druhov, štatistiky spotreby energie a ďalšie. Útoky vedľajších kanálov používajú niektoré alebo všetky tieto informácie na obnovenie kľúča, ktorý zariadenie používa. Je založený na skutočnosti, že logické operácie majú fyzikálne vlastnosti, ktoré závisia od vstupných údajov. Príklady informácií o postranných kanáloch sú časové útoky, útoky analýzy napájania, útoky analýzy chýb, elektromagnetické útoky, environmentálne útoky [4].

Útoky krypto-analýzou

Tieto útoky sú zamerané na šifrový text a pokúšajú sa zlomiť šifrovanie, t.j. nájsť šifrovací kľúč na získanie otvoreného textu, prípadne ak poznáme šifrovaný text a otvorenú správu snažíme sa o nájdenie kľúča pre ďalšie dešifrovanie. Medzi príklady kryptoanalýzových útokov patrí Ciphertext-only útok, Known-plaintext útok, Chosen-plaintext útok, Man-in-the-middle atď [4].

Softvérové útoky

Softvérové útoky sú hlavným zdrojom bezpečnostných zraniteľností v každom systéme. Softvérové útoky využívajú zraniteľnosti implementácie v systéme prostredníctvom vlastného komunikačného rozhrania. Tento druh útoku zahŕňa využívanie pretečenia vyrovnávacej pamäte a používanie programov trójskych koní, červov alebo vírusov na zámerné zavedenie škodlivého kódu do systému [4].

Sieťové útoky

Bezdrôtové komunikačné systémy sú citlivé na útoky na bezpečnosť siete v dôsledku vysielacej povahy prenosového média. V zásade útoky sú klasifikované ako aktívne a pasívne útoky. Príklady pasívnych útokov zahŕňajú monitorovanie a odpočúvanie, analýzu prevádzky, nepriateľské kamufláž atď. Príklady aktívnych útokov zahŕňajú útoky typu Denial of Service, chyba uzla, zachytenie uzla, výpadok uzla, korupcia správ, falošný uzol, útoky smerovania atď [4].

1.6.2 Príklady útokov

Haxposure

Takýmto typom útoku získava útočník citlivé informácie a následne ich zverejňuje na internete. Odhalenie citlivých informácií najmä ak tieto citlivé informácie nesú škodlivé tajomstvá môžu mať devastačné následky pre reputáciu firmy a biznis s tým spojený. Sú známe prípady únikov údajov o používateľoch stránky Ashley Madison, ktorá slúži ako zoznamka pre zadaných. Predpokladom je, že korporátne tajomstvá budú prispievať k zvyšovaniu počtu takýchto útokov.

Takýmto typom útoku bola zasiahnutá aj firma Volkswagen, úniky informácií ohľadom falšovania emisných testov mali nemalý dopad na jej reputáciu. Ide o jednu z najväčších celosvetových firiem, ktoré majú problémy s bezpečnosťou a ich nedostatky sa pohrávajú so zdravým. Takýto druh káuz je určitou motiváciou pre skupinu hackerov, aby pátrali po podobných informáciach [8].

Ransomware

Ide o jeden z najrýchlejšie sa rozvíjajúcich typov útoku. Hlavnou motiváciou hackera použiť tento druh útoku je, že dokáže ho veľmi dobre speňažiť. Je to druh škodlivého kódu, ktorý blokuje prístup k dátam, súborom na zariadení, za ich odblokovanie požaduje nemalé výkupné na svoj účet. Tento typ útoku bol po prvý krát použitý pred 25 rokmi, ale až v dnešnej dobe sa dostáva do popredia a získava na popularite. Jeho vývoj nenarazil doposiaľ na žiadne limity a je predpoklad, že spolu s pribúdajúcimi zariadeniami pripojených k internetu budú vznikať nové rafinované spôsoby [8].

DoS - Denial of Service

Predstavuje pokus o znefunkčnenie a zneprístupnenie počítača, siete, internetovej služby alebo stránky pre jeho používateľov. DoS útoky bránia komunikácii medzi postihnutými používateľmi a zabraňujú im pokračovať obvyklým spôsobom. Jedna

bežná metóda útoku zahŕňa saturáciu cieľového počítača s externými požiadavkami na komunikáciu, aby cieľový počítač nemohol reagovať na legitímny prenos, alebo odpovedal tak pomaly, aby bol účinne nedostupný. Také útoky zvyčajne vedú k preťaženiu servera. Počítače vystavené útokom DoS sa zvyčajne musia reštartovať, aby fungovali správne. Cieľom útokov DoS sú webové servery a cieľom je ich zneprístupniť používateľom po určitú dobu.

1.7 Kryptografické algoritmy využívané v IoT

Šifrovacie algoritmy používajú klúče na šifrovanie a dešifrovanie. Existujú však dve skupiny šifrovacích algoritmov na základe ich kľúča:

- **Asymetrické** šifrovacie algoritmy používajú jeden kľúč pre šifrovanie a jeden kľúč na dešifrovanie. Šifrovací kľúč je verejný a dešifrovací kľúč je súkromný. Týmto spôsobom môže každý, kto má verejný kľúč, šifrovať správy, ale iba vlastník privátneho kľúča je schopný dešifrovať správu.
- **Symetrické** šifrovacie algoritmy používajú ten istý kľúč na šifrovanie a dešifrovanie. Keď je kľúč známy, všetky správy môžu byť dešifrované a nové správy môžu byť šifrovaná. Z tohto dôvodu je mimoriadne dôležité, aby zostal tajný. Symetrické šifry sa delia na dva druhy.
  - **Prúdové symetrické** šifrovacie algoritmy spracovávajú otvorený text po jednotlivých bitoch.
  - **Blokové symetrické** šifrovacie algoritmy rozdelia otvorený text na bloky rovnakej veľkosti a doplní vhodným spôsobom posledný blok na danú veľkosť.

V súčasnosti sú preferované hybridné systémy na zabezpečenie bezpečnosti. Pri výmene kľúčov sa používa asymetrické šifrovanie kľúčov, pretože tieto vyžadujú iba verejne známy šifrovací kľúč, ktorý sa má vymieňať. Obsah posielanej správy je teda známy iba odosielateľovi verejného kľúča. Vymenené kľúče sú však symetrické kľúče. Tieto kľúče slúžia na šifrovanie a dešifrovanie správ medzi oboma stranami. Symetrické kľúče boli vybraté pre šifrovanie aktuálnej správy, pretože tieto algoritmy sú menej nákladné z hľadiska zdrojov v porovnaní s asymetrickými šifrovacími algoritmami kľúča. Treba tiež poznamenať, že dĺžka kľúča prispieva k bezpečnosti údajov. Ak je kľúč príliš krátky, potom je možné ho získať v značnom čase, napríklad útokom hrubou silou. V súčasnosti je algoritmus považovaný za bezpečný podľa NIST specifikácie [27], ak má aspoň silu 112 b . To znamená, že jediné známe útoky na získanie kľúča algoritmu majú zložitosť rovnú alebo väčšiu ako 2112 b [5].

V tejto podkapitole sú popísané základné kryptografické šifry a módy blokových šifier, ktoré sa využívajú v IoT.

Operačné módy blokových šifier

Z bezpečnostného dôvodu používanie operačných módov blokových šifier je opodstatnené. Ak šifrujeme s rovnakým tajným kľúčom viackrát rovnaký blok otvoreného textu, tento získaný šifrovaný text bude rovnaký. Z tohoto dôvodu sa zaviedli operačné módy blokových šifier, taktiež riešia aj ďalšie nedostatky blokových šifier. Je už na používateľovi čomu sa snaží predchádzať a čoho sa snaží dosiahnuť. Následne sme vybrali základné operačné módy a tie, ktoré sa používajú v IoT.

ECB (Electronic Codebook) - Najjednoduchší režim šifrovania je režim elektronickej kódovej knihy. Správa je rozdelená na bloky a každý blok je šifrovaný oddelene.

Nevýhodou tejto metódy je nedostatok difúzie. Pretože ECB zašifruje rovnaké bloky otvoreného textu do identických šifrových blokov, nezaručí tak dobre skrytie vzoru údajov. V niektorých zmysloch neposkytuje dôvernosť správ a vôbec sa neodporúča používať v kryptografických protokoloch.

Výrazný príklad miery, do akej môže ECB nechávať štruktúru dát vo formáte šifrovaného textu v šifrovanom texte, sa dá vidieť vtedy, keď sa režim ECB používa na zašifrovanie bitmapového obrazu, ktorý využíva veľké plochy s jednotnou farbou. Zatiaľ čo farba každého jednotlivého pixelu je zašifrovaná, celkový obraz môže byť stále rozoznateľný ako vzor identicky zafarbených obrazových prvkov v pôvodných pozostatkoch v šifrovanej verzii.

CBC (Cipher Block Chaining) - Zreťazenie šifrového textu je v súčasnej dobe najpoužívanejším operačným módom blokových šifier. Každý blok otvoreného textu sa v ňom najprv modifikuje predchádzajúcim blokom šifrového textu (spätná väzba), a až potom sa šifruje. V prípade CBC sa jedná o XORovanie bloku otvoreného textu s predchádzajúcim zašifrovaným blokom. Prvý blok otvoreného textu je modifikovaný náhodnou, tzv. inicializačnou hodnotou - vektorom (initializing value, IV), ktorá je vysielaná pred vlastným šifrovým textom, podobne ako u prúdových šifier. Pretože šifrový text by mal byť náhodný, stáva sa následne modifikovaný otvorený text tiež náhodným. To odstraňuje nevýhody modu ECB.

Týmto spôsobom bežný šifrový blok závisí na celom predchádzajúcom otvorenom texte z dôvodu zreťazenia tejto závislosti cez predchádzajúce šifrový text. Nevýhodou (z hľadiska difúzie a útokov) a súčasne výhodou (z hľadiska samo-synchronizácie) je, že táto závislosť sa do bežného šifrového bloku zavádza iba prostredníctvom predchádzajúceho šifrového bloku.

CTR (Counter Mode) - Čítačový modus zavádza tzv. countery. Je v princípe veľmi podobný módu OFB, taktiež prevádza blokovú šifru na synchrónnu prúdovú šifru. Odstraňuje problém s neznámou dĺžkou periódy hesla, pretože tu je dĺžka periódy hesla daná vopred, a to periódou čítača. Bloková šifra ako bijektivne zobra-

zenie zobrazí rozdielne hodnoty čítača na rozdielne hodnoty blokov hesla, čo zaistí maximálnu periódu tejto heslové postupnosti.

CTR taktiež využíva inicializačnú hodnotu IV, ktorá se načíta do vstupného registra (čítača) T. Po jeho zašifrovaní vzniká prvý blok hesla. Potom dôjde k aktualizácii čítača T, najčastejšie pričítaním jednotky (odtiaľ názov módu) a ku generovaniu ďalšieho bloku hesla. Heslo se môže využiť v plnej šírke bloku alebo iba jeho b < N bitov. CTR šifrovanie je paralelizovateľné.

CCM (Counter with CBC-MAC) - Tento mód kombinuje counter mód a Cipher Block Chainning-Message Authentication Code (CBC-MAC). Jeho funciou je zabezpečiť spoľahlivosť a autenticitu dát počas prenosu dát. Zakladá si na symetrickej blokovej šifre dĺžky 128 bitov. Pre algoritmus CCM je potreba 3 druhy dát:

- Otvorený text (P) - dáta, ktoré chceme šifrovať.
- Pridružené dáta (A), ktoré sú autentizované, ale nie sú šifrované.
- Unikátna hodnota - nonce (N), je pridelený k P a A.

Nonce musí byť unikát, nemôže byť použitý viackrát ten istý pod rovnakým kľúčom. Pridružené dáta môžu byť prázdny reťazec. Je potreba vstupné dáta naformátovať pred samotným šifrovaním.

CCM vyžaduje dve blokové šifrovacie operácie bloku na každom bloku šifrovanej a autentizovanej správy a jedno šifrovanie na každom bloku pridružených autentifikovaných dát.

GCM (Galois Counter Mode) - Zabezpečuje dôvernosť a autenticitu dát s použitím pridružených dát. GCM je režim s vysokým výkonom, ktorý ponúka paralelizáciu. Režim prijíma inicializačné vektory ľubovoľnej dĺžky, čo zjednodušuje požiadavku, aby všetky IMS boli odlišné.

Overenie správ (prostredníctvom GMAC / GHASH) sa vykonáva na šifrovanom texte. (Toto je žiaduce po väčšinu času.) Môžme si zmieniť, že vo väčšine implementácií sa kontrola autentizácie a dešifrovanie dochádza paralelne z dôvodov výkonu. Výkonnosť stojí jednu operáciu AES a jednu operáciu GHASH na blok (GHASH je všeobecne rýchlejší ako AES, takže GCM je rýchlejší).

Vstupom sú tri druhy dát:

- otvorený text (P)
- pridružené dáta (A)
- inicializačný vektor (IV)

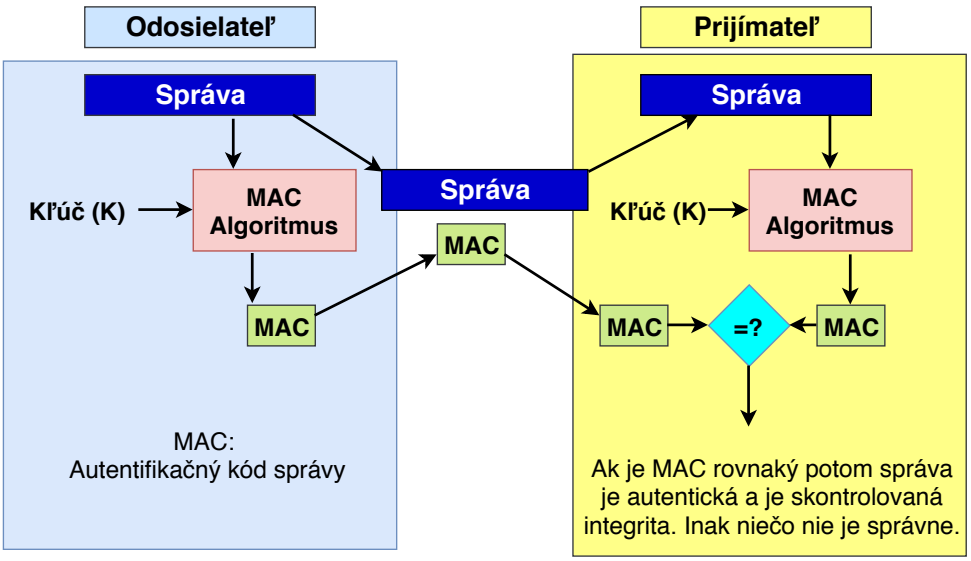
Vstupné dáta by mali spĺňať tieto požiadavky dĺžky v bitoch:

- dĺžka $P \leq 2^{39} - 256$
- dĺžka $A \leq 2^{64} - 1$
- $-1 \leq$ dĺžka $IV \leq 2^{64} - 1$

Dĺžka P, A aj IV by mala byť násobkom 8 a nevyhnutnou podmienkou bezpečnosti je, že pod tým istým kľúčom nebude viackát použitý ten istý IV.

1.7.1 MAC - Message authentication code

Autentizačný kód správy je ďalším módom blokovej šifry, ktorý rieši práve zaistenie neporušenosti dát. Kryptografická funkcia podobná hashovacím funkciám, rozdiel je však v tom, že funkcia nie je iba výsledkom zpracovánia dát ale aj kľúča. Je to krátka časť informácie používaná k autentizácií správy. Teda pre potvrdenie, že správa prišla od uvedeného zdroja a nebola zmenená. Hodnota MAC chráni integritu dát aj ich autentičnosť tým, že povolí overovateľom, ktorí majú aj tajný kľuč, zistiť prípadné zmeny v obsahu správy. Autentizačná funkcia A produkuje autentizačný kód h správy Z, ktorý je závislý na použitom tajnom kľúči K: $h{=}A(Z, K)$. MAC je krátky kód, ktorý vznikne spracovaním správy s tajným kľúčom, ktorý by mal byť iný ako ten, ktorý je použitý k šifrovaniu správy. Výpočet MAC prebieha tak, že sa správa akoby šifruje v móde CBC s nulovým inicializačným vektorom, pričom priebežný šifrovaný text sa neodosiela nikde. MAC je potom tvorený posledným blokom šifrovaného textu, pričom je možné ešte jedno prídavné šifrovanie naviac. Z výsledného bloku sa obvykle berie iba určitá časť o dĺžke potrebnej k vytvoreniu odolného zabezpečeného kódu. Výhodou kódu MAC je skutočnosť, že útočník nedokáže tento kód vytvoriť ani overiť, pretože nepozná tajný kľúč K.



Obr. 1.6: Príklad MAC

V príklade na obrázku 1.6 správa odosielateľa prechádza cez MAC algoritmus na vytvorenie MAC dátovej značky. Správa a značka MAC sa potom posielajú k prijímateľovi. Prijímateľ postupne spúšťa kontrolu. Kontroluje časť správy prenosu pro-

stredníctvom rovnakého MAC algoritmu pomocou toho istého kľúča, pričom produkuje druhú MAC dátovú značku. Prijímateľ potom porovná prvú MAC značku prijatú v prenose s druhou vygenerovanou značkou MAC. Ak sú identické, prijímač môže bezpečne predpokladať, že správa nebola počas prenosu zmenená alebo neoprávnená (integrita údajov).

Aby však prijímač mohol detektovať opakované útoky, samotná správa musí obsahovať údaje, ktoré zabezpečujú, že tá istá správa môže byť odoslaná iba raz (napr. Časové razítko, poradové číslo alebo použitie jednorazovej MAC). V opačnom prípade by útočník mohol - bez toho, aby pochopil jeho obsah - túto správu zaznamenať a neskôr ju prehrať, čo bude mať rovnaký výsledok ako pôvodný odosielateľ.

1.7.2 Advanced Encryption Standard

Jedná sa o symetrickú blokovú šifru, ktorá slúži k šifrovaniu blokov dát dĺžky 128 bitov. Symetrické šifry sú známe tým, že kľúč, ktorý sa používa pre šifrovanie dát sa používa aj pre ich dešifrovanie. Šifrovací kľúč sa líši od typu AESu a je dlhý 128, 192 alebo 256 bitov. Táto šifra má taktiež nízke hardvérové nároky a je jednoduchá na implementovanie. Pri šifrovaní dát sa najprv vykoná inicializácia, pri ktorej dochádza k vytvoreniu prvého podkľúča. Ďalej prechádza algoritmus týmito krokmi [2]:

1. Zámena bitov
2. Prehodenie riadkov
3. Kombinovanie stĺpcov
4. Pridanie podkľúča

Tieto kroky sa vykonávajú 10 krát pri 128-bitovom kľúči, 12 krát pri 192-bitovom kľúči a 14 krát pri 256-bitovom kľúči pričom posledná iterácia sa vykonáva už bez kombinovania stĺpcov. Na konci vzniknú zašifrované dáta, ktoré sú nahraté do úložiska pomocou IoT zariadenia. Tieto dáta sa z úložiska dajú znova načítať pomocou inverzného algoritmu.

Najprv prebehne inicializácia pri ktorej sa vytvorí prvý podkľúč a po nej prebiehajú nasledujúce kroky [2]:

1. Inverzná zámena bitov
2. Inverzné prehodenie riadkov
3. Inverzné kombinovanie stĺpcov
4. Inverzné pridanie podkľúča.

Zmienené kroky sa opakujú v rovnakom počte ako pri šifrovaní a znova to záleží od veľkosti šifrovacieho kľúča. Pred odoslaním správy musia obe strany disponovať rovnakým symetrickým kľúčom, ktorý si musia vymeniť. Na výmenu sa zvykne používať kryptografický protokol Diffie-Hellman. Po výmene je už možná bezpečná

komunikácia. Správa je teda najprv zašifrovaná šifrovacím algoritmom AES, potom je odoslaná cez nezabezpečený kanál a po prijatí je dešifrovaná pomocou rovnakého šifrovacieho kľúča, ktorým bola zašifrovaná ale už pomocou reverzného algoritmu AES [2].

1.7.3 ChaCha20

ChaCha20 je prúdová šifra, ktorú navrhol D. J. Bernstein. Je to zdokonalenie algoritmu Salsa20 a používa kľúč s 256 bitmi. ChaCha20 postupne volá blokovú funkciu ChaCha20 s rovnakým kľúčom a nonce a s postupne sa zvyšujúcimi parametrami blokového počítadla. ChaCha20 následne serializuje výsledný stav napísaním čísiel v malom-endiánskom poradí a vytvára kľúčový blok.

Spojenie kľúčových blokov z nasledujúcich blokov tvorí kľúčový prúd. Funkcia ChaCha20 potom vykoná XOR tohto kľúčového prúdu a otvoreného textu. Alternatívne môže byť každý kľúčový prúdový blok predbežne vytvorený ďalší blok, čím sa ušetrí nejaká pamäť. Neexistuje žiadna požiadavka, aby bol otvorený text celočíselný násobok 512 bitov. Ak existuje extra kľúčový prúd z posledného bloku, bude zničený. Špecifické protokoly môžu vyžadovať, aby otvorený text a šifrovaný text mali určitú dĺžku. Takéto protokoly musia špecifikovať, ako je otvorený text vyplnený a koľko výplne dostane. Vstupy do ChaCha20 sú:

- 256-bitový kľúč.
- 32-bitové počiatočné počítadlo. Môžete ho nastaviť na ľubovoľné číslo, ale zvyčajne bude nula alebo jedna. Je rozumné používať jeden, ak používame nulový blok pre niečo iné, ako je generovanie jednorazového autentizačného kľúča, ako súčasti algoritmu AEAD.
- 96-bitový nonce. V niektorých protokoloch sa to nazýva inicializačný vektor.
- Otvorený text s ľubovoľnou dĺžkou.

Výstup je šifrovaná správa alebo šifrovaný text rovnakej dĺžky [26].

1.7.4 HC-128

Prúdová šifra HC-128 je odľahčená verzia šifry HC-256 pre 128 bitovú bezpečnosť. HC-128 je jednoduchá, bezpečná, softvérovo efektívna šifra a je voľne dostupná. Skladá z dvoch tajných tabuliek, každá z nich pozostáva z 512tich 32 bitových slov. V každom kroku aktualizujeme jeden prvok tabuľky s funkciou nelineárnej spätnej väzby. Všetky prvky týchto dvoch tabuliek sú aktualizované každých 1024 krokov. V každom kroku sa vygeneruje jeden 32-bitový výstup z funkcie nelineárneho filtrovania výstupu. HC-128 je vhodný pre moderné (a budúce) superskalárne mikroprocesory. Závislosť medzi operáciami v systéme HC-128 je veľmi nízka: tri kroky sa

dajú vypočítať paralelné; v každom kroku môžu byť spätnoväzobné a výstupné funkcie vypočítané paralelne. Vysoký stupeň paralelnosti umožňuje HC-128 pracovať efektívne na moderných procesoroch [32].

1.7.5 DSA

Je založený na probléme výpočtu diskrétneho logaritmu, je podobný algoritmu ElGamat. V prvej fáze algoritmu sa generujú tri verejné parametre dostupné pre skupinu užívateľov. Sú to parametre *p, q* a *g*. Prvočíslo *p* sa vyberá v rozmedzí 512-1024 bitov, pričom je vždy násobkom čísla 64. Prvočíslo *q* má dĺžku 160bitov a je deliteľom čísla (*p*-1). Číslo *g* sa vyjadruje v tvare $g = h^{(p-1)/q}$, kde *h* je celé číslo v rozsahu 1 až (*p*-1) a tiež pre *h* platí: $h^{(p-1)/q} \bmod p > 1$.

V druhej fáze DSA sa generuje verejný a súkromný kľúč odosielateľa. Súkromný kľúč SK_a, tvorí náhodné, resp. pseudonáhodné číslo *x* v rozmedzí 1 až (*q*-1). Verejný kľúč VK_a tvorí číslo *y*, ktoré dostaneme zo súkromného kľúča podľa vzťahu $y = g^x \bmod p$. Výpočet *y* pre dané *x* a *g*, resp. *p* je relatívne ľahký a zároveň výpočet *x* z *y* je ťažký, lebo *x* je diskrétnym logaritmom *y* so základom *g* v module *p*.

Digitálny podpis tvorí dvojica hodnôt *r, s*, ktorá je funkciou prvkov (*p,q,g*) súkromného kľúča *x*, hešovacieho kódu *h = H(M)* a pseudonáhodného čísla k ($0<k<q$), ktoré je jedinečné pre každý podpis a musí byť utajené. Potom $r = (g^{\mathrm{k}} \bmod \mathrm{p}) \bmod q$ a $s = (\ k^{-1}\ (H(M)) + x\ r)) \bmod q$. Používa sa hešovacia funkcia SHA-1.

Verifikácia digitálneho podpisu pozostáva z výpočtu parametrov *w*, u_1, u_2 a v z prijatých verzií *M',r',s'*, podľa vzťahov $w = (s')^{-1} \bmod q$, $u_1 = (H(M")w) \bmod q$, $u_2 = (r'w) \bmod q$, $v = ((g^{u1} y^{u2})) \bmod p$. Platnosť podpisu potvrdzuje rovnosť $v = r'$ [44].

1.7.6 ECDSA

Je analógiou ku algoritmu DSA. Je to široko štandardizovaná schéma na báze eliptických kriviek. Eliptické krivky majú viacero výhod oproti RSA a DL schémam akou je DSA a pod. Je to predovšetkým absencia totálnou skúškou a dostupná bitová dĺžka v rozmedzí 160 - 256 bitov, ktorá poskytuje ekvivalentnú bitovým dĺžkam 1024 - 3072 bitov algoritmu RSA či DL schémam. Kratšia bitová dĺžka ECC má často za následok urýchlenie doby vykonávania a použitie kratších podpisov. Kvôli týmto dôvodom bol systém ECDSA štandardizovaný v USA Americkým národným štandardizačným inštitútom (ANSI) v roku 1998.

Pozostáva z troch základných krokov:

- Generovanie kľúčov odosielateľa.
- Generovanie digitálneho podpisu.
- Verifikácia digitálneho podpise.

Algoritmus ECDSA má nasledovné spoločné črty s algoritmom DSA:

- DSA a ECDSA sú založené na algoritme digitálneho podpisu ElGamal a používajú identickú rovnicu na výpočet parametra $s = (k^{-1} (H(M)) + d\ r))$ mod n.
- Používajú množinu parametrov, ktoré sú označené ako systémové parametre. V algoritme DSA sú to p, q, resp. g a v algoritme ECDSA sú to parametre E,P resp. n. Určenie systémových parametrov je výpočtovo náročné. Po vygenerovaní súkromného kľúča, je relatívne ľahké generovať verejný kľúč.
- Používajú hašovaciu funkciu SHA-1, ktorá sa dá do budúcna nahradiť inou.

Rozdielom medzi ECDSA a DSA je výpočet hodnoty r a v digitálnom podpise (r,s). Tento krok zahŕňa operácie na špecifickej eliptickej krivke s použitím dočasného kľúča k: $r = x1$ mod n, $(x1,x2) = xP$. Výpočet hodnoty s sa používa statický privátny kľúč d: $s = (k^{-1} (H(M)) + d\ r))$ mod n.

Generovanie digitálneho podpisu ECDSA. Vstupom sú skupinové parametre $D = (q,FR,S,a,b,P,n,h)$, privátny kľúč d a správa M. Najprv sa vyberie náhodné celé číslo k v rozsahu od 1 do (n-1). Číslo k sa vyskytuje pri výbere práve raz. Ďalej sa vypočíta $kP=(x_1, y_1)$,x_1 sa konvertuje na celé číslo $\overline{x_1}$ a $r = \overline{x_1}$ mod n. Ak sa $r = 0$, zvolí sa iné k. Nasleduje výpočet hašovacieho kódu správy $e = H(m)$. H je hašovacia funkcia (SHA-1), ktorej hešovací kód nemá bitovú dĺžku väčšiu ako n (ak to nie je splnené, potom je hešovací kód skomolený). Hodnota s sa vypočíta: $s = k^{-1}$ $(e + d\ , r)$ mod n. Ak je $s = 0$, zvolí si iné číslo k. Výstupom je podpis v tvare (r,s).

Verifikácia digitálneho podpisu ECDSA. Vstupom sú skupinové parametre $D = (q,FR,S,a,b,P,n,h)$, verejný kľúč Q, správa M a digitálny podpis (r,s). Výstupom bude buď akceptácia alebo zamietnutie podpisu. Verifikuje sa, či r a s sú celé čísla z intervalu (l, n-1). Ak verifikácia zlyhá, podpis sa zamietne. Ďalej sa vypočíta hešovací kód $e = H(M)$. Hodnota w sa vypočíta $w = s^{-1}$ mod n. Hodnoty u_1 a u_2 sa vypočítajú $u_1 = e{\cdot}w$ mod n, $u_2 = r{\cdot}w$ mod n. Následne sa vypočíta súčet $X = u_1{\cdot}P + u_2{\cdot}P$. Ak je rovné ∞ podpis sa zamietne. Na konci sa konvertuje súradnica x_1 na celé číslo $\overline{x_1}$ a vypočíta sa $v = \overline{x_1}$ mod n. Ak sa $v = r$, potom je podpis prijatý a ak nie, je zamietnutý [11].

1.7.7 RSA

Tento algoritmus bol publikovaný v roku 1978 a je pomenovaný po jeho troch autoroch, ktorými sú Rivest, Shamir a Adleman. Jedná sa o asymetrickú šifru, ktorá používa verejný a súkromný kľúč. Bezpečnosť tohto algoritmu je postavená na probléme rozloženia veľkého čísla na súčin prvočísel (faktorizácia).

Ak chcú dve strany medzi sebou komunikovať, musia sa riadiť nasledujúcim postupom, ktorým si každá strana vygeneruje verejný a súkromný kľúč :

- Užívateľ si zvolí dve náhodné prvočísla p a q,
- spočíta si ich súčin $n = p.q$,
- spočíta hodnotu Eulerovej funkcie pomocou vzorca $\Phi\ (n) = (p\text{-}1).(q\text{-}1)$
- zvoli si celé číslo označené ako e, tak aby platilo $1 \leq e \leq \Phi(n)$ a zároveň s $\Phi(n)$ nesúdeliteľné,
- vypočíta si číslo označené písmenom d tak, aby platilo $de \equiv 1 \pmod{\Phi(n)}$, pričom symbol $\equiv$ označuje ekvivalenciu zvyškových tried [44].

Po vykonaní týchto krokov dostávame verejný a súkromný kľúč. Verejným kľúčom je dvojica (n,e) pričom n sa označuje ako modulo a e ako šifrovací exponent. Súkromný kľúč je dvojica (n,d), kde n označujeme znova ako modulo a d je dešifrovací exponent. Verejný kľúč posiela užívateľ druhej strane, zatiaľ čo súkromný kľúč zostáva utajený.

Pre komunikáciu je potrebné, aby si odosielateľ zistil verejný kľúč prijímateľa. Po zistení verejného kľúča odosielateľ zašifruje svoju správu podľa vzorca $c = (m^e \bmod n)$ a zašifrovanú správu odošle prijímateľovi. Prijímateľ si po prijatí správy zistí verejný kľúč odosielateľa a správu dešifruje podľa vzorca $m = (c^d \bmod n)$ [44].

1.7.8 Diffie-Hellman

Tento princíp je založený na cyklickej grupe G, v ktorej vystupuje veľmi ťažko riešiteľný problém diskrétneho logaritmu DLP. Zadefinujeme si pole Z_p, kde p je dostatočne veľké prvočíslo a g, ktoré je generátorom pola Z_p^*. Hodnoty p a g sú verejné. Majme účastníkov komunikácie m_1 a m_2 . M_1 si zvolí náhodné číslo a_1, ktoré vyberie z intervalu $< 1, p-2 >$ a vypočíta $b_1 = g^{a1} \bmod p$ a pošle b_1 účastníkovi m_2. Ten spraví to isté ako m_1 a pošle b_2 účastníkovi m_1. Po prijatí b_1 a b_2 môžu účastníci vypočítať spoločný súkromný kľúč. $SK = b_2^{a_1} = g^{a_1 a_2} = b_1^{a_2} \bmod p$. Potencionálny útočník nevie vypočítať SK, aj keď pozná verejné parametre p a g a odchytí b_1 a b_2. Tretia strana, ktorá dokáže prelomiť DLP na Z_p^*, je schopná poskladať SK. Problém zostrojenia SK z g, p, b_1 a b_2 sa nazýva Diffie-Hellmanov problém (DHP). Je „slabší“ než DLP v tom zmysle, že riešenie DLP vyrieši DHP, ale nie na opak. K dnešnému dátumu nebola publikovaná zmienka o tom, že by niekto prelomil DHP bez vyriešenia DLP [7].

1.7.9 ECDH

Tento algoritmus na výmenu kľúčov je určitá modifikácia Diffie-Hellmana spomenutého vyššie. Algoritmus prebieha v troch krokoch, ktorými sú zistenie verejných prvkov eliptickej krivky, generovanie verejného a súkromného kľúča oboch komunikujúcich a generovanie tajného kľúča pre komunikáciu [11].

V kroku zisťovania základných verejných prvkov eliptickej krivky sa zisťuje aká rovnica je použitá pre definovanie eliptickej krivky a aké sú jej parametre a, b a q. Takisto sa určite bod P na eliptickej krivke, o ktorom musí platiť, že má veľký rád. Ďalším krokom je generovanie súkromného a verejného kľúča účastníkmi komunikácie. Zvolí si náhodné číslo $n_{\mathrm{i}} < n$ a to slúži ako súkromný kľúč. Z jeho hodnoty sa potom vypočíta verejný kľúč $Q_{\mathrm{j}} = n_{\mathrm{i}} \cdot P$. Pre každého účastníka komunikácie stačí generovať dvojicu kľúčov iba jeden krát za predpokladu, že pri nadväzovaní spojenia s inými účastníkmi komunikácie budú zachované rovnaké základné verejné prvky eliptickej krivky [11].

Posledným krokom je generovanie tajného kľúča K pre účely použitia v aktuálne nadviazanej komunikácií. Tento tajný kľúč K sa vypočíta ako súčin vlastného súkromného kľúča a verejného kľúča druhého komunikujúceho. Platí vzťah $K = n_i \cdot Q_{\mathrm{j}}$, kde pre jedného účastníka komunikácie platí, že sa násobí súkromný kľúč s verejným kľúčom druhého účastníka a naopak [11].

2 POROVNANIE BEZPEČNOSTNÝCH SCHÉM V IOT

Kľúčové schémy založené na asymetrickej kryptografii, známej aj ako kryptografia verejného kľúča (PKC - public key cryptography) sa považujú za bežný prístup na vytvorenie bezpečnej komunikácie medzi dvoma (alebo viacerými) stranami. Používajú asymetrické algoritmy a sú široko nasadené v bežnom Internet. Použiteľnosť PKC v rámci internetu vecí má niektoré hlavné nepríjemnosti, čo je náročný výpočet a spotreba energie. Napriek náročným operáciám, vývoj a implementácia PKC v kontexte IoT nikdy nebola zastavená. V skutočnosti nové zlepšenia niekoľkých primitívnych prvkov (tj. ECC, NTRU) naďalej znižujú náklady na kryptografické operácie, takže záujem o PKC je rastúci vzhľadom k obmedzeným zariadeniam.

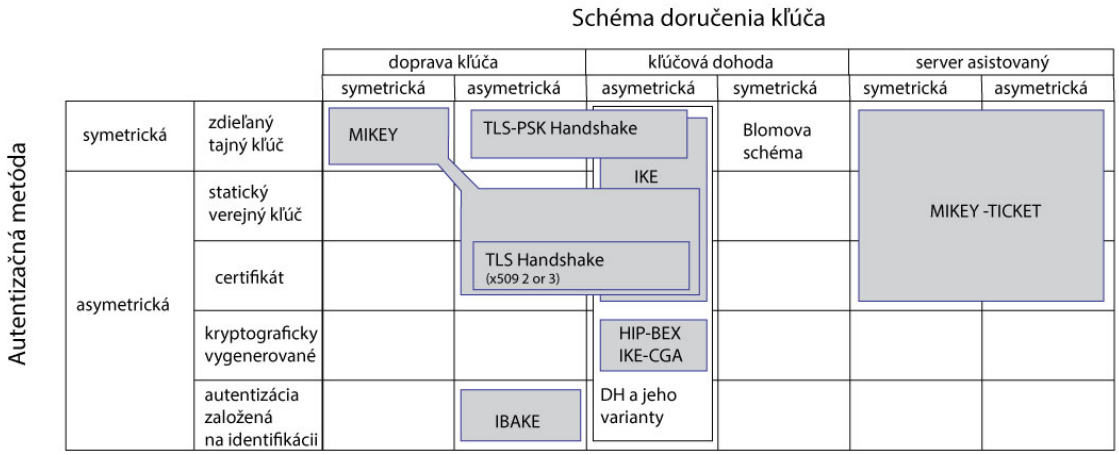
2.1 Celkový prehľad

Táto časť má za cieľ poskytnúť celkový pohľad na existujúce protokoly na ustanovenie kľúča, s cieľom uľahčiť identifikáciu najlepších kandidátov medzi nimi pre zriadenia internetu vecí v oblasti ustanovenia kľúča. Tento globálny pohľad je poskytnutý vo forme tabuľky, do ktorej sú vložené najznámejšie alebo najpoužívanejšie komunikačné protokoly.

Na obrázku 2.1 sú vyobrazené existujúce komunikačné protokoly na ustanovenie kľúča, zakladajú sa hlavne na asymetrickej kryptografii, či už ide o samotnú schému dodávky / dohody, alebo o autentifikačnú metódu implementovanú v protokole. Prázdne bunky v tabuľke sa väčšinou nachádzajú v stĺpcoch symetrickej kľúčovej dopravy a symetrických kľúčových dohodách. Napriek tomu existujú prepravné protokoly na báze symetrické kľúče, avšak v podstate pozostávajú z protokolov na ustanovenie kľúča, ktoré nie sú plne kvalifikované ako protokoly na ustanovenie kľúča. Do stĺpca je zahrnutý iba protokol MIKEY, pretože sa všeobecne používa na distribúciu kľúčov relácie z dlhodobých zdieľaných kľúčov. Protokoly o symetrických kľúčových dohodách nie sú zvyčajné a vyžadujú zložité nastavenie (predbežná distribúcia).

2.1.1 Špeciálne požiadavky na ustanovenie kľúča v IoT

V tejto časti sa skúmajú špecifické požiadavky, ktoré sa týkajú identifikácie protokolu na ustanovenie kľúča internetu vecí. Tieto požiadavky spadajú do troch hlavných kategórií: tie, ktoré súvisia s plnením bezpečnostných požiadaviek; tie, ktoré súvisia s prenikavosťou; tie, ktoré súvisia s efektívnosťou.



Obr. 2.1: Klasifikácia protokolov na ustanovenie kľúča podľa schémy kľúčových dodávok a spôsobu autentifikácie s hlavnými komunikačnými protokolmi na ustanovenie kľúča.

Bezpečnosť

Bezpečnosť v kontexte internetu internetu zahŕňa komunikáciu typu end-to-end. Decentralizovaná a obojsmerná komunikačná paradigma IoT tiež vylučuje definíciu rolí statických klientov a serverov: v závislosti od kontextu je očakávané, že uzol IoT bude konať alternatívne ako klient a ako server. Tieto úvahy sa premietajú do dvoch bezpečnostných požiadaviek. Na jednej strane by sa mala zabezpečiť bezpečnosť medzi koncami. Znamená to, že prístup k vygenerovanému kľúču by mali mať iba dvaja účastníci zapojení v protokole párovú výmenu kľúčov. Na druhej strane sa musí zabezpečiť vzájomná autentizácia. Dvaja komunikujúci, ktorí si medzi sebou vytvoria kľúč, by mali medzi sebou navzájom autentizovať a viazať vygenerovaný kľúč na svoju identitu [36].

Všadeprítomnosť

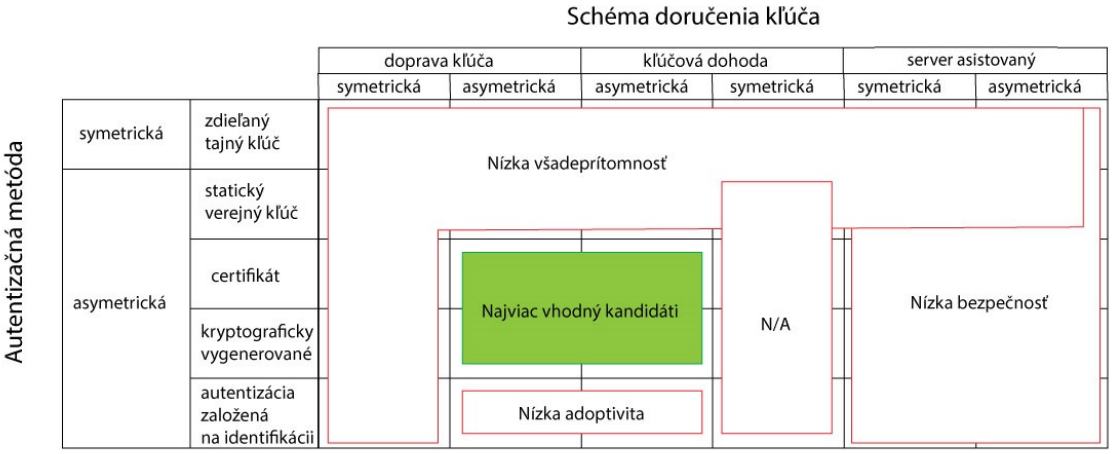
Kvalifikovaním internetu vecí ako všadeprítomného sa možno odvolať na jeho predpokladanú univerzálnosť ako na komunikačnú sieť prepájajúc oveľa viac uzlov než dnešný internet. Priestupnosť kladie dodatočné požiadavky protokolu na ustanovenie kľúča pre internet vecí. Najmä je veľmi nepravdepodobné, že dva uzly, ktoré si želajú vytvoriť kľúč medzi sebou, môžu využiť predtým existujúci bezpečnostný vzťah založený na dlhodobých zdieľaných tajomstvách alebo statických verejných kľúčoch. Z tohto dôvodu by mali byť navrhnuté dynamické asymetrické schémy dodávania kľúčov a autentifikačné metódy pri navrhovaní protokolu na ustanovenie kľúča IoT [36].

Efektívnosť

Účinnosť sa vždy musí brať do úvahy pri navrhovaní nového protokolu. Štyri kritériá sú osobitne dôležité pri posudzovaní účinnosti kryptografického protokolu: počet vymieňaných správ, potrebná šírka pásma, zložitosť výpočtov a možnosť predbežných výpočtov. Význam týchto kritérií sa zvyšuje pri navrhovaní protokolu, ktorý bude musieť spúšťať uzly s obmedzeným zdrojom s nízkym výpočtovým výkonom, nízkou pamäťou a obmedzenou kapacitou batérie. Celková spotreba energie, vyvolaná výpočtami a výmenami správ, je dobrým ukazovateľom pre tieto uzly. Protokol bude definovaný účinnejší ako druhý, ak získa metrickú hodnotu, ktorá je nižšia ako hodnota druhého protokolu, zatiaľ čo poskytuje rovnakú úroveň zabezpečenia [36].

2.1.2 Zhodnotenie

Z vyššie uvedených požiadaviek môžeme prispôsobiť počiatočnú klasifikáciu protokolu na ustanovenie kľúča, aby sme medzi nimi identifikovali najvhodnejšie pre internet vecí. Výsledky tejto identifikácie sú uvedené na obrázku 2.2. Niektorí kandidáti sú vylúčení z toho dôvodu, že nie sú dostatočne zabezpečený , alebo preto, že by nespĺňali požiadavky týkajúce sa internetu vecí, alebo ich prijateľnosť bola hodnotená ako nízka vzhľadom na ich dnešné použitie.



Obr. 2.2: Zlepšenie klasifikácie protokolov na ustanovenie kľúča.

Obrázok 2.2 sa získal nasledovne. Po prvé, riešenia, ktoré sa spoliehajú na kľúčovú predbežnú distribúciu, boli odstránené, pretože nespĺňali požiadavky na bezpečnosť medzi koncami. Následne sa riešenia založené na symetrickej kryptografii alebo predpokladanej počiatočnej znalosti verejného kľúča vylúčili, pretože nespĺňali požiadavku všadeprítomnosti. Relevantné riešenia pochádzajú zo zelenej oblasti.

2.2 Bezpečnostné porovnanie

Protokol Diffie-Hellman (DH) a jeho varianty sú klasickými príkladmi dohody o asymetrickom kľúči. DH protokoly sa však považujú za nákladné a nevhodné najmä pre obmedzené uzly. Vo všeobecnosti RSA taktiež nepatrí do ľahkého kryptografického systému kvôli veľkej veľkosti kľúča. Vďaka použitiu dvoch veľkých prvočísel a vykonávaniu modulo operácie poskytuje RSA väčšiu bezpečnosť a zachováva súkromie používateľov. Kryptografia eliptických kriviek v porovnaní s algoritmom RSA, ECC vyžaduje menšiu veľkosť kľúča. Ako taká má rýchlu rýchlosť spracovania a vyžaduje menej pamäte. Preto sa uplatňuje na obmedzených zariadeniach, čo vedie k rýchlejšiemu výpočtu v reálnom čase [9].

Bezpečnosť kryptosystémov, ktoré využívajú eliptické krivky je postavená na ťažko riešiteľnom matematickom probléme zvanom problém diskrétneho logaritmu (nad eliptickými krivkami označovaný skratkou ECDLP). Zložitosť nájdenia riešenia problému diskrétneho logaritmu nad eliptickými krivkami je väčšia, než je zložitosť klasického diskrétneho logaritmu v multiaplikatívnej grupe alebo v kryptografii často využívaná zložitosť faktorizácie veľkých (rádovo v stovkách až tisíckach bitov) čísel. Z tohto dôvodu je možné pri zachovaní rovnakej úrovne kryptografickej bezpečnosti voliť kľúče menších dĺžok, než pri iných asymetrických kryptosystémoch ako je napr. RSA, ktoré je založené na faktorizácii veľkých čísel. Najrýchlejšie známe algoritmy umožňujúce riešiť ECDLP ako sú napr. „Pollard's Rho“ a „baby step – giant step“ majú zložitosť riešenia tohto problému odmocninovú, z čoho vyplýva, že veľkosť rádu konečného poľa nad ktorým je definovaná eliptická krivka by mala byť rovná dvojnásobku požadovanej úrovne bezpečnosti. Keď chceme teda dosiahnuť bezpečnosť o veľkosti 128 bitov, tak používaná eliptická krivka by mala byť definovaná nad poľom Fp, kde parameter p predstavuje číslo o veľkosti 2^{256}.

Tab. 2.1: Bezpečtnostné porovnanie pre rôzne algoritmy

Požadovaná úroveň bezpečnosti [b]	Symetrické kryptosystémy [b]	Štandardné asymetrické kryptosystémy [b]	Kryptosystémy na báze eliptických kriviek [b]
80	80	1024	160
112	112	2048	224
128	128	3072	256
192	192	7680	384
256	256	15360	512

Porovnanie dĺžok kľúčov pre jednotlivé typy kryptosystémov pri požadovanej úrovni bezpečnosti prezentuje nasledujúca tabuľka. V tabuľke 2.1 môžeme prehľadne

vidieť odporúčané dĺžky kľúčov pre jednotlivé typy kryptosystémov uvedené v bitoch. Z tabuľky taktiež vyplýva, že rovnakú mieru bezpečnosti vieme s eliptickými krivkami dosiahnuť pri výrazne menšej dĺžke kľúča, než je tomu pri štandardných asymetrických kryptosystémoch a pri dvakrát väčšej dĺžke kľúča, než je tomu pri symetrických kryptosystémoch. Zvolíme si pri symetrickom kryptosystéme napríklad 128 bitovú úroveň bezpečnosti, tak ekvivalentnú bezpečnosť dostaneme s použitím kryptosystému využívajúceho eliptické krivky, ktorý má kľúče dĺžky 256 bitov. Ak však chceme dosiahnuť totožnú bezpečnosť so štandardnými asymetrickými kryptosystémami, musíme zvoliť extrémne veľké kľúče – v tomto prípade až o dĺžke 3072 bitov. To sa samozrejme nepriaznivo prejavuje rastom požiadaviek na výpočtový výkon zariadenia a značným spomalením rýchlosti operácií, ktoré sú využívané pri spracovávaní kľúča.

3 VÝSLEDKY MERANIA NA RASPBERRY PI

Táto kapitola sa zaoberá porovnaním kryptografických algoritmov z hľadiska ich výkonnosti na obmedzenom zariadení. Predstavili sme si vybrané kryptografické primitíva. Následne podrobíme tieto a ďalšie primitíva meraniu výkonnostných parametrov. Pod meraním výkonnostných parametrov budeme v tomto prípade rozumieť meranie počtu cyklov procesora potrebných na vykonanie určitej zvolenej výpočtovej úlohy. Samotné merania budeme samozrejme realizovať pre rôzne konfigurácie kryptosystémov.

Raspberry Pi

Raspberry Pi je počítač o veľkosti kreditnej karty, ktorý dokáže vykonávať mnoho funkcií podobne ako stolný počítač. Medzi tieto funkcie môžeme zaradiť tabuľkové procesy, spracovanie textu a hry. O dostatočný výkon sa stará čip BCM2835, ktorý obsahuje ARM1176JZFS s frekvenciou 700 MHz a VideoCore 4 GPU. Má port 10/100 Ethernet, takže poskytuje aj možnosť práce v internetovej sieti. Dva vstavané USB porty poskytujú pripojenie pre myš a klávesnicu, alebo USB rozbočovač ak je potrebných viac zariadení. Rozmery má 85,60mm x 56mm x 21mm.

Vlastnosti:

- Broadcom BCM 2835 SoC
- 700 MHz základný procesor ARM1176JZF-S
- Broadcom VideoCore IV GPU
- 512 MB RAM
- 2 x porty USB2.0
- Video výstup prostredníctvom kompozitného (PAL a NTSC), HDMI alebo Raw LCD (DSI)
- Audio výstup cez konektor 3,5 mm alebo zvuk cez HDMI
- Úložisko: SD / MMC / SDIO
- 10/100 Ethernet (RJ45)
- Periférne zariadenia nízkej úrovne:
  - 8 x GPIO
  - UART
  - I2C zbernica
  - SPI zbernica s dvoma čipmi
  - + 3,3V, + 5V, GND
- Požiadavky na napájanie: 5V, 700 mA cez zásuvku MicroUSB alebo GPIO
- Podporuje Debian GNU / Linux, Fedora, Arch Linux, RISC OS a ďalšie.

3.0.1 Testovanie časť 1.

Na testovanie bolo použité zariadenie Raspberry Pi s operačným systémom RASPBIAN Wheezy s knižnicou Openssl 1.0.1. Metóda testovania bola zvolená nasledovná s využitím knižnice openssl a parametrom speed a daného algoritmu, pre jednotlivé kryptografické algoritmy bol príkaz spustený 10 krát s náhodným rozmedzím medzi spusteniami testu, jednotlivé behy boli zalogované do jednotlivých súborov, z ktorých bol následne urobený priemer. Výsledné hodnoty je možné vidieť v jednotlivých tabuľkách.

Tab. 3.1: ECDSA

Veľkosť kľúča [bit]	**Typ**	**Podpis [s]**	**Overenie [s]**	**Počet operácií podpisu za 1 s**	**Počet operácií overenia za 1**
160	secp160r1	0,00195	0,00617	514,37	161,96
192	nistp192	0,00239	0,00828	420,06	120,78
224	nistp224	0,00293	0,01096	341,6	91,31
256	nistp256	0,00354	0,01407	281,88	71,11
384	nistp384	0,00696	0,03222	143,83	31,06
521	nistp521	0,01373	0,07153	72,87	13,98
163	nistk163	0,0051	0,01801	195,87	55,55
233	nistk233	0,00966	0,03184	103,5	31,42
283	nistk283	0,01437	0,05798	69,6	17,26
409	nistk409	0,03502	0,12874	28,51	7,77
571	nistk571	0,08267	0,2989	12,1	3,13
163	nistb163	0,00497	0,01925	200,98	52
233	nistb233	0,00979	0,03568	102,18	28,04
283	nistb283	0,01453	0,06476	68,82	15,43
409	nistb409	0,03507	0,14668	28,51	6,82
571	nistb571	0,08294	0,34299	12,07	2,9

Tab. 3.2: DSA

Veľkosť kľúča [bit]	**Podpis [s]**	**Overenie [s]**	**Počet operácií podpisu za 1 s**	**Počet operácií overenia za 1**
512	0,002442	0,002342	409,42	427,1
1024	0,006978	0,007261	143,42	137,7
2048	0,024364	0,026191	41,03	38,19

Tab. 3.3: RSA

Veľkosť kľúča [bit]	**Podpis [s]**	**Overenie [s]**	**Počet operácií podpisu za 1 s**	**Počet operácií overenia za 1**
512	0,0023691	0,000219	422,14	4569
1024	0,012313	0,000649	81,22	1542
2048	0,080411	0,002309	12,39	433,2
4096	0,571667	0,00877	1,72	114

Tab. 3.4: ECDH

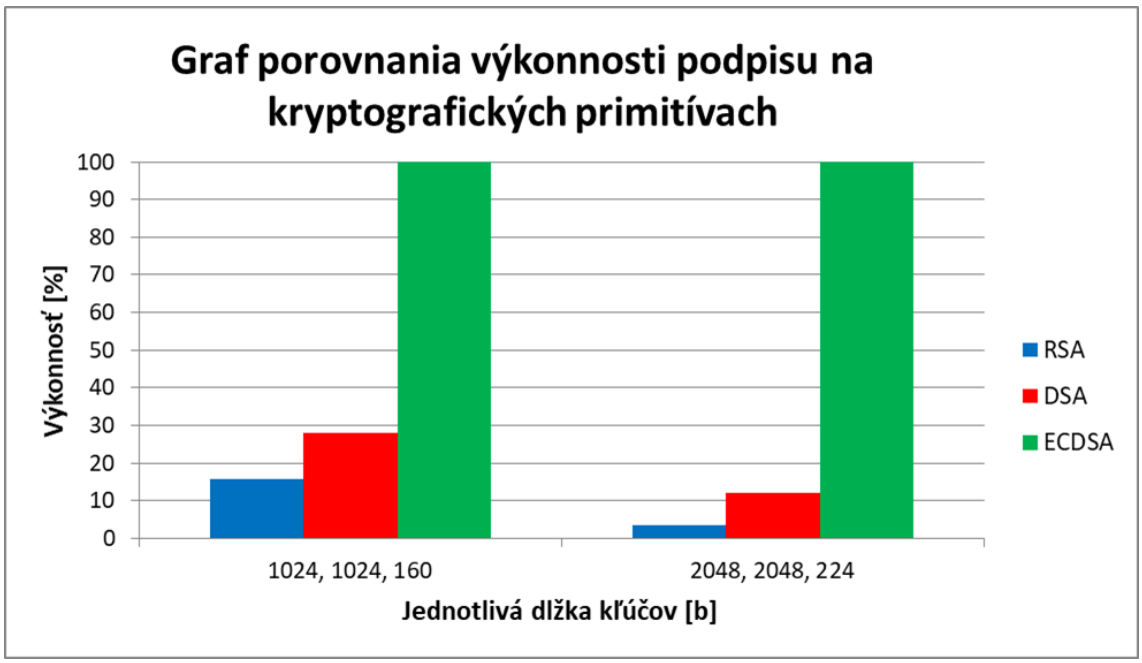
Veľkosť kľúča [bit]	**Typ**	**operácia [s]**	**Počet operácií za 1**
160	secp160r1	0,00511	195,38
192	nistp192	0,00682	146,85
224	nistp224	0,00896	111,8
256	nistp256	0,01146	87,36
384	nistp384	0,02677	37,36
521	nistp521	0,05878	17,01
163	nistk163	0,00844	118,24
233	nistk233	0,0155	64,49
283	nistk283	0,02853	35,05
409	nistk409	0,06343	15,78
571	nistk571	0,14769	6,78
163	nistb163	0,00902	110,88
233	nistb233	0,01698	58,95
283	nistb283	0,03166	31,57
409	nistb409	0,07208	13,86
571	nistb571	0,16951	5,9

Tab. 3.5: Porovnanie schém v počte operácií podpisu za 1s

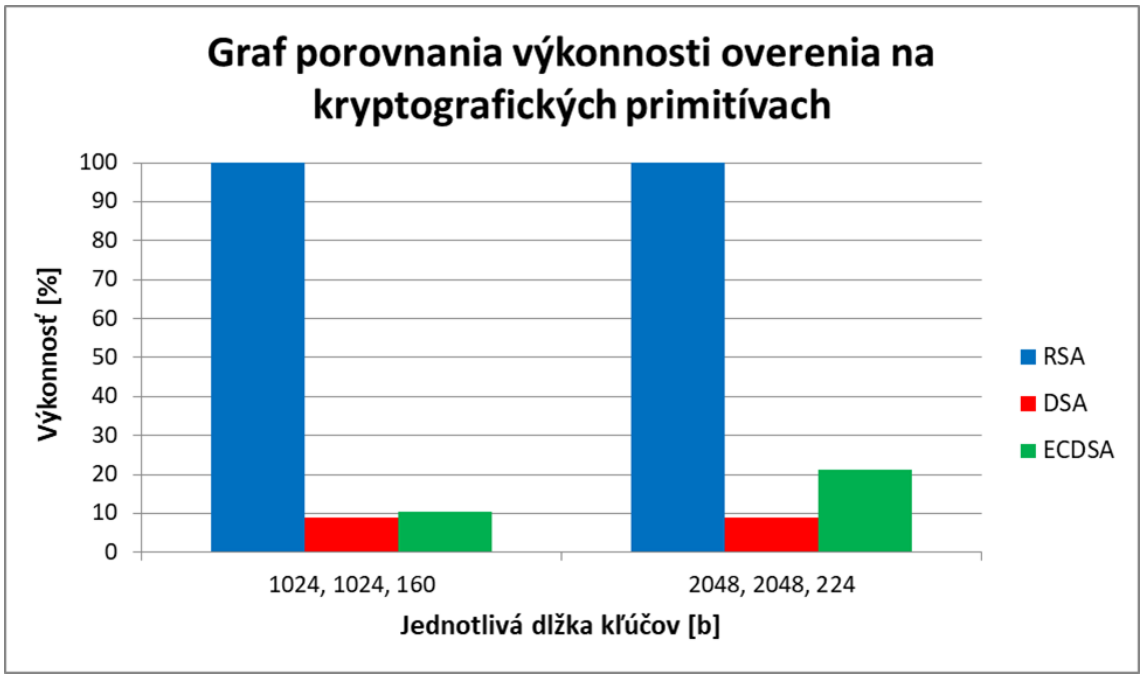
Veľkosť kľúča [bit]	**DSA Počet operácií podpisu za 1**	**ECDSA Počet operácií podpisu za 1**	**RSA Počet operácií podpisu za 1**
1024/1024/160secp	143,42	514,37	81,22
2048/2048/224nistp	41,03	341,6	12,39

Tab. 3.6: Porovnanie schém v počte operácií overenia za 1s

Veľkosť kľúča [bit]	**DSA Počet operácií overenia za 1**	**ECDSA Počet operácií overenia za 1**	**RSA Počet operácií overenia za 1**
1024/160secp/1024	137,7	161,96	1542
2048/224nistp/2048	38,19	91,31	433,2



Obr. 3.1: Zobrazenie grafu percentuálneho porovnania výkonnosti na kryptografických primitívach pri zachovaní rovnakej bezpečnosti



Obr. 3.2: Zobrazenie grafu percentuálneho porovnania výkonnosti na kryptografických primitívach pri zachovaní rovnakej bezpečnosti

Na obrázku 3.1 je ako referenčná hodnota výkonnosti 100% určené kryptografické primitívum ECDSA. V porovnaní výkonnosti podpisu pri zachovaní rovnakej bezpečnosti (1024 bitov pre RSA a DSA, 160 bitov pre ECDSA) je kryptografické primitívum DSA približne o 70% menej výkonné ako ECDSA, a RSA približne o 16% menej výkonné. Pri náraste dĺžky kľúča sa tieto rozdieli ešte zväčšujú.

Na obrázku 3.2 je ako referenčná hodnota výkonnosti 100% určené kryptografické primitívum RSA. V porovnaní výkonnosti overenia pri zachovaní rovnakej bezpečnosti (1024 bitov pre RSA a DSA, 160 bitov pre ECDSA) je kryptografické primitívum DSA približne o 90% menej výkonné ako RSA, a ECDSA približne o 89% menej výkonné. Pri náraste dĺžky kľúča sa rozdieli pri RSA a ECDSA zmenšujú.

Tabuľky 3.5 a 3.6 prehladne zobrazujú porovnanie jednotlivých kryptografických algoritmov pre rôzne veľkosti kľúčov.

Z nameraných hodnôt a vyhodnotenia je zrejmé, že eliptické krivky sú jednoznačne vhodnejšie pre implementáciu do zariadení internetu vecí ako ich varianta bez dodatku na základe ECC.

Potvrdzuje to aj práca pána Leenta, z ktorej vyplýva, že čím je väčšia dĺžka kľúča, tým je väčšia aj spotreba energie. ECDH využíva približne tri krát menej energie ako DH pre generovanie kľúča a približne šesť krát menej energie ako DH pre výmenu kľúča [17].

3.0.2 Testovanie časť 2.

V tejto podkapitole sme sa venovali otázke, či by bolo možné zlepšiť výkonnosť šifrovania na obmedzených zariadeniach tým, že by sme blokové šifry nahradili prúdovými. Na testovanie blokových a prúdových šifier bolo použité taktiež zariadenie Raspberry Pi, ale s operačným systémom RASPBIAN STRETCH LITE. Táto verzia operačného systému bola vydaná v Apríli 2018 s verziou jadra 4.14. Lite verzia je minimálnou verziou Rasbian obrazu pre Raspberry Pi, to znamená menej nainštalovaného softvéru. Na testovanie bola využitá knižnica Wolfssl 3.14.0 a Openssl 1.1.0f s tou skutočnosťou, že neobsahuje všetky šifry ako knižnica wolfssl. Zariadenie Raspberry Pi bolo pripojené do siete pomocou Ethernet portu, následne pomocou ssh sme sa pripojili k nemu z notebooku. Pri čistej inštalácii novšej verzie raspbianu bolo nutné povoliť ssh, na čo bola využitá skutočnosť pridanie súboru s názvom ssh na sd kartu do priečinku boot. Metóda testovania bola zvolená obdobne ako pri prvom testovaní knižnice openssl a pri wolfssl bola využitá funkcia benchmark s rôznymi veľkosťami blokov. Pri funkci benchmark bolo nutné najprv povoliť niektoré kryptografické šifry, čo sme vykonali následným príkazom:

```
./configure --enable-des3 --enable-rabbit --enable-chacha
```

Pri testovaní pamäťovej náročnosti sme využili príkaz top. Na obrázku 3.3 môžeme vidieť využitie RAM pamäti a aj CPU. RAM pamäť bola využitá minimálne, z toho dôvodu sme testovanie pamäťovej na Raspberry Pi ďalej nevykonávali.

a)
```
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 2417 pi        20   0    4132   3228   2888 R  98.3  0.7   0:12.03 openssl
 2385 pi        20   0    3388   2192   1780 R   1.3  0.5   0:05.92 top
```

b)
```
  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
13680 pi        20   0    4872   3452   1288 R 97.7  0.8   0:20.42 lt-benchmark
13679 pi        20   0    8096   3376   2832 R  1.6  0.8   0:00.55 top
```

Obr. 3.3: Zobrazenie výsledku príkazu top a) openssl b) wolfssl

Výsledné hodnoty je možné vidieť v tabuľkách 3.7 a 3.8.

Následne sme spracovali údaje do grafov. Grafický obrázok 3.4 prehľadne zobrazuje výkonnosť blokových a prúdových symetrických šifier. Dĺžka kľúčov jednotlivých šifier je vidieť v grafickom zobrazení, väčšina dĺžok kľúčov je 128 bitov okrem šifry Chacha (256 b) a 3DES (168 b) a AES (rôzne dlžky klúčov a operačné módy). Najväčšiu výkonnosť pri rovnakej úrovni bezpečnosti má prúdová šifra HC-128, popis tejto šifry je spomenutý v kapitole 1.7.4 jej vhodnosť pre obmedzené zariadenia je ale otázna, z toho dôvodu, že táto šifra využíva paralelného výpočtu. Obmedzené zariadenia majú väčšinou jedno-jadrový procesor, tým postráda zmysel implementácie tejto šifry do obmedzených zariadení. Ako vhodným kandidátom za náhradu

Tab. 3.7: Benchmark Wolfssl 3.14

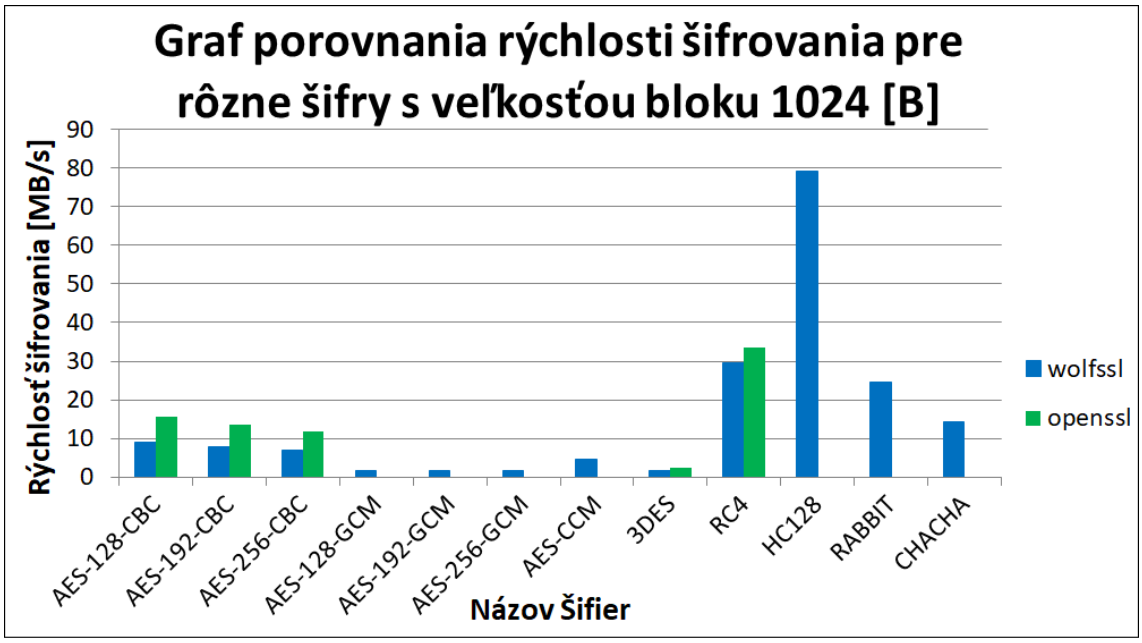
Veľkosť bloku	16 [B]	64 [B]	256 [B]	1024 [B]	8192 [B]
Blokové šifry	[MB/s]				
AES-128-CBC	8,56	8,96	9,07	9,09	9,048
AES-192-CBC	7,46	7,74	7,827	7,84	7,80
AES-256-CBC	6,6	6,83	6,89	6,91	6,88
AES-128-GCM	0,63	1,22	1,6	1,73	1,756
AES-192-GCM	0,60	1,17	1,52	1,65	1,676
AES-256-GCM	0,58	1,12	1,46	1,58	1,607
AES-CCM	1,64	3,17	4,15	4,47	4,584
3DES	1,75	1,776	1,77	1,79	1,774
Prúdové šifry	[MB/s]				
RC4	24,47	28,09	29,20	29,58	29,53
HC128	13,23	67,91	76,56	79,23	78,96
RABBIT	20,044	23,25	24,19	24,45	24,43
CHACHA	4,61	13,31	14,119	14,26	14,26

Tab. 3.8: Benchmark Openssl1.1.0f

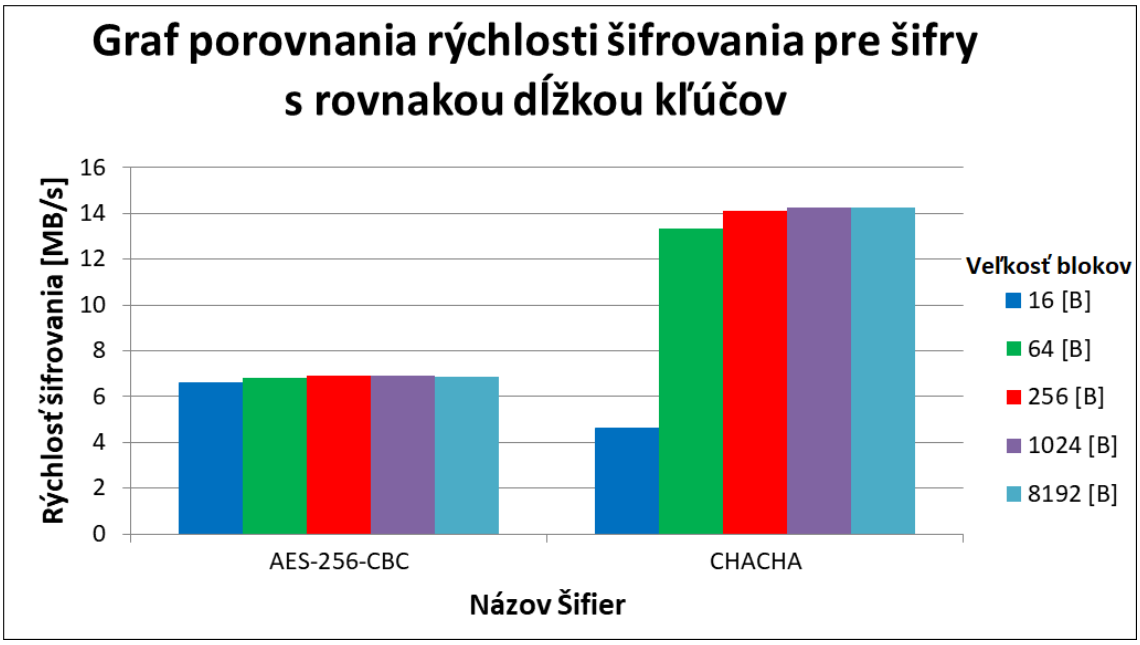
Veľkosť bloku	16 [B]	64 [B]	256 [B]	1024 [B]	8192 [B]
Blokové šifry	[MB/s]				
AES-128-CBC	13,57	15,11	15,55	15,61	15,66
AES-192-CBC	11,97	13,10	13,49	13,52	13,58
AES-256-CBC	10,70	11,59	11,90	11,92	11,95
3DES	2,30	2,39	2,41	2,43	2,42
Prúdové šifry	[MB/s]				
RC4	26,90	31,60	33,08	33,57	33,46

AES sa javí prúdová šifra Chacha20, ponúka bezpečnostnú úroveň 256 bitov. Porovnali sme tieto dve šifry v grafickom zobrazení na obrázku 3.6, prúdová šifra Chacha ponúka približne dva krát väčšiu výkonnosť ako bloková šifra AES v operačnom móde CBC (Cipher Block Chaining) - Mód zreťazenia šifrového textu. Tieto šifry ponúkajú, ale len šifrovanie, narozdiel od šifry AES v operačných módoch GCM a CCM, tieto módy ponúkajú aj MAC - Message Authentication Code, popis MAC je možný nájsť v kapitole 1.7.1. Výkonnosť týchto šifier je porovnaná pri bezpečnosti 128 bitov. Rýchlosť šifrovania operačného módu CCM je približne dva krát väčšia ako pri operačnom móde GCM. GCM využíva napríklad bezpečnostná technológia Medium Access Control Security (MACsec) v štandarde IEE 8021AE, ktorá zabez-

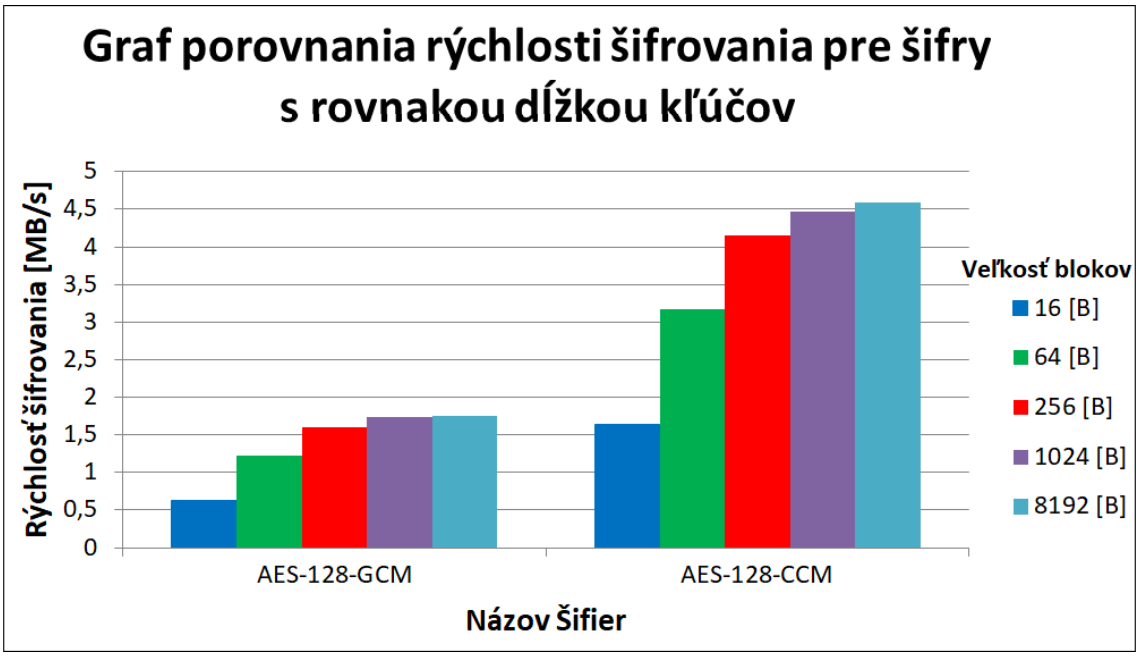
pečuje bezpečnú komunikáciu pre celú prevádzku na sieťach Ethernet. Operačný mód CCM využíva LoRaWAN.



Obr. 3.4: Zobrazenie grafu porovnania rýchlosti šifrovania pre rôzne šifry s veľkosťou bloku 1024 B



Obr. 3.5: Zobrazenie grafu porovnanie rýchlosti šifrovania pre šifry s rovnakou dĺžkou kľúčov



Obr. 3.6: Zobrazenie grafu porovnanie rýchlosti šifrovania pre šifry s rovnakou dĺžkou kľúčov

4 ANALÝZA VHODNOSTI TECHNOLÓGIÍ IOT

V predchádzajúcich častiach sme opísali technológiu IoT. Jej možné využitie bude v rôznych odvetviach, kde v budúcnosti bude táto technológia automatizovaná zefektívňovať jednotlivé úlohy a procesy, aktivity, zber a vyhodnocovanie veľkého množstva dát. Pre dosiahnutie tohoto cieľa je nutné vytvoriť novú národnú resp. svetovú sieť pre zariadenia Internetu vecí. Táto sieť resp. oddelené siete mobilní operátori, poskytovatelia internetu (ISP) alebo komerčné subjekty budujú už v dnešných dňoch, môžeme sa o tom dočítať vo voľnodostupných článkoch, ktoré opisujú aktuálnu situáciu IoT na domácom a zahraničnom trhu. V nasledujúcich kapitolách boli na základe definovaných požiadaviek na IoT sieť porovnané jednotlivé technológie. Ďalej sme na základe komparácie a analýzy vybrali jednu technológiu, ktorú považujeme za vhodnú na prevádzku IoT siete. Ďalšie kapitoly opisujú detailnejšie technickú stránku vybratej technológie.

4.1 Predpoklady na technológiu pre IoT sieť

Prvoradým účelom siete pre Internet vecí je priniesť nízko nákladovú technológiu a služby pre komunikáciu a prevádzku zariadení s nízkou spotrebou a nárokmi na objem prenesených dát. Typickým použitím sú monitorovacie a meracie senzory (priemysel, poľnohospodárstvo, životné prostredie, domácnosti) a sledovanie pohybu a polohy osôb alebo zvierat, dopravných prostriedkov či tovaru. Na základe získaných údajov z rôznych zdrojov. Spôsob získavania údajov a ich zdroje, sme pre výber vhodnej technológie pre IoT sieť definovali nasledovné parametre.

4.1.1 Predpoklady pre IoT sieť obecne

Jedná sa o globálnu infraštruktúru siete, kombinujúca fyzické a virtuálne objekty prostredníctvom využívania zberu dát a komunikačných schopností. Táto infraštruktúra zahŕňa existujúce aj vyvíjajúce sa prvky internetu a siete. Sieť poskytuje špecifickú objektovo orientovanú identifikáciu, snímače a senzory zo schopnosťou spojenia sa ako základ pre vývoj a prevádzku nezávisle spolupracujúcich služieb a aplikácií. Tie sa budú vyznačovať vysokou mierou autonómneho zberu dát, prenosom udalostí, pripojením k sieti a interoperabilitou.

4.1.2 Predpoklady pre technológiu IoT siete

Zvolená technológia musí spĺňať nasledovné požiadavky:

- nízka energetická náročnosť,

- možnosť prevádzky ako privátnej, regionálnej, národnej alebo globálnej siete,
- prenos informácií v bezdrôtovom, voľnom a neregulovanom pásme,
- prenos informácie obojsmerným prenosom,
- možnosť použitia frekvencie danej technológie aj mimo Európy napr. v Spojených štátoch,
- možnosť definovať počet odoslaných dát z koncových senzorov podľa konkrétneho IoT projektu,
- pokrytie signálom pre jednu bázovú stanicu pre:
  - vnútorné prostredie aspoň 1,5 km,
  - vonkajšie prostredie aspoň 7 km,
- možnosť pripojenia minimálne 500 tisíc koncových senzorov pre každú bázovú stanicu,
- štandardizácia použitých komunikačných protokolov,
- implementované prvky bezpečnosti pre komunikáciu,
- technológia dostupná ako "open-source" s dohľadom existujúceho združenia alebo aliancie,
- voľne dostupná dokumentácia technológie pre vývojárov a prevádzkovateľov,
- možnosť voľby vlastného biznis modelu pre prevádzkovateľa siete,
- jednoduchá dostupnosť koncových senzorov pre zvolenú technológiu,
- existujúci aplikačný softvér od viacerých výrobcov pre zbieranie, analýzu a vyhodnocovanie dát z koncových senzorov pre zvolenú technológiu.

4.1.3 Požiadavky pre hardvér – koncové senzory

- Jednoduchá dostupnosť koncových senzorov pre zvolenú technológiu, ktoré dokážu merať rôzne veličiny ako teplota, vlhkosť, prietok vody, elektrický prúd, rýchlosť, hluk, svetlo, akceleráciu objektu alebo GPS polohu.
- Napájanie senzoru z batérie zo životnosťou minimálne jeden rok (závisí od spôsobu použitia).
- Možnosť certifikácie senzorov pre použitie v IoT sieti.
- Malé fyzické prevedenie senzora.

4.2 Výber vhodnej technológie pro IoT simuláciu

Na základe nadobudnutých poznatkov a vyššie definovaných požiadaviek pre IoT sieť a jej komponenty sme vypracovali technické porovnanie jednotlivých technológií. Bezdrôtové technológie ako Wi-Fi, Bluetooth, ZigBee alebo ZWave neboli do vyhodnotenia zaradené, keďže v súvislosti s IoT sa primárne používajú pre riešenie tzv. inteligentných domácností (Smart Home). Pri vyhodnocovaní požiadaviek sme brali

do úvahy aj faktor, ako veľmi je dôležitá resp. kritická požiadavka, ktorú musí daná technológia spĺňať. Zamerali sme sa teda na siete typu LPWAN - Sigfox,LoRaWAN, NB-IoT, ich vlastnosti sú zhrnuté v tabuľke 4.2. Mali by sa zvážiť mnohé faktory pri výbere vhodnej technológie LPWAN pre aplikáciu IoT vrátane kvality služby, životnosti batérie, latencie, škálovateľnosti, dĺžky užitočného zaťaženia, pokrytia, rozsahu, nasadenia a nákladov.

4.2.1 QoS - Kvalita služieb

Sigfox a LoRa využívajú nelicencované spektrá a asynchrónne komunikačné protokoly. Môžu odraziť rušenie. Nemôžu však ponúkať rovnaké QoS, aké poskytuje NB-IoT. NB-IoT využíva licencované spektrum a synchrónny protokol založený na LTE, ktoré sú optimálne pre QoS na úkor nákladov, licencované spektra LTE sa pohybujú cenovo viac ako 500 miliónov EUR za MHz. Vďaka službe QoS a nákladovej kompenzácii je NB-IoT uprednostňované pre aplikácie, ktoré vyžadujú zaručenú kvalitu služieb, zatiaľ čo aplikácie, ktoré nemajú toto obmedzenie, by si mali zvoliť LoRa alebo Sigfox [40].

4.2.2 Model nasadenia

Špecifikácie NB-IoT boli uvoľnené v júni 2016, preto bude nutný dodatočný čas pred vytvorením siete. Ekosystémy Sigfox a LoRa sú však zrelé a v súčasnosti sú v komerčné v rôznych krajinách a mestách. LoRa má tú výhodu, že umožňuje v súčasnosti nasadiť v 42 krajinách verzus 31 krajín pre Sigfox. Napriek tomu sa celosvetové nasadenia LoRy a Sigfoxu sa stále rozširuje.

Okrem toho jednou z významných výhod ekosystému LoRa je jeho flexibilita. Na rozdiel od SigFoxu a NB-IoT, LoRa ponúka lokálnu sieť, t.j. LAN využívajúcu bránu LoRa, ako aj prevádzku verejnej siete cez základňové stanice. V priemyselnej oblasti by sa mohol použiť hybridný operačný model na nasadenie lokálnej siete LoRa v oblastiach výrobných podnikov a využívanie verejnej siete LoRa na pokrytie vonkajších oblastí [22].

4.2.3 Cena

V tabuľke 4.1 sú prehľadne zhrnuté cenové náklady Sigfox, LoRa a NB-IoT. Sigfox a LoRa sú nákladovo efektívnejšie v porovnaní s NB-IoT.

Tab. 4.1: Rozdiely cien Sigfoxu, LoRa a NB-IoT [40]

	Cena spektra	**Cena nasadenia**	**Cena koncového zariadenia**
Sigfox	Zadarmo	>4000€/základová stanica	<2€
LoRa	Zadarmo	>100€/brána >1000€ /základová stanica	3–5€
NB-IoT	>500 M€ /MHz	>15 000€/základová stanica	>20€

4.2.4 Výber vhodnej technológie IoT pre simuláciu

Po dôkladnej analýze sme vybrali technológiu LoRa resp. LoRaWAN, ktorá spĺňa všetky naše požiadavky na technológiu vhodnú pre IoT sieť. Technológia SigFox je vhodná taktiež, avšak nespĺňa niektoré požiadavky, ktoré sme vyhodnotili ako kritické. Ako sme už spomínali, nemusí to znamenať, že technológia SigFox a NB-IoT sú horšie alebo nevhodné. Je na konkrétnom zadávateľovi ako postaví svoje požiadavky pre plánovanú IoT sieť. Pre objektívnosť výberu spomenieme niektoré požiadavky, ktoré sme vyhodnotili ako kritické a technológia SigFox ich v našom zadaní nespĺňa. Spoločnosť vlastní všetky svoje technológie – dáta z backendu, cloudový server až po softvér koncových zariadení. SigFox samozrejme poskytuje výrobcom koncových zariadení prístup k technológii avšak za stanovených licenčných podmienok. Pre každú krajinu resp. zoskupenie krajín je možný len jeden národný operátor, ktorý musí súhlasiť s licenčnými a obchodnými podmienkami, čo môže byť pre danú krajinu nevýhodné z pohľadu konkurenčného prostredia resp. monopolného pôsobenia. Keďže technológiu vyvinula a vlastní súkromná spoločnosť jedná sa o proprietárnu technológiu čo môže do veľkej miery negatívne ovplyvniť jej ďalší rozvoj a taktiež záujem zo strany národných operátorov, výrobcov, vývojárov a koncových užívateľov. Aj kvôli vyššie popísaným dôvodom, môžeme ďalej konštatovať že SigFox nespĺňa aj ďalšie dôležité požiadavky ako napr. možnosť prevádzky ako privátnej siete alebo možnosť voľby vlastného biznis modelu pre prevádzkovateľa siete či voľne dostupná dokumentácia technológie pre vývojárov a prevádzkovateľov alebo jednoduchá dostupnosť backbone hardvéru a softvéru pre zvolenú technológiu. Pokiaľ by sme chceli naplniť cieľ tejto práce, technológia SigFox je absolútne nevhodná z dôvodu svojej "uzatvorenosti" ako pred bežnými užívateľmi tak aj akademickým svetom.

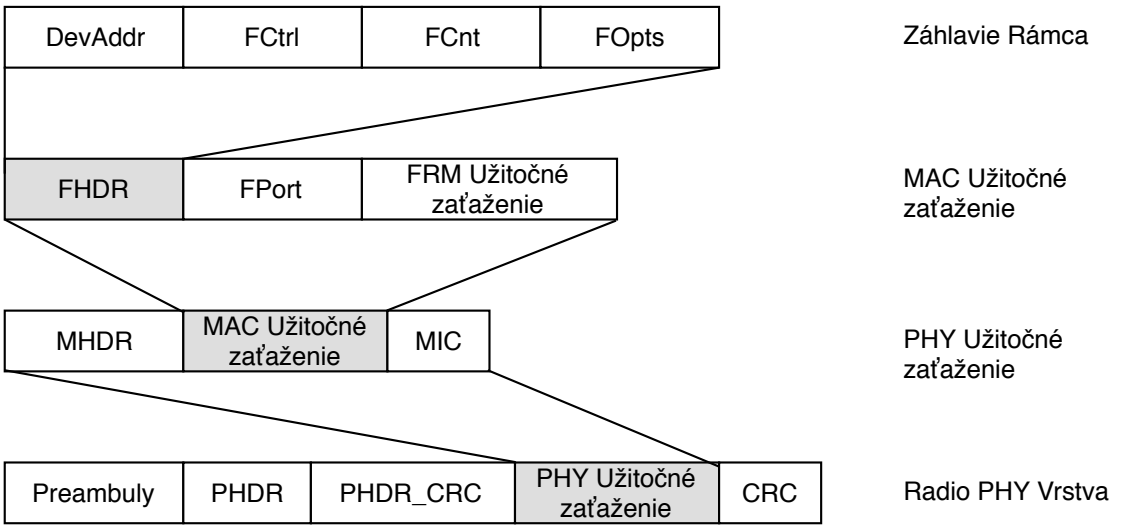
Tab. 4.2: Prehľad vlastostí LPWAN sietí.

	Sigfox	**LoRaWan**	**NB-IoT**
Modulácia	BPSK	CSS	QPSK
Frekvencia	868 MHz	868 MHz	Licencované LTE
Šírka pásma	100 Hz	250 kHz a 125 kHz	200 kHz
Maximálna rýchlosť prenosu dát	100 b/s	50 kb/s	200 kb/s
Obojsmerný	limitované polovičný duplex	áno polovičný duplex	áno polovičný duplex
Maximum správ za deň	140 UL, 4 DL	neobmedzený	neobmedzený
Maximálna dĺžka zaťaženia	12 bajtov (UL), 8 bajtov (DL)	243 bajtov	1600 bajtov
Dosah	10 km (mesto), 40 km (vidiek)	5 km (mesto), 20 km (vidiek)	1 km (mesto), 10 km (vidiek)
Odolnosť voči rušeniu	Veľmi vysoká	Veľmi vysoká	Nízka
Autentizácia a šifrovanie	Nepodporované	Áno(AES 128 b)	Áno(LTE šifrovanie)
Adaptívna rýchlosť prenosu údajov	Nie	Áno	Nie
Odovzdanie	Konečné zariadenia sa nezapájajú do jednej základnej stanice	Konečné zariadenia sa nezapájajú do jednej základnej stanice	Konečné zariadenia sa zapájajú do jednej základnej stanice
Lokalizácia	Áno (RSSI)	Áno (TDOA)	Nie
Povolenie privátnej siete	Nie	Áno	Nie
Štandardizácia	Spoločnosť Sigfox spolupracuje s ETSI na štandardizácii siete založenej na spoločnosti Sigfox	LoRa-Alliance	3GPP

4.3 Bližšia technická bezpečnostná analýza vybranej technológie LoRA

LoRa je prvým komerčným riešením s nízkymi investičnými i prevádzkovými nákladmi a obrovským obchodným využitím. Hlavnou výhodou technológie LoRa je jej dlhý dosah. Jedna brána resp. základňa môže rýchlo pokryť aj veľmi rozsiahle územia, napr. celé mestá alebo stovky kilometrov štvorcových. Celkový dosah tejto technológie je závislý na prekážkach, ktoré musí signál v prostredí prekonať (hustota zastavanosti, členitosť terénu atď.).

LoRa je fyzická vrstva resp. rádiová modulácia, ktorá sa používa pre vytvorenie telekomunikačného spojenia na veľkú vzdialenosť. Systém LoRa je založený na modulácii rozptýleného spektra, ktorý má veľmi podobnú charakteristiku ako FSK modulácia, avšak na oveľa väčšiu vzdialenosť. Prevádzka v rozprestretom spektre sa začala používať v armáde už pred niekoľkými desiatkami rokov predovšetkým z dôvodu dlhého dosahu a odolnosti voči rušeniu.



Obr. 4.1: Znázornenie fyzickej vrstvy

LoRaWAN definuje komunikačný protokol a sieťovú architektúru systému, zatiaľ čo fyzická vrstva LoRa umožňuje komunikačné spojenie na veľkú vzdialenosť. Protokol a sieťová architektúra majú najväčší vplyv na životnosť batérie, kapacitu siete, kvalitu služieb, bezpečnosť a paletu aplikácií použiteľných v sieti.

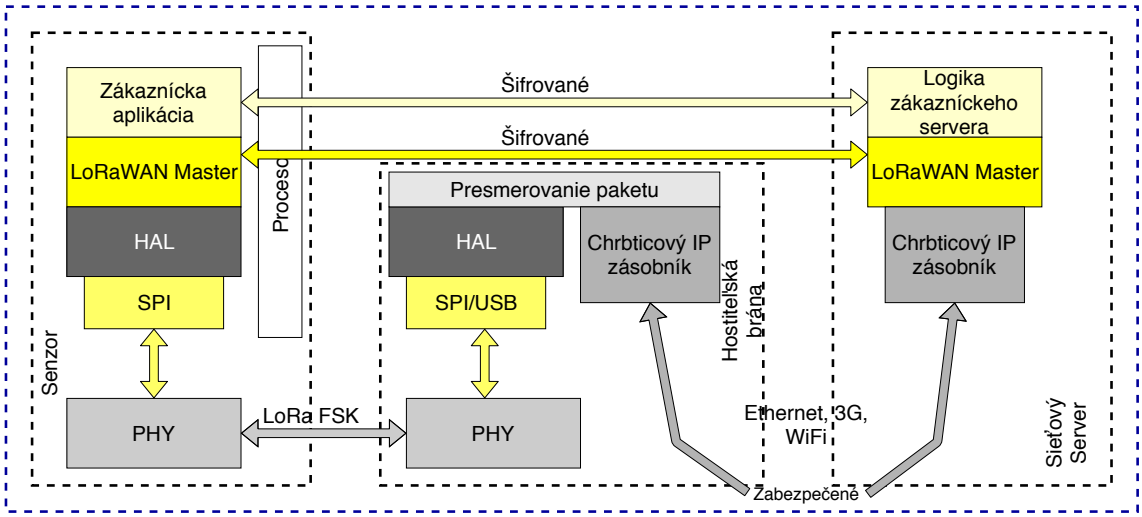
LoRa využíva zmeny rýchlosti prenosu, pre docielenie optimalizácie spotreby a zlepšenie škálovateľnosti siete. V Európe môže LoRa využívať rýchlosti až do 100 kb/s pri GFSK (Gaussian frequency-shift Keying) modulácii. Rýchlosti prenosu sa tiež líšia podľa implementácie. Z tohto dôvodu sa využíva algoritmus ADR (Adaptive datarate algorytm), ktorý dynamicky mení rýchlosť prenosu, tak aby vysielané

pakety dorazili bez straty.

Modulácia pre prenos dát podporuje rôzne sieťové topológie avšak najviac doporučenou je topológia Hviezda (Star). Koncové senzory zapojené v hviezdicovej topológii sú bezdrôtovo pripojené na gateway resp. bázovú stanicu. Vzdialenosť pripojenia závisí podľa prostredia a danej implementácie. Počet koncových senzorov, ktoré môžu byť pripojené na jednu bázovú stanicu je závislý na počte paketov ktoré senzory odošlú za jednu hodinu. Bázová stanica dokáže spracovať za jednu hodinu cca 1,5 milióna paketov.

Národné celoeurópske siete zamerané na IoT ako kritickú infraštruktúru pre zber dát osobných údajov, alebo kriticky dôležitých hodnôt pre spoločnosť, majú zvláštne potreby zabezpečenia tejto komunikácie. Táto požiadavka bola vyriešená niekoľkými vrstvami šifrovania:

- Unikátny sieťový kľúč Network Session Key (EUI64) pre bezpečnosť na sieťovej úrovni
- Unikátny sieťový kľúč Application Session Key (EUI64) pre bezpečnosť endto-end komunikácie na aplikačnej úrovni
- Unikátny kľúč Application Key (EUI128) pre bezpečnosť pripojenia koncového senzora do IoT siete



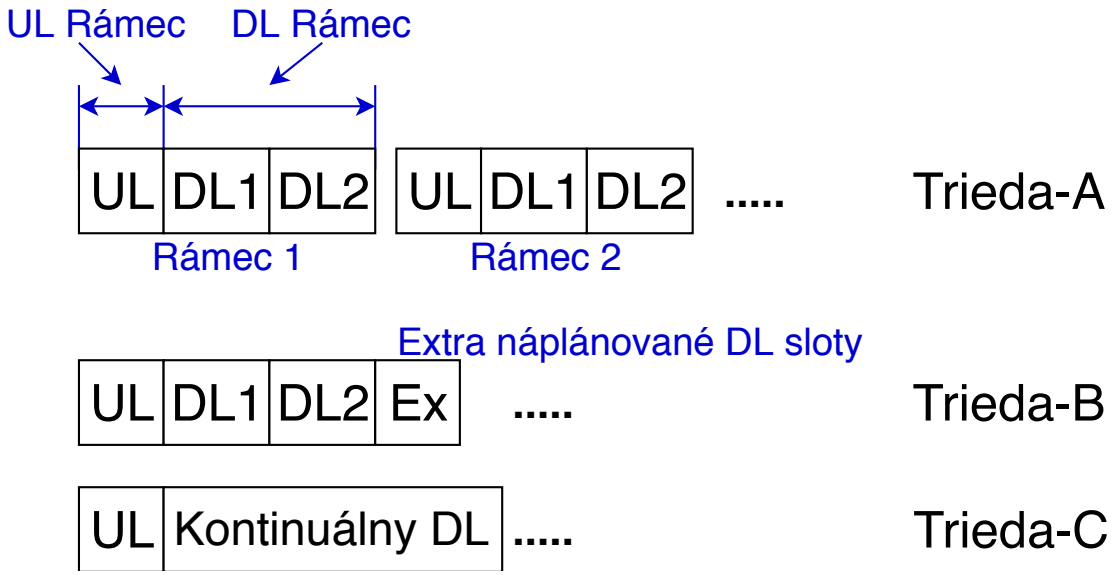
Obr. 4.2: Fyzická topológia LoRaWAN

Kľúče sú zdieľané, kvôli symetrickej metóde šifrovania (PSK – Pre Shared Key), preto musia byť vymieňané mimo média, ako je sieť, pre ktorú sú určené. LoRaWAN používa dĺžky kľúčov 128 bitov. Ako sme zmienili v kapitole 1.7, táto dĺžka kľúčov sa ešte považuje za bezpečnú. Väčšie kľúče by mali za následok väčšiu spotrebu energie a zariadenia by potrebovali väčší výkon. Je teda zvolený rozumný pomer medzi výkonom a bezpečnosťou.

4.3.1 Triedy koncových senzorov

LoRaWAN má niekoľko rôznych tried koncových zariadení, ktoré riešia rôzne potreby a možnosti použitia širokou škálou aplikácií:

- **Obojsmerná komunikácia koncových zariadení (Trieda A)** - Koncové zariadenia triedy A umožňujú obojsmernú komunikáciu, kedy je uplink prenos každého koncového zariadenia nasledovaný dvoma krátkymi downlink správami. Prenosový slot plánovaný koncovým zariadením je založený na základe komunikačných požiadaviek konkrétneho senzora. Táto trieda A je vhodná pre senzory a aplikácie, ktoré potrebujú dáta hlavne posielať. Na príjem správy musí senzor počkať, až do plánovaného "okna", kedy prebehne vysielanie – napr. raz za hodinu.
- **Obojsmerná komunikácia koncových zariadení s naplánovaným slotom pre príjem (Trieda B)** – Koncový senzor triedy B otvára extra "okno" pre príjem správy v naplánovanom čase. Vďaka synchronizácii s bázovou stanicou táto vie, kedy je senzor pripravený na príjem správ (kedy "počúva").
- **Obojsmerná komunikácia koncových zariadení s maximálnym počtom prijímacích slotov (Trieda C)** – Koncové senzory triedy C majú takmer trvale otvorené sloty pre príjem správ. Sloty sú uzatvorené len pri odosielaní správ.



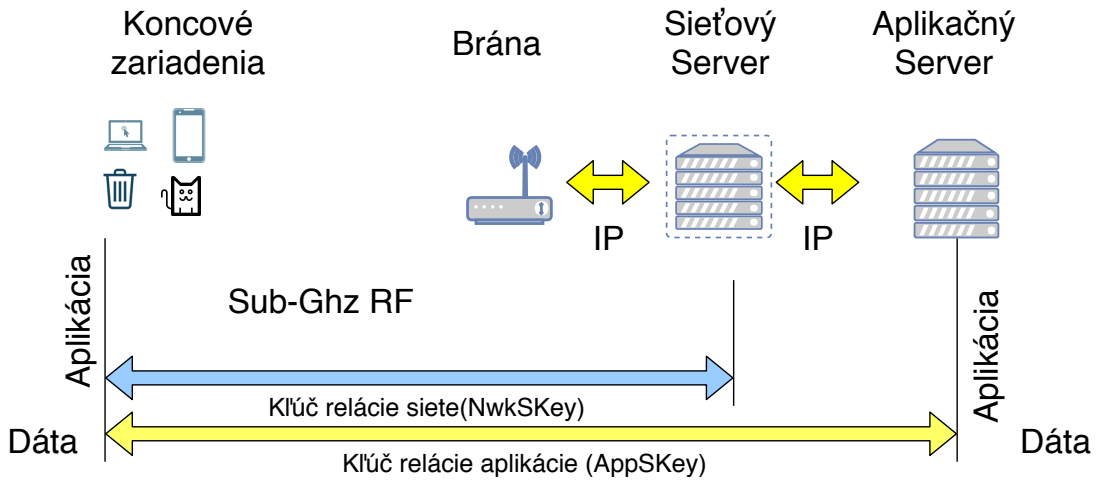
Obr. 4.3: Znázornenie tried rámcov pre uplink a downlink

Typ použitej triedy senzora a početnosť správ ktoré vysiela a prijíma úzko súvisí s jeho výdržou. Senzory typu A sú skoro vždy napájané z malých batérií, ktoré môžu fungovať až 10 rokov. Na opačnej strane senzory typu B alebo C poháňajú 2-3

tužkové batérie napr. typu CLR14, prípadne sú permanentne pripojené do elektrickej siete.

4.3.2 Sieťová architektúra

Základná architektúra v LoRaWAN sieti je nasledovná: koncové zariadenie teda senzor komunikuje s použitou bázovou stanicou LoRaWAN. Bázová stanica odovzdá "surové" dáta zo zariadenia do sieťového servera cez sieťové rozhranie s vyššou priepustnosťou, typicky Ethernet alebo 3G. V dôsledku toho, sú bázové stanice aj tzv. konvertory protokolu. Sieťový server je zodpovedný za dekódovanie paketov odoslaných z koncových senzorov a generovanie paketov, ktoré majú byť odoslané späť do zariadenia. Sieťový server taktiež zabezpečuje správne smerovanie dát do rôznych koncových aplikácií.



Obr. 4.4: Topológia LoRaWAN siete.

4.3.3 Adresácia

Zariadenia a aplikácie majú 64 bitový jedinečný identifikátor (DevEUI a AppEUI). Keď sa senzor pripojí k sieti, dostane dynamickú (nie jedinečnú) 32-bitovú adresu (DevAddr).

4.3.4 Aktivácia senzorov

Pred tým ako koncové zariadenie je schopné komunikovať so sieťovým serverom tak by malo byť toto zariadenie aktivované a malo by prejsť procesom spojenia. Tento mechanizmus zabraňuje neznámym koncovým zariadeniam pripojiť sa na sieťový

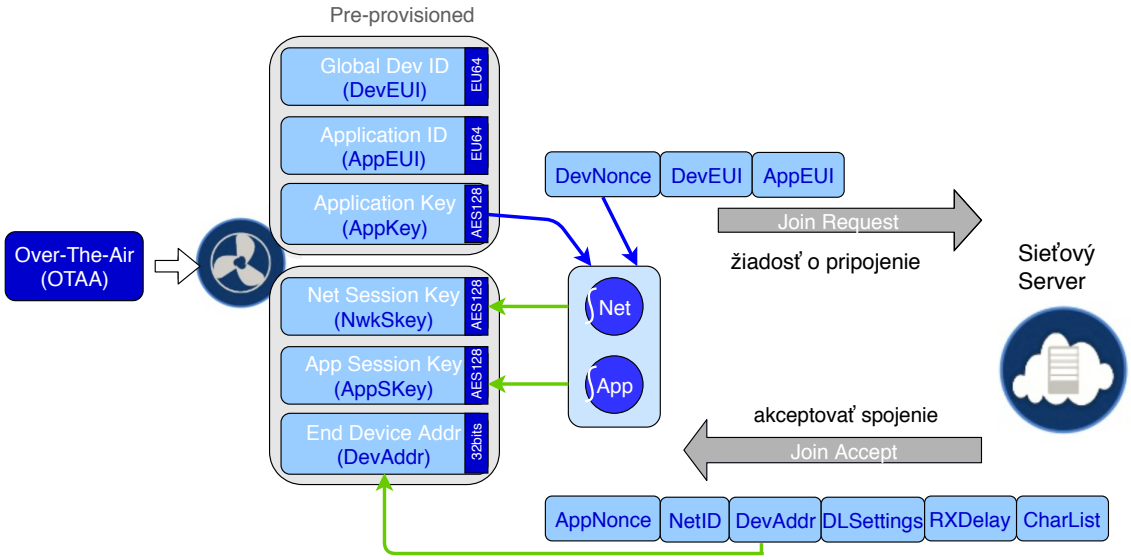
server a tak vyraďuje tieto zariadenia z účasti na komunikácii. Pre LoRaWAN sú možné dva typy aktivácie senzorov do siete:

- Automatická - Over-the-Air Activation (OTAA)
- Manuálna – Activation by Personalization (ABP)

Over-the-Air Activation (OTAA)

Je preferovaný a najbezpečnejší spôsob, ako sa môže senzor pripojiť do siete. Koncové zariadenie-senzor vykoná pripájacie procedúry so sieťou, počas ktorej mu je pridelená dynamická "DevAddr" a dohodnú sa bezpečnostné kľúče.

OTAA poskytuje niektoré bezpečnostné mechanizmy. Najprv používa jedinečné parametre. V OTAA, AppKey, DevEUI, AppEUI, AppNonce a DevNonce by mali byť všetky jedinečné medzi koncovými zariadeniami . V tomto prípade ohrozenie jedného koncového zariadenia neznamená ohrozenie celej siete. Po druhé, pre DevNonce existuje vyrovnávacia pamäť, aby sa zabránilo opakovanému útoku. Pri každom prijatí novej žiadosti o pripojenie by mal server skontrolovať vyrovnávaciu pamäť, aby zistil, či bol predtým použitý nonce. Ak sa používa, koncové zariadenie sa nesmie pripojiť k sieti. V tomto prípade nie je možné kopírovať žiadosť o pripojenie a prehrať ju.



Obr. 4.5: Schéma aktivácie senzoru pomocou OTAA.

Výhodou OTAA je väčšia bezpečnosť oproti ABP, pretože sieť generuje a odosiela šifrovacie kľúče. Vzhľadom na vyššiu úroveň bezpečnosti je OTAA najčastejšie používanou metódou v rámci IoT a LoRaWAN.

Za nevýhodu možno považovať to, že objekt musí implementovať tento mechanizmus pripojenia, ktorý pridáva dodatočnú vrstvu zložitosti. Aby sme vytvorili spojenie so sieťou a identifikovali objekt, potrebujeme nejaké informácie.

Activation by Personalization (ABP)

Použitie aktivačnej metódy Activation by Personalization (ABP) znamená, že v niektorých prípadoch môže byť nutné napevno zadať "DevAddr" rovnako, ako aj kľúče zabezpečenia pre senzor. Táto metóda by sa mohla zdať ako jednoduchšia, pretože môžeme preskočiť inicializačné spojenie. ABP má aj niektoré nevýhody spojené s bezpečnosťou. Výhoda je jednoduché pripojenie k sieti a tak zariadenie môže byť spustené len v krátkom čase. Nevýhodou je že šifrovacie kľúče umožňujúce komunikáciu so sieťou sú v zariadení predkonfigurované a toto oslabuje bezpečnosť. Hodnoty počítadla rámcov by mali byť použité len raz vyvolanie rovnakého kľúča s režimom CCM, aby neboli zneužité. Pri ABP je nutné používať energeticky nezávislú pamäť na ukladanie čítačiek rámcov, aby táto hodnota nebola resetovaná.

4.3.5 Kľúčový manažment

Ako sme sa už zmienili v predošlých kapitolách LoRaWAN používa pre zabezpečenú dátovú komunikáciu tri rôzne typy šifrovacie kľúče, a to:

- Application Key (AppKey)
- Application Session key (AppSKey)
- Network Session key (NwkSKey)

Tabuľka 4.3 stručne predstavuje tieto 3 kľúče vrátane ich názvu, typu, dĺžky, spôsobu vytvárania kľúčov a ich použitia.

Tab. 4.3: Tabuľka kľúčov v LoRaWAN

Názov kľúča	Typ kľúča	Dĺžka[b]	Vygenerovanie	Použitie
AppKey	Symetrický	128	Aplikáciou	MIC pre žiadosť o pripojenie a akceptovanie Šifrovanie prijatia spojenia Vytvorenie kľúča relácie
AppSKey	Symetrický	128	AppKey	Šifrovanie dátových správ
NwkSKey	Symetrický	128	AppKey	MIC pre správy Šifrovanie správ iba s príkazom

Application Key

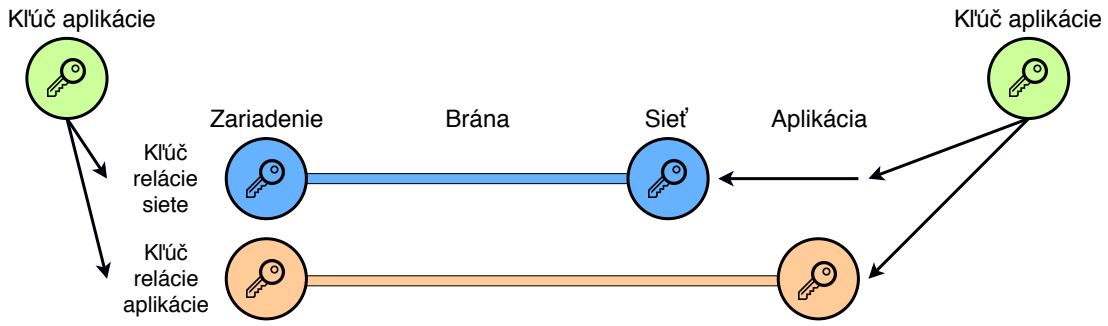
Application Key umožňuje užívateľovi nastaviť 128-bitové hexadecimálne číslo predstavujúce Application Key. Kedykoľvek sa koncový senzor pripojí k sieti cez OTAA, aplikačný kľúč sa použije na odvodenie sieťového kľúča. Network Session Key a Application Session Key, sú špecifické pre dané koncové zariadenie pre šifrovanie a overenie sieťovej komunikácie a dát aplikácií.

Application Session Key

Application Session Key umožňuje užívateľovi nastaviť 128bitové hexadecimálne číslo predstavujúce kľúč aplikácie relácie. Dáta sú zašifrovaný pomocou algoritmu AES s 128-bitovým tajným kľúčom, aplikácie Session Key. Každé koncové zariadenie má svoj vlastný jedinečný aplikačný kľúč relácie ktorý je známy len koncovému zariadeniu a aplikačnému serveru.

Network Session Key

Network Session Key umožňuje užívateľovi nastaviť 128bitové hexadecimálne číslo predstavujúce kľúč siete relácie. Kľúč relácie siete slúži sieťovému serveru a koncovým zariadením pre výpočet a overenie kódu integrity správy. Ďalej sa používa na zašifrovanie a dešifrovanie pola užitočného obsahu MAC iba pre dátové správy. Všetky sieťové rámce obsahujú 32-bitový šifrovací podpis (Message Integrity Check), vypočítaný s využitím algoritmu AES s 128-bitovým tajným kľúčom. Každé koncové zariadenie má vlastný Network Session Key, ktorý pozná jedine koncové zariadenie a sieťový server.



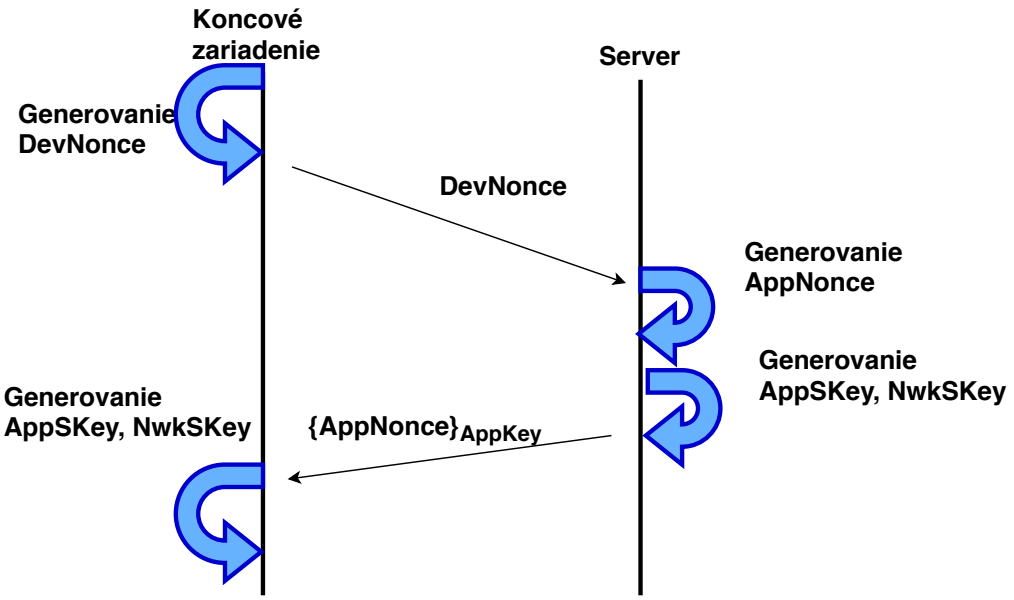
Obr. 4.6: Náčrt zabezpečenej komunikácie.

Generovanie kľúčov

AppKey je kľúč jedinečný pre 16 bajtov. Je pridelený vlastníkmi aplikácií koncovým zariadeniam. Generovanie NwkSKey a AppSKey je v OTAA a ABP odlišná. Pre OTAA sú tieto dva kľúče generované AppKey pomocou aplikácie AppNonce zo strany servera a DevNonce zo strany koncového zariadenia. Zakaždým, keď sa koncové zariadenie obnoví alebo znovu spojí, tieto dva kľúče sa regenerujú novým nonceom. V ABP, NwkSKey a AppSKey sú tiež jedinečné pre každé koncové zariadenie. Tieto dva kľúče sú priamo priradené a uložené v koncovom zariadení pred prenosom. Sú to statické kľúče a po resetovaní sa nezmenia.

Kľúčová výmena

Výmena kľúčov opisuje ako sú kľúče a ostatné informácie vymieňané, aby nedošlo k úniku. V OTAA, AppKey je pred komunikáciou priradený obom, koncovému zariadeniu a serveru. Opíšeme si, ako sa vymieňajú dva kľúče relácie.



Obr. 4.7: Výmena kľúčov relácii v OTAA

Obrázok 4.7 znázorňuje výmenný proces NwkSkey a AppSKey. Za prvé, pripojenie k serveru, koncové zariadenie pošle žiadosť o pripojenie-(join request), ktorá obsahuje niektoré identifikátory a DevNonce. Na strane servera server odpovie na žiadosti o pripojenie so správou akceptovať spojenie (join accept), ak koncové zariadenie má povolené pripojenie k sieti. Join accept zahŕňa ďalší AppNonce. V tomto prípade obidve strany môžu generovať AppSKey a NwkSKey s týmito dvoma nonce.

4.3.6 Zhrnutie

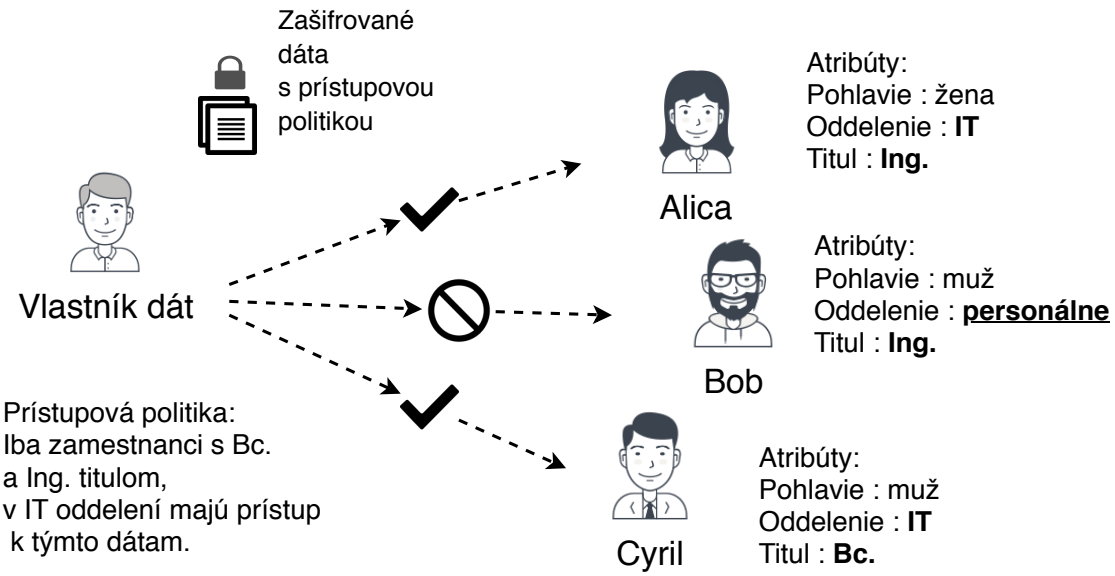
Skúmanie a analyzovanie zrianiteľných miest protokolu vedie nás k tomu že bezpečnosť, LoRaWAN nie je až tak dobre rozvinutá a je potrebné ju ešte zlepšiť. Hlavným faktorom je generovanie, doručovanie a ukladanie kľúčov. Je nutné teda zabezpečiť to aby si ostatný nevygenerovali alebo neodvodili tieto kľúče na základe dostupných informácii. V prípade vniknutia do zariadenia je narušená bezpečnosť a môže dôjsť k odcudzeniu kľúčov a tak k poškodeniu zhromaždených údajov. Je preto nutná znalosť spôsobov ako je možné LoRaWAN napadnúť pre vylepšienie toho protokolu a teda aj vylepšovať samotnú bezpečnosť LoRaWAN.

4.4 Zlepšenie

Ako sme si už povedali zariadenia IoT sú prevažne senzory, ktoré majú obmedzené zdroje s obmedzeným výkonom batérie a výpočtovými schopnosťami. Multicast je veľmi vyžadovaný v IoT scenároch. Týmto môžu uľahčovať odosielateľovi komunikáciu so skupinou prijímateľov. Je to teda efektívnejšie , ako odosielať rovnaké správy, ktoré spotrebúvajú energiu, každému individuálnemu zariadeniu. Zabezpečenie založenia skupinového kľúča sa vedie k vytvoreniu kľúčových funkcií na zabezpečenie integrity, autentifikácie a dôvernosti prenosu správ v týchto multicastových skupinách. Typické architektúry pre multicasting obsahujú centrálny kontrolér skupiny, ktorý riadi skupinu. Členovia sa pripoja do skupiny a zdieľajú medzi sebou skupinový kľúč na bezpečnú komunikáciu. Skupinový kľúč sa obnovuje vždy, keď dôjde k zmene členov, ktorí sa pripoja alebo vystúpia z tejto skupiny, aby zachovali tajnosť. Odosielateľ odošle správu zašifrovanú pomocou skupinového kľúča a prijímače dešifrujú správu pomocou rovnakého kľúča skupiny. Najväčšou nevýhodou tohto mechanizmu je však to, že ide o centralizovaný systém a centrálny kontrolér sa môže stať ústredným bodom útoku. Taktiež nie je dobrá škálovateľnosť pre miliardy zariadení, čo je potreba IOT. To vedie k motivácií zaviesť decentralizovaný systémom, ktorý by vyhovoval potrebám internetu vecí a bol tiež škálovateľný.

V prostredí multicastu je skutočný prenos dát zašifrovaný symetrickým algoritmom, ktorý používa bežný skupinový kľúč. Ako sme si už uviedli symetrické algoritmy sú ľahšie z hľadiska výpočtu a sú teda vhodné pre aplikácie IoT. Hlavnou výzvou je teda nájdenie spôsobu distribúcie spoločného skupinového kľúča, ostatným členom skupiny. Predzdieľané kľúče nie sú riešením, pretože vo väčšine IoT aplikácií nespĺňajú požiadavky dynamických charakteristík skupiny. Existujúce riešenia, ako je DTLS, sú dobré pre aplikácie s unikástom, ale nie sú vhodné pre multicastové. Pri unikástovom riešení je nevyhnutné zvyšovanie šírky pásma, taktiež môže spôsobovať preťaženie, kolízie, straty paketov, oneskorenie a podobne. Pre veľmi dynamické prostredie multicastu je preto potrebné flexibilné, ale mierne odľahčené riešenie.

Návrh zlepšenia siete by bol založený na kryptografických mechanizmoch ABE (Attribute Based Encryption) šifrovanie založené na atribútoch, najmä na CPABE (Ciphertext Policy Attribute-Based Encryption). Mechanizmy ABE sú generalizovanou formou identifikácie založenej na šifrovaní (Identity-Based Encryption - IBE), ktorá má identitu pre každého člena, ktorý sa zúčastňuje bezpečného prenosu správ. CPABE, podľa ktorého šifrovateľ šifruje správu pomocou verejného parametra a prístupovú štruktúru, ktorú musí dešifrovateľ splniť, aby dešifroval správu. Každý prijímateľ má súkromný kľúč daný generátorom súkromného kľúča (PKG), ktorý sa používa na dešifrovanie správy, za predpokladu, že skutočne vyhovuje prístupovej štruktúre, ktorú vytvoril odosielateľ. Celý mechanizmus je založený na Sha-



Obr. 4.8: Prehľad funkcie CPABE

mirovom tajnom zdieľacom mechanizme. Koreňový kľúč v prístupovej štruktúre sa rekurzívne rozdelí na listy na strane odosielateľa. Na strane prijímateľa sa proces obráti a koreňové tajomstvo sa znova generuje z listov rekurzívnym spôsobom pomocou polynomickej interpolácie Lagrange. Celý mechanizmus sa skladá zo štyroch hlavných fáz, konkrétne Set-up, Keygen, šifrovanie a dešifrovanie. Na obrázku 4.8 je prehľadne zobrazená funkcionalita kryptografického mechanizmu CPABE. Myšlienka sa opiera o zachovanie bezpečnostných aspektov mechanizmov ABE. Odľahčené riešenie CPABE by spočívalo v znížení zaťaženia z koncových zariadení s nízkym výkonom tým, že by bola pretlačená intenzita výpočtov na bránu. Brána by mohla robiť hlavnú časť dešifrovania, ale nebude vykonávať celé dešifrovanie. Čiastočne dešifrované dáta by boli predané do koncových uzlov, ktoré potom dokončia zvyšok dešifrovania. Zabránilo by sa tým extrakcii obyčajného textu (správy alebo kľúča), aby sa zachovala bezpečnosť medzi koncovými bodmi a súčasne by sa odľahčili koncové uzly od vykonanie hlavných výpočtov pre úsporu energie. Riešenie má tak výhody mechanizmov ABE ale znižuje režijné náklady mechanizmov ABE z koncových zariadení [6].

Zlúčenie flexibilnosti bezpečnostných mechanizmov ABE pre multicast na jednej strane a zníženie výpočtov na koncových uzloch na druhej strane poskytuje dokonalú predstavu o dosiahnutí bezpečného prostredia pre multicast pre zariadenia s obmedzeným príkonom IoT. Takýto prístup je nezávislý od akejkoľvek technológie fyzickej vrstvy a tak by sa mohol hodiť pre budúce 5G technológie.

5 VYUŽITE SIEŤOVÉHO SIMULÁTORA NS-3 V IOT

NS-3 je voľne dostupný a šíriteľný sieťový simulátor, ktorý je určený na výskum a vzdelávacie účely. Tento sa začal v roku 2006 a jeho vývoj pokračuje aj v súčasnosti. V nasledujúcich bodoch môžeme vidieť zhrnuté všeobecné informácie o simulátore NS-3:

- Vývojári - NS-3 Projekt
- Prvé vydanie - 30 Jún 2008
- Repozitár code.nsnam.org
- Podporovaný jazyk C++, Python
- Os - Linux, FreeBSD, Mac OS/X, Windows(Cygwin)
- Platformy IA-32, x86, x64
- Typ - simulátor
- Licencia - GNU GPLv2
- Webová stránka - www.nsnam.org

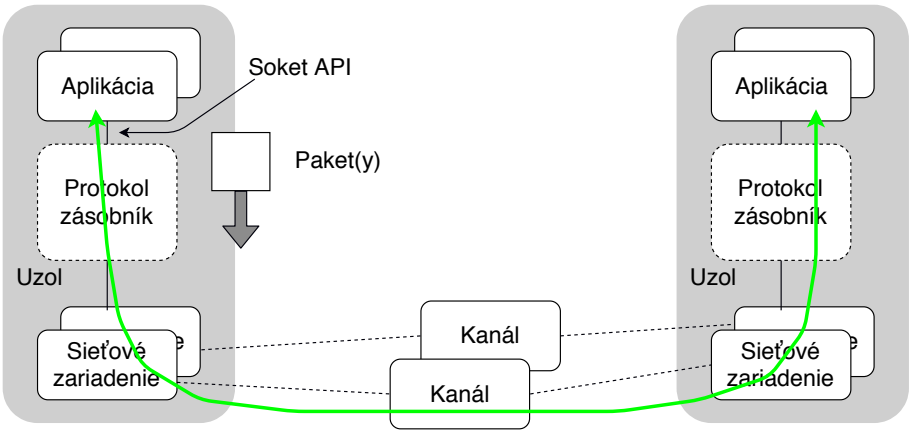
Projekt NS-3 je open-source projekt a od roku 2006 sa aktívne využíva pri vývoji programu NS-3. Cieľom programu NS-3 malo byť, že bude lepšia náhrada za simulátor NS-2. Aj keď NS-3 nie je kompatibilný spätne s verziou NS-2, obidva simulátory sú napísané v programovacom jazyku C++. NS-3 je však nový simulátor, ktorý nepodporuje aplikačné rozhranie NS-2. Určité moduly z NS-2 boli prenesené do NS-3. Využitie modulov nie je obmedzené len pre prácu s internetovými protokolmi alebo internetom vo všeobecnosti, ale taktiež pre iné systémy, ktoré nie sú založené na internete.

NS-3 project sa má za úlohu vybudovať pevné simulačné jadro, ktoré je dobre zdokumentované, užívateľsky jednoduché a pohodlné na ladenie. Je ústretové potrebám kompletnej simulácie pracovného postupu ako je konfigurácia simulácie na sledovanie, zbieranie a analýzu dát a podobne. taktiež infraštruktúra NS-3 podporuje rozvoj simulačných modelov, ktoré sú dostatočne realistické, aby NS-3, ktorý má byť použitý ako emulátor sietí v reálnom čase, bol prepojený s realitou a umožňoval mnoho implementácií protokolov existujúcich v reálnom svete. Tento simulátor podporuje výskum na sieťach založených na IP a non-IP. Avšak, veľká väčšina jeho užívateľov je zameraná na bezdrôtové IP simulácie, ktoré zahŕňajú modely pre bezdrôtovú sieť Wi-Fi, WiMAX alebo LTE pre vrstvy 1 a 2, či dokonca simuláciu rôznych statických alebo dynamických smerovacích protokolov, ako je OLSR, GPSR alebo AODV.

5.1 Architektúra

NS-3 dokáže simulovať komunikáciu medzi rôznymi zariadeniami, uzlami, ktoré si medzi sebou vymieňajú informácie (Packets) cez dané prostredie (Ethernet alebo Wi-Fi sieť). Uzol (Node) je všeobecný termín používaný pre akékoľvek zariadenie s určitou funkcionalitou, ako sú napríklad vstupno-výstupné rozhranie, aplikácia alebo protokolový zásobník. Uzlami môžeme rozumieť mobilné telefóny, tlačiarne, Wi-Fi smerovače alebo dokonca YouTube servery. Hlavnou časťou uzlov sú aplikácie (applications), ktoré plnia určité úlohy. Sú schopné komunikovať s rôznymi protokolmi a pôsobí ako generátor dát. Komunikáciu medzi uzlami zaisťujú NetDevices. Tie chápeme ako sieťové karty, ktoré môžu byť zapojené do vstupno-výstupného rozhrania uzla. V Linuxe sa tieto NetDevices vystupujú pod názvom „eth0“. Uzol môže zahŕňať viacero NetDevices alebo rozhraní, napr. Bluetooth, WiFi alebo Ethernet [42].

Na Obrázku 5.1 je znázornená základná architektúra simulátora NS-3.



Obr. 5.1: Architektúra NS-3

5.2 Moduly

Tento simulačný nástroj ponúka využitie viacerých modulov. Môžu byť modifikované podľa potreby, ale kvôli zachovaniu funkcionality simulátora to nie je odporúčané. Každý z modulov je reprezentovaný vlastnou zložkou v adresári „src/“. Užívatelia si ich môžu vytvárať, čo im uľahčuje prácu na rozsiahlych projektoch. Základnou zložkou je tzv. „core modul“, na ktorom sú závislé všetky ostatné. Súbor „wscript“predpisuje závislosť, tento súbor je napísaný v jazyku Python a musí byť súčasťou každého projektu. Takisto sa používa na jeho zostavenie. S každou novou verziou sieťového simulátora sa tieto moduly môžu meniť, preto nie je garantovaná

kompatibilita medzi verziami. Súčasný variant NS-3 ponúka veľké množstvo modulov, s ktorými je možno pracovať. Následne si popíšeme vybrané moduly a tie, ktoré by bolo vhodné využiť v IoT [29].

- Core je základný modul, ktorý umožňuje programátorovi používať rôzne užitočné metódy, ako sú napr. nastavenie, plánovanie, vykonávania udalostí času simulácie, generovanie náhodných premenných alebo dokonca tzv. callback funkcie, ktoré zohrávajú v simulačnom nástroji veľkú úlohu.
- Mobility je modul, ktorý sa využíva pri simulácií pohybu napríklad vozidiel. Tie menia svoju pozíciu v závislosti na čase. Nastavujú sa im súradnice x, y, z.
- Komunikáciu medzi vozidlami a nastavenie sieťových zaradení umožňuje modul WiFi.
- Modul Building je vhodný na modelovanie 3D budov, napríklad aby sa mohol testovať aj faktor šírenia signálu v meste.
- Modul 6LoWPAN ponúka kompresiu paketov IPv6 podľa špecifikácie RFC 4944 a RFC 6282

5.3 Výhody a nevýhody simulátora

Ako každý nástroj, aj NS-3 má svoje výhody a nevýhody. Hlavné výhody tohto simulátora sú následovné:

- Podporuje offline animátor NetAnim pre LAN a bezdrôtové siete
- NS-3 poskytuje externé nástroje pre analýzu prenesených dát počas simulácie, ako je napr. Wireshark určený pre *.pcap súbory
- PyViz je online vizualizátor, ktorý slúži pre spúšťanie spolu so simuláciou a je vhodný na ladenie programu
- Využíva Mercurial (http://code.nsnam.org/) ako spravovací systém zdrojových kódov (VSC)
- Jeden z najrýchlejších a najefektívnejších simulátorov v rámci spravovania pamäte
- Dokumentácia k simulátoru NS-3 obsahuje vyše 120 strán a takisto je dostupný vyše 500 stranový dodatočný manuál k modelom projektu NS-3

Vzhľadom k tomu, že každému vyhovuje niečo iné, má každý simulátor pomerne veľa nevýhod. Nevýhodami pre tento nástroj sú:

- Pomerne zložitý na použitie z dôvodu, že nemá grafické používateľské rozhranie
- Vizualizácia sa stále iba vyvíja
- Staršie verzie programu nie sú kompatibilné s aktuálnymi, z toho dôvodu je potrebná analýza a modifikácia kódu

6 SIMULÁCIA

Pre správne fungovanie simulačného nástroja NS3 je potreba ho správne nakonfigurovať. Jednotlivé komponenty modulu lora modelujú rôzne aspekty siete Lora, avšak jednotlivé triedy musia byť správne navzájom prepojené, aby mohli simulovať sieť. Je na to potrebný simulačný skript, ktorý využíva systém asistentov na vytvorenie a konfiguráciu veľkého počtu zariadení. Okrem toho sa simulačný skript používa aj na zhromažďovanie údajov zo simulácie, pričom sa využívajú stopové zdroje, ktoré boli umiestnené v rámci niektorých významných premenných triedy. Vždy, keď nastane určitá udalosť počas simulácie, uskutoční sa volanie na funkciu na úrovni skriptu, udalosť môže byť zaregistrovaná v jednej zo skriptových dátových štruktúr, ktoré sa majú neskôr analyzovať.

Na simuláciu sme vytvorili tri scenáre, ktoré simulujú LoRaWAN sieť. K simulácií sme využili sieťový simulátor NS-3 vo verzií N3.28 a modul lorawan, ktorý bol vytvorený pre simuláciu siete LoRaWAN. Odkaz pre stiahnutie toho modulu je možné nájsť na odkaze `https://github.com/signetlabdei/lorawan`. Prvý scenár je scénar s nízkym počtom uzlov, rádovo desiatky uzlov až sto uzlov. Tento scenár by mohol simulovať využitie LoRaWAN siete pre meranie kvality ovzdušia vo veľkom meste ako je napríklad Brno.

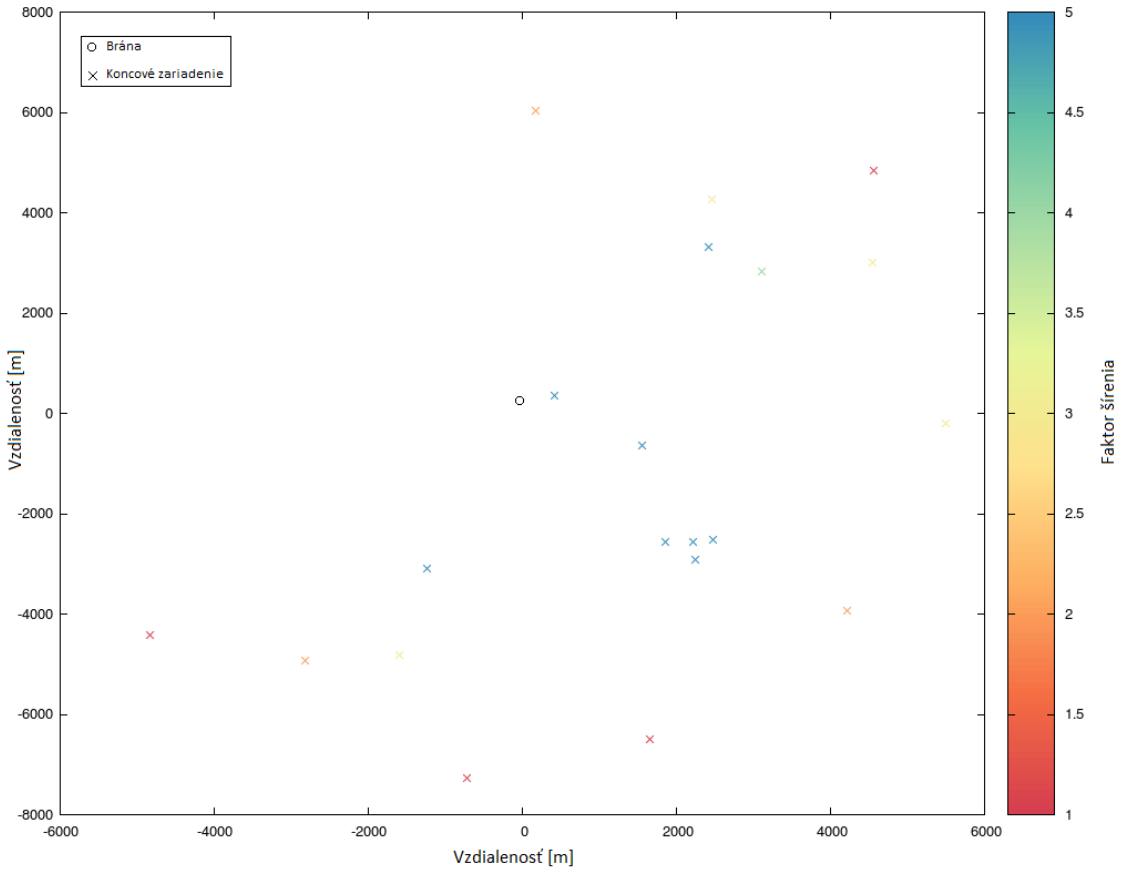
Druhý scenár sa zameriava na simuláciu pre počet uzlov rádovo v stovkách. Takýto scenár môže simulovať parkovisko v parkovacom dome, v ktorom je výhodné monitorovať počet voľných miest pre zaplnenie parkovacieho domu. Toto monitorovanie môže uľahčiť život ľudí, tým že napomôže organizácií takéhoto parkovacieho domu, či sú ešte parkovacie miesta voľné. Zároveň takýto senzor môže napomôcť aj ku rýchlejšiemu zaparkovaniu ak sa prepojí so svetlom, ktoré bude nad parkovacím miestom signalizovať voľno.

Tretí scenár simuluje nasadenie veľkého množstva senzorov rádovo v tisíckach pre potreby veľkej siete.

6.1 Prvý scenár - meranie kvality ovzdušia

Tento scenár simuluje možnosť monitorovať kvalitu ovzdušia pomocou LoRaWAN siete. V väčších mestách je často krát problém s kvalitou ovzdušia. Z toho dôvodu je potreba monitorovať kvalitu ovzdušia aby mohli byť občania včas varovaný pred možnou hrozbou spojenou s kvalitou ovzdušia. Poprípade je možnosť predchádzať zvýšenému smogu patričnými opatreniami, ako je napríklad bezplatný týždeň mestskej hromadnej dopravy. Pre túto simuláciu bol vytvorený simulačný script s názvom **lorawan-measuring-air-quality.cc**.

V tomto scenári sme simulovali dvadsať senzorov s periódou zhromažďovania dát desať minút vo väčšom meste. Dobu trvania simulácie sme nastavili na jeden deň. Na obrázku 6.1 môžeme vidieť rozloženie daných dvadsiatich senzorov. Senzory sú rozložené v rôznych pásmach šírenia. Výsledky merania preukázali, že pri takomto nízkom počte senzorov je postačujúca aj jedna brána a nestrácajú sa žiadne pakety.

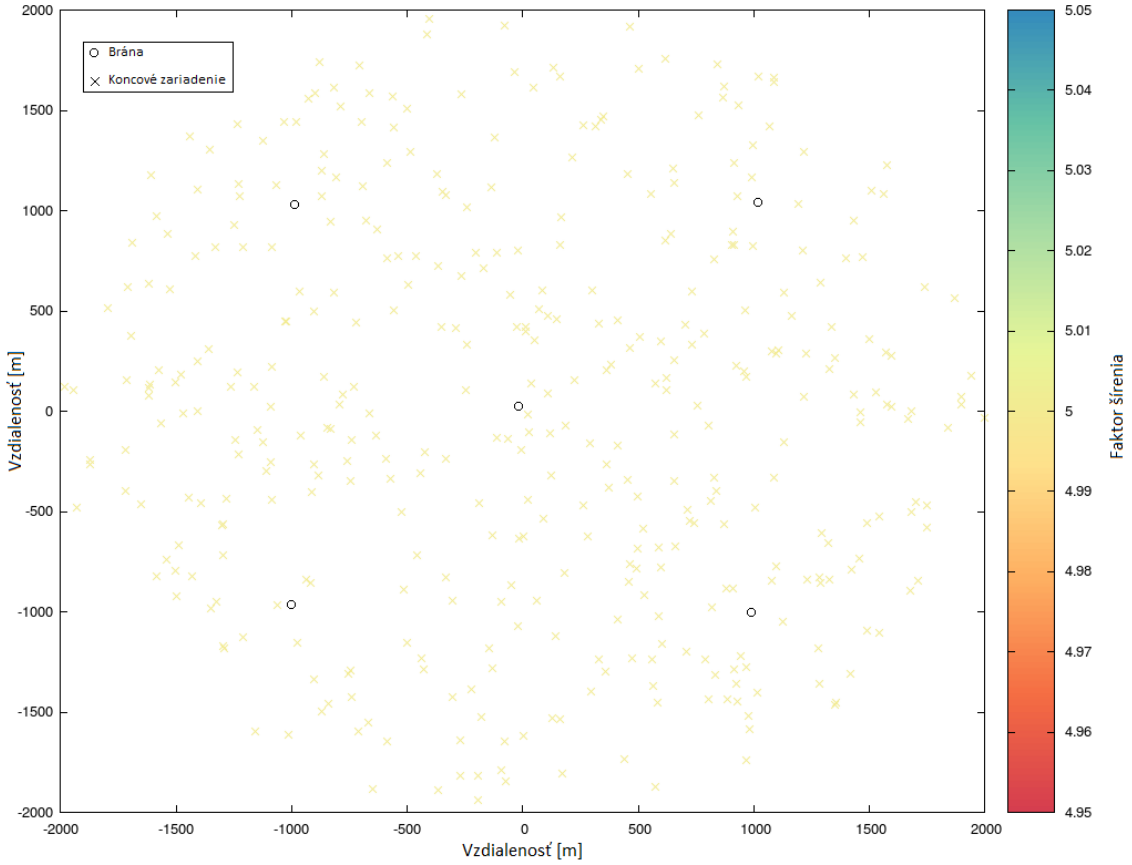


Obr. 6.1: Zobrazenie rozloženia senzorov pre prvý scenár s 20 senzormi.

6.2 Druhý scenár - parkovací dom

Tento scenár simuloval parkovací dom pod štadiónom. Nasadených bolo štyristo senzorov s periódou zhromažďovania dát jedna minúta v parkovacom dome. Dobu trvania simulácie sme nastavili na šesť hodín. Na obrázku 6.2 môžeme vidieť rozloženie daných štyristo senzorov. Rádius siete bol zvolený Senzory sú rozložené v rôznych pásmach faktoru šírenia. Pre túto simuláciu bol vytvorený simulačný script s názvom **lorawan-parking-house.cc**.

Simulovanie takéhoto scenára môže pomôcť k pochopeniu problematiky potreby väčšieho počtu brán pri väčšom počte senzorov. Nasadenie takéhoto spôsobu mo-



Obr. 6.2: Zobrazenie rozloženia senzorov pre druhý scenár s 400 senzormi.

nitorovania do každého parkovacieho domu alebo podobného miesta, môže priniesť okrem výhod popísaných vyššie aj výhodu pri nasadzovaní stratégie predajnej stratégie.

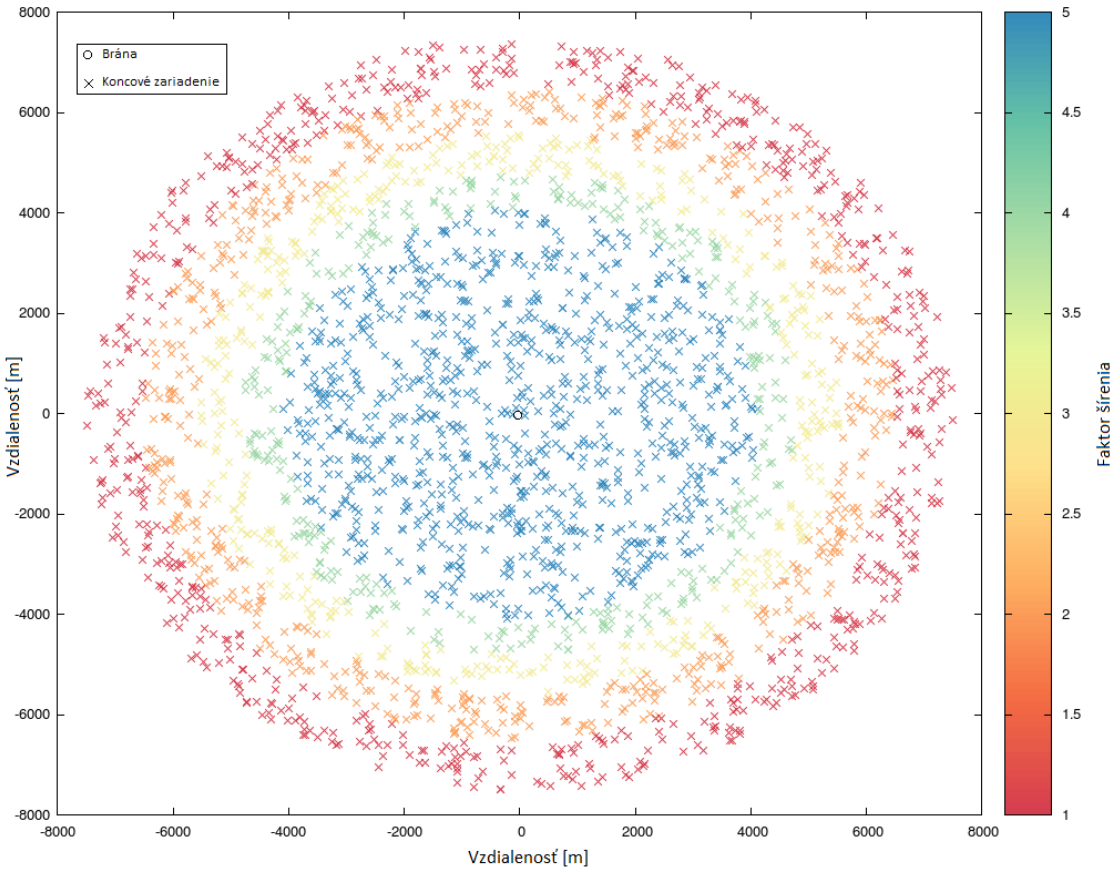
Pri simuláci s 5 bránami bolo prijatých 19421 packetov, zablokovaných 2508 a nedoručených 30. Výsledky merania preukázali, že pri nižšej ploche ale vyššom počte senzorov sa pakety začínajú strácať v sieti. Percentuálny pomer prijatých ku zablokovaným a nedoručeným dosiahol 13%.

6.3 Tretí scenár - 3000 senzorov

Tento scenár môže simulovať prepojenie všetkých senzorov a zariadení vo veľkomeste. Senzory sú odlíšené farebne podľa toho v akom pásme šírenia sa nachádzajú. Pre túto simuláciu bol vytvorený simulačný script s názvom **lorawan-3000-end-device.cc**.

Pri simulácií boli použité parametre: 3000 zariadení; 5 brán; rádius oblasti bol 7,5 km; doba vysielania 1800 sekúnd; perióda vysielania 60 sekúnd. Pri simulácii s

jednou bránou bolo prijatých 3,8 packetov, zablokovaných 0,88 a nedoručených 0,32. Percentuálny pomer prijatých ku zablokovaným a nedoručeným dosiahol 31%.



Obr. 6.3: Zobrazenie rozloženia senzorov pre druhý scenár s 3000 senzormi.

6.4 Rozšírenie modulu LoRaWAN

Do budúcna je možné tento modul rozšíriť o možnosť simulácie bezpečnostných vlastností, ako napríklad vplyv DoS útokov na topológiu. Následne je dobré zistiť vplyv na komunikáciu pri zväčšení záhlavia paketov a akým spôsobom bude ovplyvnená komunikácia v prípade zvýšenia počtu prenášaných správ z dôvodu autentizácie.

7 ZÁVER

Cieľom práce bolo v teoretickej rovine vymedzenie problematiky internetu vecí, kryptografických metód vhodných pre internet vecí. V práci boli popísané protokoly, komunikačné technológie a koncové prvky, ktoré sa využívajú v internete vecí. Boli vymedzené aj hrozby a potencionálne útoky, ktoré sa pri internete vecí môžu vyskytnúť. Popísané kryptografické šifry boli využité pri ich testovaní. Testovanie kryptografických primitív bolo realizované na obmedzenom zariadení Raspberry Pi. Výsledky merania boli zhrnuté do tabuliek a následne graficky spracované a vyhodnotené. Meranie preukázalo výhodnosť využívania Eliptických kriviek v internete vecí oproti konvenčným kryptografickým primitívam. Taktiež preukázalo, že vhodným kandidátom za náhradu AES-CBC módu je prúdová ChaCha20. Následne sme analyzovali vhodnú technológiu vhodnú na prevádzku IoT siete. Taktiež sme si predstavili aj predpoklady na IoT sieť, čo zúžilo rozsah na LPWAN siete. V tejto kapitole sme sa venovali aj bližšej technickej analýze siete LoRa, v ktorej sme si predstavili aj možné bezpečnostné riziká. Možné vylepšenie tejto siete pramení z vylepšenia technológie CPABE a jej nasadenia. Následne sme sa zamerali na sieťový simulátor NS-3 a jeho využitie v IoT. Sieťový simulátor má viaceré funkcionality, ktoré napomáhajú pri modelovaní sietí. Záverečná kapitola predstavila simuláciu LoRaWAN siete. S rastúcim počtom zariadení, napr. senzorov, stúpa zložitosť takejto siete a s tým je spojená aj ztráta paketov v siete, ako sme odsimulovali v tejto kapitole.

Internet vecí je ďalším logickým krokom vo vývoji internetu. Internet vecí zbližuje odvetvia a špecializácie, spája informačné technológie a operačné technológie a prispieva k priemyselnej transformácii (revolúcií) a prináša vlnu prípadov použitia, ktoré sú buď medziodvetvové, alebo typické pre konkrétny sektor. S rastúcim záujmom o internet vecí rastie aj záujem o zvýšenie bezpečnosti internetu vecí. Práve z tohto dôvodu je táto práca, ktorá sa zaoberá bezpečnosťou internetu vecí, prínosom.

LITERATÚRA

[1] *An Overview of Wi-Fi*[online] 9. 12. 2017 [cit. 29. 10. 2017]. Dostupné z URL: <https://www.lifewire.com/what-is-wi-fi-2377430>.

[2] *Announcing the ADVANCED ENCRYPTION STANDARD.* [online]. FIPS PUBS 26. 11. 2001 [cit. 10. 11. 2017]. Dostupné z URL: <https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf>.

[3] ASHTON, K. *That 'Internet of Things' Thing* [Online]. 22. 6. 2009 [cit. 9. 10. 2017] Dostupné z URL: <http://www.rfidjournal.com/articles/view?4986>.

[4] BABAR, S., STANGO, A., PRASAD, N., SEN, J., PRASAD, R. *Embedded Security Framework for Internet of Things (IoT)* [Online]. 2. 2011 [cit. 9. 10. 2017] Dostupné z URL: <https://www.researchgate.net/publication/252013823_Proposed_Embedded_Security_Framework_for_Internet_of_Things_IoT>.

[5] BARKER, E. *Recommendation for Key Management. Part 1: General.* [Online]. National Institute of Standards and Technology 1. 2016 [cit. 28. 3. 2018] Dostupné z URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf>.

[6] BASU, S., S., TRIPATHY, S. *Securing Multicast Group Communication in IoT-Enabled Systems.* [online]. 20. 3. 2018 [cit. 6. 5. 2018]. Dostupné z URL: <http://www.randomnoise.info/2016/06/the-ns-3-architecture-and-abstractions/>.

[7] DIFFIE, W., HELLMAN, M. *Multiuser cryptographic techniques.* [online]. New York 10. 6. 1976 [cit. 10. 11. 2017]. Dostupné z URL: <https://dl.acm.org/citation.cfm?id=1499815>.

[8] *Digitálna bezpečnosť v roku 2016 podľa ESETu: Internet vecí, mobilné zariadenia a ochrana detí* In Computer Networks [online]. 26. 1. 2016 [cit. 12. 10. 2017]. Dostupné z URL: <https://www.eset.com/sk/o-nas/press-centrum/tlacove-spravy/ine/article/digitalna-bezpecnost-v-roku-2016/internet-veci-mobilne-zariadenia-a-ochrana-deti/>.

[9] EISENBARTH, T., KUMAR, S. *A Survey of LightweightCryptography Implementations* [online]. 4. 10. 2007 [cit. 11. 11. 2017]. Dostupné z URL:

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.124.8413&rep=rep1&type=pdf>.

[10] GUPTA, N. *Inside Bluetooth Low Energy. Second Edition.* Boston: Artech House, 2016. 427 s. ISBN 978-1-63081-089-4.

[11] HANKERSON, D., VANSTONE, S., MENEZES, J., A. *Guide to elliptic curve cryptography.* Reprint. New York: Springer, 2011. ISBN 9781441929297.

[12] HUNKELER, U., TRUONG, H., STANFORD-CLARK, A. *MQTT-S – A Publish/Subscribe Protocol For Wireless Sensor Networks* [Online]. 27. 6. 2008 [cit. 12. 10. 2017] Dostupné z URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4554519>.

[13] HYDER, K., PERRIN, B. *Embedded Systems Design using the Rabbit 3000 Microprocessor: interfacing, networking, and application design.* Boston: Newnes, 2005. 458 s. ISBN 0-7506-7872-0.

[14] International Business Machines Corporation (IBM), Eurotech *MQTT V3.1 Protocol Specification* [Online]. [cit. 10. 10. 2017] Dostupné z URL: <http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html>.

[15] KULKARNI, V., KALMANI, S., VERNEKAR, S. Secured *Hash2 based Message Authentication Code using GUI Controls.* [online]. 8. 2013 [cit. 6. 4. 2018]. Dostupné z URL: <https://www.semanticscholar.org/paper/Secured-Hash2-based-Message-Authentication-Code-GUI-Kulkarni-/Kalmani/a0a3e0a7d2bbeb3d70e0c9e8a10eccf7fd48d19e>.

[16] LEVICKÝ, D. *Kryptografia v informačnej bezpečnosti.*. Košice: Elfa, 2005. ISBN 80-8086-022-X.

[17] LEENT, V., M. *An improved key distribution and updating mechanism for low power wide area networks (LPWAN).* Cyber Security Academy [online]. 18 1. 2017 [cit. 4. 1. 2018]. Dostupné z URL: <https://www.csacademy.nl/images/scripties/2017/Van-Leent-An-improved-key-distribution-and-updating-mechanism-/for-low-power-wide-a-1.pdf>.

[18] LORA ALLIANCE *What is LoRa?.*[online] 10. 2010 [cit. 30. 10. 2017]. Dostupné z URL: <https://www.lora-alliance.org/technology>.

[19] *LoRa Protocol Stack-LoRa Physical layer, LoRa MAC layer* [online]. [cit. 12. 2. 2018]. Dostupné z URL: <http://www.rfwireless-world.com/Tutorials/LoRa-protocol-stack.html>.

[20] *LoRaWAN Classes | Class A,Class B,Class C | RF Wireless World* [online]. [cit. 22. 2. 2018]. Dostupné z URL: <http://www.rfwireless-world.com/Tutorials/LoRaWAN-classes.html>.

[21] MÁCHA, M. *LoRa Technology.*[online] 10. 2010 [cit. 29. 10. 2017]. Dostupné z URL: <http://www.osel.cz/8732-lora-technology.html>.

[22] MEKKI, K., BAJIC, E., CHAXEL, F., MEYER, F., *A comparative study of LPWAN technologies for large-scale IoT deployment.* [Online]. ICT Express 4. 1. 2018 [cit. 25. 3. 2018] Dostupné z URL: <https://www.sciencedirect.com/science/article/pii/S2405959517302953#b14>.

[23] MIČEK, J. *Bezdrôtové senzorické siete – súčasnosť, perspektívy, aplikácie.* [online]. [cit. 5. 10. 2017]. Dostupné z URL: <http://www.atpjournal.sk/buxus/docs/atp_journal_10_2011_str_49.pdf>.

[24] *Mqtt.org* [online] MQTT community, 2014 [cit. 7. 10. 2017]. Dostupné z URL: <http://mqtt.org/>.

[25] *Near Field Communication Technology Standards.*[online] [cit. 29. 10. 2017]. Dostupné z URL: <http://nearfieldcommunication.org/technology.html>.

[26] NIR, Y., LANGLEY, A. *ChaCha20 and Poly1305 for IETF Protocols. RFC 7539*[online] Google, Inc. 5. 2015 [cit. 4. 3. 2018]. Dostupné z URL: <https://tools.ietf.org/html/rfc7539>.

[27] NIST Special Publication 800-131A Revision 1, *Transition: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.* [Online]. . 11. 2015 [cit. 17. 3. 2018] Dostupné z URL: <http://dx.doi.org/10.6028/NIST.SP.800-131Ar1.>.

[28] NORDRUM, A. *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated* [Online]. 18. 8. 2016 [cit. 9. 10. 2017] Dostupné z URL: <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-device/by-2020-is-outdated>.

[29] *NS-3 Tutorial.* [online]. 14. 3. 2017 [cit. 6. 3. 2018]. Dostupné z URL: <https://www.nsnam.org/docs/release/3.26/tutorial/ns-3-tutorial.pdf>.

[30] *Opel Onstar* [online]. [cit. 5. 10. 2017]. Dostupné z URL: <http://www.opel.sk/onstar/onstar.html>.

[31] *RFID tagging*[online] 10. 2010 [cit. 29. 10. 2017]. Dostupné z URL: <http://internetofthingsagenda.techtarget.com/definition/RFID-tagging>.

[32] ROBSHAW, M., BILLET, O. *New stream cipher designs the eSTREAM finalists.* Berlin: SpringerLink , 2008. ISBN 978-3-540-68351-3.

[33] RODRIGO, R., NAJERA, P., LOPEZ, J. *Securing the Internet of Things* In Computer [online]. 12. 9. 2011 [cit. 17. 11. 2017]. Dostupné z URL: <http://ieeexplore.ieee.org/document/6017172/>.

[34] ROUSE, M. *Internet Key Exchange (IKE)* [Online]. [cit. 25. 11. 2017] Dostupné z URL: <http://searchsecurity.techtarget.com/definition/Internet-Key-Exchange>.

[35] SAHRAOUI, S., BILAMI, A. *Efficient HIP-based approach to ensure lightweight end-to-end security in the internet of things* In Computer Networks [Online]. 20. 8. 2015 [cit. 25. 11. 2017] Dostupné z URL: <http://searchsecurity.techtarget.com/definition/Internet-Key-Exchange>.

[36] SAIED, B., Y., OLIVEREAU, A., ZEGHLACHE, D., LAURENT, M. *Lightweight collaborative key establishment scheme for the Internet of Things* In Computer Networks [online]. 18. 2. 2014 [cit. 17. 11. 2017]. Dostupné z URL: <http://www.sciencedirect.com/science/article/pii/S1389128614000437#b0195>.

[37] SCHATZ, G. *SigFox Vs. LoRa: A Comparison Between Technologies & Business Models.* [Online]. 13. 1. 2016 [cit. 15. 10. 2017]. Dostupné z URL: <https://www.link-labs.com/blog/sigfoxvs-lora>.

[38] SHELBY, Z., HARTKE, K., BORMANN, C. *The Constrained Application Protocol (CoAP). RFC 7252*[online] Bremen: Universita et Bremen . 6. 2014 [cit. 7. 10. 2017]. Dostupné z URL: <https://tools.ietf.org/html/rfc7252>.

[39] *Simplecell networks slovakia a.s, "Technológia SIGFOX"* [Online]. [cit. 15. 10. 2017] Dostupné z URL: <http://www.simplecell.sk/pages/technologia_sigfox/>.

[40] SINHA, R., S., WEI, Y., Hwang, S., *A survey on LPWA technology: LoRa and NB-IoT.*[online] Dongguk University-Seoul, Republic

of Korea. 14 3. 2017 [cit. 15. 4. 2018] Dostupné z URL: <https://ac.els-cdn.com/S2405959517300061/1-s2.0-S2405959517300061-main.pdf?_tid=58283584-906d-4a71-91f2-89491d22f319&acdnat=1526551208_dbe727d7f2e991a5aa7a4f26a57c41b6>.

[41] SPASOV, P. *Microcontroller technology, the 68HC11 and 68HC12. 5th ed.*. Upper Saddle River, N.J.: Pearson/Prentice Hall, 2004. 712 s. ISBN 0-13-112984-8.

[42] *The NS-3 Architecture and Abstractions.* [online]. 6. 10. 2016 [cit. 6. 3. 2018]. Dostupné z URL: <http://www.randomnoise.info/2016/06/the-ns-3-architecture-and-abstractions/>.

[43] *TLS Handshake Protocol* [Online]. [cit. 25. 11. 2017] Dostupné z URL: <https://msdn.microsoft.com/en-us/library/windows/desktop/aa380513(v=vs.85).aspx>.

[44] VAN OORSCHOT, P., C., VANSTONE, S., A., MENEZES, J., A. *Guide to elliptic curve cryptography.* Boca Raton: CRC Press, 1997. ISBN 0-8493-8523-7.

[45] VOCAL Technologies *Datagram Transport Layer Security (DTLS)* [online]. [cit. 5. 11. 2017]. Dostupné z URL: <https://www.vocal.com/networking/datagram-transport-layer-security-dtls/>.

[46] *What is the LoRaWAN™ Specification?* [online]. [cit. 17. 2. 2018]. Dostupné z URL: <https://lora-alliance.org/about-lorawan>.

ZOZNAM PRÍLOH

A OBSAH PRILOŽENÉHO CD

- Zip archív sieťového simulátora NS-3 v3.28 s modulom lorawan.
- Diplomová práca v súbore BezpecnaAutentizaciaAKlucovyManagementVInterneteVeci.pdf