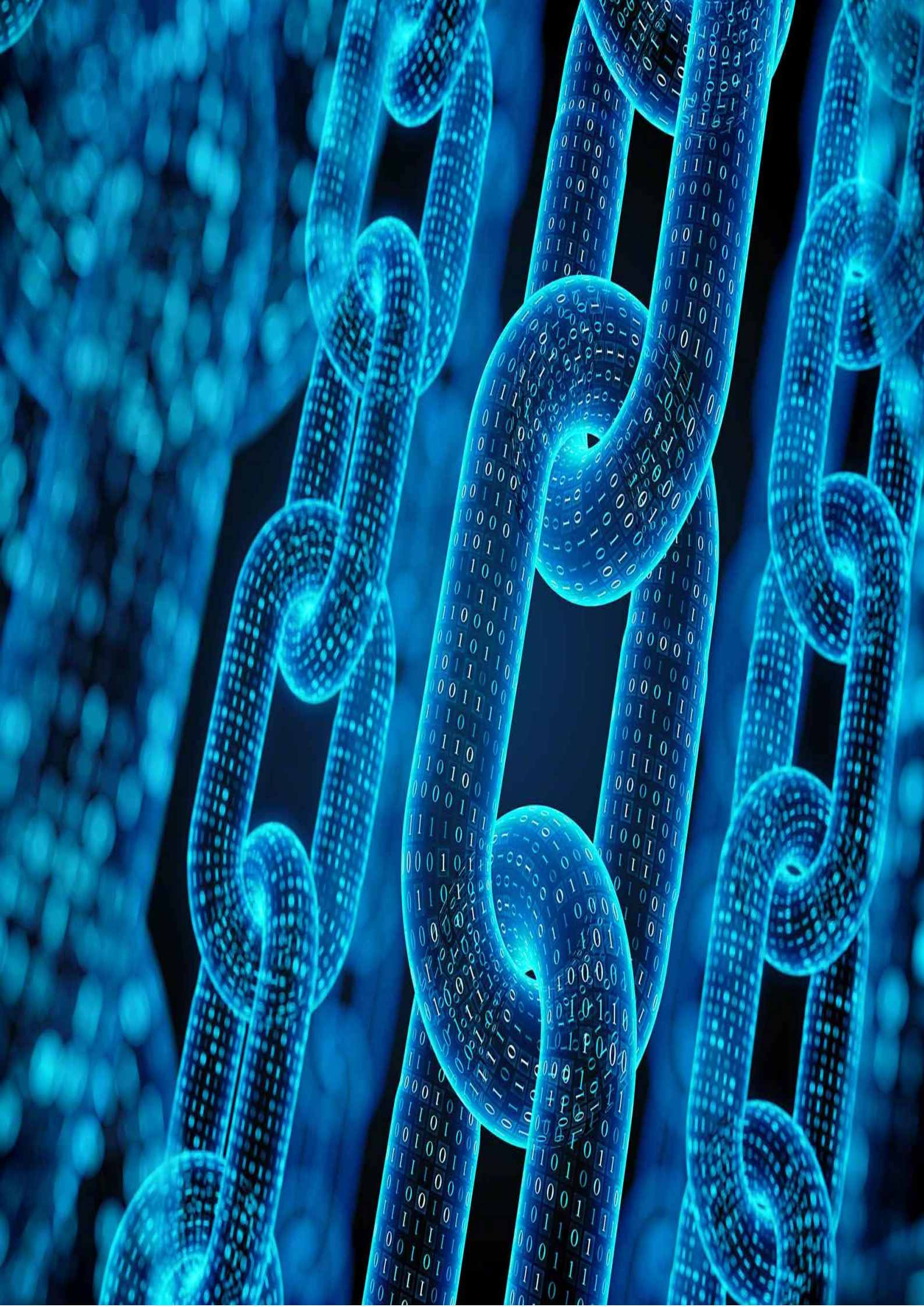




**FAKULTA INFORMATIKY A INFORMAČNÝCH TECHNOLOGIÍ
SLOVENSKÁ TECHNICKÁ UNIVERZITA BRATISLAVA**

Jaroslav Erdelyi

Auto referát dizertačnej práce

Komunikácia v prostredí Internetu vecí

na získanie akademického titulu philosophiae doctor - PhD

v doktorandskom študijnom programe aplikovaná informatika D-AI

v študijnom odbore aplikovaná informatika D-AI

Forma štúdia Denná

Miesto a dátum Bratislava 15.12.2021

Dizertačná práca bola vypracovaná na Ústave počítačového inžinierstva a aplikovanej informatiky Fakulty informatiky a informačných technológií v Bratislave v študijnom odbore aplikovaná informatika

Predkladateľ: Ing. Jaroslav Erdelyi

Ústav počítačového inžinierstva a aplikovanej informatiky
Fakulta informatiky a informačných technológií
Ilkovičová 2, 842 16 Bratislava

Školiteľ: prof. Ing. Pavel Čičák, PhD..

Ústav počítačového inžinierstva a aplikovanej informatiky
Fakulta informatiky a informačných technológií
Ilkovičová 2, 842 16 Bratislava

Oponenti: prof. Ing. Milan Dado, PhD.

Katedra multimédií a informačno-komunikačných technológií
Fakulta elektrotechniky a informačných technológií
Univerzitná 8215/1, 010 26 Žilina

doc. Ing. Peter Fecil'ák, PhD.

Katedra počítačov a informatiky
Fakulta elektrotechniky a informatiky
Letná 9, 040 01 Košice

Auto referát bol rozoslaný

Obhajoba dizertačnej práce sa bude konať dňao.....h na ústave aplikovanej informatiky Fakulty informatiky a informačných technológií v Bratislave (Ilkovičová 2, 842 16 Bratislava)

prof. Ing. Ivan Kotuliak, PhD.

Dekan FIIT STU Bratislava

Abstrakt

Dizertačná práca prezentuje výskum architektúry na zabezpečenie senzorovej siete v IoT prostredí, pomocou ktorej chceme zvýšiť bezpečnosť v sieti a kvalitu poskytovaných služieb. V rámci súčasného stavu poznania sme zistili, že dôležitou vlastnosťou prostredia Internetu vecí je poskytovanie kvality služieb. To sa dá dosiahnuť zlepšením výpočtových algoritmov pre poskytovanie kvality služieb alebo zvýšením zabezpečenia komunikácie v IoT sieti. Preto sme v rámci práce navrhli bezpečnostnú architektúru. Architektúra na zlepšenie bezpečnosti využíva známe prístupy (synchronizácia vysielania, šifrovanie komunikácie) a technológiu blockchain, ktorá bola upravená. Výskum práce je zameraný na zvýšenie bezpečnosti komunikácie v IoT sieti. Na zvýšenie bezpečnosti sme vytvorili bezpečnostnú architektúru, kde sme pozorovali, aké zahltenie vytvára v sieti blockchain s rôznymi konsenzuálnymi algoritmami, aké hrozby vieme pomocou architektúry odhaliť a aké šifry sú vhodné pre prostredie Internetu vecí. Na základe skúmania sme zistili, že v rámci architektúry vieme efektívnejšie detegovať napadnutie siete. Dôsledkom je, že sieť sa dokáže z útoku rýchlejšie zotaviť a ďalej kvalitne poskytovať služby.

Obsah

1	Úvod.....	1
2	Súčasný stav	2
2.1	Vlastnosti Internetu vecí	2
2.1.1	Architektúry v IoT.....	2
2.1.2	Aplikačné riešenia	3
2.2	Komunikačné technológie a protokoly	3
2.3	Kvalita služieb	4
2.4	Bezpečnosť	5
3	Ciele dizertačnej práce	7
4	Bezpečnostná architektúra.....	8
4.1	Dôležité bezpečnostné prvky	9
4.2	Dôkaz funkčnosti bezpečnostného procesu	10
4.3	Dôkaz bezpečnosti blockchain technológie.....	12
5	Experimentálne výsledky	14
5.1	Opis prototypov	14
5.2	Experimentálne merania	14
5.2.1	Sieťové zahltenie	14
5.2.2	Odozva bezpečnostného modulu.....	17
5.2.3	Dopady šifrovania na IoT zariadenia	18
5.3	Porovnanie	19
6	Zhodnotenie.....	20
7	Použitá literatúra	22
8	Publikačná činnosť	24

1 Úvod

V dnešnej dobe sa dostáva v informatike do popredia pojem Internet vecí. Internet vecí je prostredie, v ktorom sú prepojené rôzne zariadenia, ktoré sa dokážu pripojiť k Internetu. Každým dňom sa pripojí do Internetu vecí viac a viac zariadení. Tieto zariadenia sú často prenosné, dokážu sa napájať pomocou externého elektrického zdroja alebo priamo z elektrickej siete a dokážu komunikovať medzi sebou bezdrôtovo. Tieto zariadenia musia medzi sebou komunikovať. Komunikácia týchto zariadení, preto musí byť bezpečná, musí byť aj energeticky nenáročná. Zároveň sieť musí zachovať poskytovanie kvality služieb pre zariadenia v IoT sieti. V súčasnosti existuje veľa spôsobov, ako komunikovať v prostredí Internetu vecí a ako zlepšiť poskytovanie kvality služieb. Preto je výskum práce zameraný na problém poskytovania kvality služieb. Tento problém priamo ovplyvňuje komunikáciu v prostredí Internetu vecí. Tento problém je v rámci IoT prostredia priamo prepojený s poskytovaním kvality služieb. Jedná sa o to, že ak je zariadenie, služba alebo sieť napadnutá útokom, tak prestane fungovať, čiže sa výsledkom je nedostupnosť zariadenia, služby alebo siete. Jedným z princípov bezpečnosti je práve dostupnosť služby. Zachovaním tohto princípu v IoT prostredí umožníť poskytovanie služieb. Výskum práce je venovaný tomu, aby sa rýchlo zotavila služba, zariadenie alebo sieť z útoku. Tým, že sa urýchli zneškodnenie útoku sa priamo zvýši dostupnosť služby a takisto sa zlepši poskytovanie služby. Na urýchlenie odhalenia útoku je preto potrebné zvýšiť bezpečnosť.

2 Súčasný stav

Z pohľadu komunikácie v prostredí Internetu vecí (IoT) bola analyzovaná komunikácia a prostredie Internetu vecí, aby sa na základe analýzy boli správne identifikované problémy. Z tohto dôvodu sme sa najprv zamerali na prostredia ako také. Následne sme upriamili pozornosť na komunikačné technológie a protokoly a na konci sme tieto dve celky spojili, za účelom hlbšej analýzy a identifikovania problému.

2.1 Vlastnosti Internetu vecí

Vlastnosti IoT prostredia nám definujú charakter tohto prostredia a vieme na základe nich predikovať aké potenciálne problémy sa môžu v tomto prostredí vyskytnúť. Medzi základné vlastnosti IoT prostredia radíme týchto päť [21]:

- mobilita,
- škálovateľnosť,
- životnosť,
- komunikácia zariadení,
- multihopping.

Tieto vlastnosti nám hovoria o tom, že zariadenia majú istú životnosť lebo sú napojené na externom zdroji energia. Takisto z týchto vlastností vieme určiť, že sieť je vďaka mobilite vysoko dynamická a nemá žiadnu sieťovú topológiu. Škálovateľnosť nám zas hovorí o tom, že do siete vieme rýchlo pridávať zariadenia ale aj rýchlo odoberať, čo nám zvyšuje kolízie v sieti. Preto na základe týchto vlastností je nutné pozrieť si potreby jednotlivých aplikačných riešení v IoT prostredí.

2.1.1 Architektúry v IoT

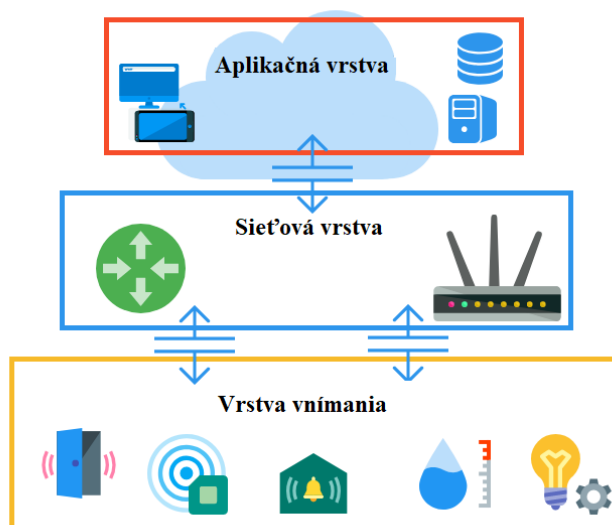
Vo všeobecnosti, architektúra ako prvok nám dáva abstraktný pohľad na fungovanie IoT prostredia. Z tohto pohľadu nám dáva abstraktný nadhľad na fungovanie komunikácie v prostredí IoT a na vzťah aplikačných riešení voči technológiám a naopak. V rámci IoT prostredia neexistuje žiadny konsenzus ohľadom jednotnej architektúry v prostredí IoT, na ktorom by sa zhodli všetci. Preto sa používajú rôzne typy architektúr (systémové, sieťové a iné).

Najznámejšia je trojvrstvová architektúra [1][2](obr. č. 1). Obsahuje tri vrstvy a to vrstvu vnímania (perception), sieťovú a aplikačnú. Vrstva vnímania je v podstate fyzická vrstva, kde senzory snímajú a zbierajú informácie. Sieťová je zodpovedná za prepojenie zariadení, prenos a spracovanie údajov. Aplikačná má na starosti doručenie služieb používateľovi. Táto architektúra však nemusí byť postačujúca, hlavne čo sa týka výskumu, pretože výskumníci potrebujú detailnejšie oddelenie niektorých vrstiev.

Druhou architektúrou používanou v IoT prostredí je IoT Stack [3]. Táto architektúra má viac vrstiev, ktoré sú detailnejšie špecifikované. Primárne IoT Stack architektúra slúži na používanie IPv6 protokolu v IoT prostredí. Jednotlivé vrstvy sú:

- fyzická vrstva – IEEE 802.15.4 PHY,
- MAC vrstva – IEEE 802.15.4 MAC,
- adaptačná vrstva – 6LoWPAN,
- sieťová vrstva – Ipv6,

- transportná vrstva – UDP,
- aplikačná vrstva – CoAP.



Obr. č. 1 – Všeobecná architektúra Internetu vecí¹

2.1.2 Aplikačné riešenia

V súčasnosti sa aplikácie Internetu vecí objavujú v mnohých prostrediach a riešeniach, s ktorými sú ľudia v bežnom kontakte. Tieto aplikácie pre svoju funkčnosť potrebujú rôzne parametre z pohľadu objemu prenosu údajov, odozvy prenosu údajov, bezpečnosti údajov a zariadení a pod. Medzi najčastejšie aplikácie Internetu vecí [4][5][6] patria:

- Smart City (inteligentné mestá),
- Smart Home (inteligentný dom),
- Smart Agriculture (alebo Smart Farming – inteligentné poľnohospodárstvo),
- Smart Metering (tu patrí Smart Grid a podobné aplikácie),
- Security and Emergency (bezpečnosť a pohotovosť),
- Retail and Logistics (maloobchod a logistika),
- Intelligent Transportation System (inteligentné dopravné systémy),
- eHealth (zdravie),
- Wearables (nositeľné zariadenia, ako rôzne smartfóny, hodinky ...)
- Smart Environment Monitoring (inteligentné monitorovanie životného prostredia).

2.2 Komunikačné technológie a protokoly

Na základe analýzy vlastností prostredia Internetu vecí a použitých aplikačných riešení sa ukázalo, že aplikačné riešenia potrebujú škálu parametrov pre správne fungovanie s tým, že pre väčšinu aplikačných riešení sú tieto parametre rozdielne. Napríklad Smart Metering nepotrebuje rýchlu odozvu pri prenose údajov a e-Health aplikačné riešenie potrebuje

¹ <https://www.netburner.com/learn/architectural-frameworks-in-the-iiot-civilization/>

realizovať prenos údajov v reálnom čase. Preto sme sa v rámci komunikačných protokolov a technológií sústredili na tieto vlastnosti:

- prenosová rýchlosť,
- dosah,
- zabezpečenie komunikácie,
- frekvencia,
- poskytovanie QoS služieb.

Celkové zhodnotenie a porovnanie komunikačných technológií a protokolov môžete vidieť v *Tabuľke 1*.

Názov	Prenosová rýchlosť	Vysielací dosah	Zabezpečenie komunikácie	QoS služby	Frekvencia
IEEE 802.11 - WiFi	6 Gbit/s	100 metrov	AES-256 + WPA3	WME, WMS	2,4 GHz - 6GHz
IEEE 802.16 - WiMAX	70 Mbit/s	10 km	PKMv2 + EAP protokol	pomocou tokov služieb	2 GHz - 66 GHz
IEEE 802.15.1 - Bluetooth	1 Mbit/s	150 metrov	E0-128 šifrovací algoritmus	mechanizmus dopytovania	2,4 GHz
Rozšírený ISO/IEC 14443 - NFC	420 kbit/s	10 cm	---	---	13,56 MHz
ISO/IEC FDIS 18000-7:2014 - RFID	4 Mbit/s	100 metrov	---	MuteQ	125 kHz - 5.875 GHz
3G	14 Mbit/s	200 km	O&M IP vrstva, aplikačná vrstva	monitoring, policy provisioning	900 MHz - 2,1 GHz
4G	1 Gbit/s	100 km	KASME	e-Node B + QCI, ARP	700 MHz - 2,6 GHz
5G	20 Gbit/s	500 metrov	NEA128 + RFC 5448	pomocou tokov služieb + QFI	600 MHz - 76 GHz
ZigBee	250 kbit/s	100 metrov	128 bitové kľúče	delenie rádiových frekvencií	2,4 GHz
Z-Wave	100 kbit/s	30 metrov	AES	XXX	900 MHz
6LoWPAN	---	---	AES	IPv6 TF bity	XXX
Thread	250 kbit/s	30 metrov	---	---	2,4 GHz
Sigfox	100 kbit/s	50 km	---	---	868 MHz
LoRaWAN	50 kbit/s	15 km	EUI128	---	433 MHz - 928 MHz

Tabuľka č. 1 – vlastnosti komunikačných technológií a protokolov

2.3 Kvalita služieb

Na základe vlastností Internetu vecí, komunikačných požiadaviek aplikačných riešení a analýze komunikačných protokolov a technológií nám vyplynulo, že poskytovanie kvality služieb (QoS [7]) v prostredí Internetu vecí má významný dopad na komunikáciu. Kvalitu služieb ovplyvňuje veľa rôznych mechanizmov. Najzákladnejším mechanizmom ktorý ovplyvňuje poskytovanie kvality služieb sú prístup k médiu a zdrojom a algoritmy na výpočet

parametrov potrebných na poskytovanie QoS služieb pre potreby aplikačného riešenia. Ďalšími významnými vplyvmi, ktoré majú dopad na poskytovanie QoS služieb, sú:

- smerovanie,
- bezpečnosť,
- rozdelenie rádiových frekvencií,
- rozloženie záťaže v sieti.

Pri hlbšom skúmaní sa zistilo, že zásadným vplyvom z vyššie spomenutých je práve bezpečnosť. Z bezpečnosti je známy princíp dostupnosti, ktorý musí byť dodržaný. V literatúre [8] a [9] autori uvádzajú, že pojmy poskytovanie služby a kvalita služby (QoS) v IoT prostredí sú reprezentované tým istým pojmom.

2.4 Bezpečnosť

Na základe analýzy prostredia IoT, komunikačných potrieb aplikačných riešení a kvality služieb sa ukázalo, že bezpečnosť je s komunikačného hľadiska prepojená s poskytovaním QoS služieb hlbšie ako iba šifrovanie prenášaných údajov. V rámci prepojenia QoS a bezpečnosti je dôležité zachovať princíp dostupnosti. Preto je bezpečnosť jednou z kľúčových zložiek poskytovania QoS služieb. Z pohľadu bezpečnosti v IoT existuje mnoho zraniteľností, ktoré sú zdedené z Internetu a vďaka použitiu bezdrôtových komunikačných technológií a nízko výkonných zariadení napájaných pomocou externého zdroja energie sa objavili ďalšie zraniteľnosti. Existujú bezpečnostné nástroje pomocou, ktorých vieme sieť zabezpečiť voči útokom z vonku. Sú to nástroje:

- šifrovacie algoritmy,
- firewall [10],
- honeypot [11],
- SIEM systémy [12],
- IDS a IPS systémy [13],
- blockchain [14].

Z pohľadu existujúcich výskumných riešení sme v rámci práce analyzovali dva typy výskumných riešení:

- riešenie zabezpečujúce komunikáciu pomocou blockchain technológie,
- IDS riešenia využívajúce blockchain technológiu na zdieľanie informácií.

Riešenia zabezpečujúce komunikáciu pomocou blockchain technológie sú primárne riešenia v Smart Home prostredí [15]. Základný princíp týchto riešení je, že v sieti existuje ťažiacie zariadenie (angl. *mining device*), ktoré ťaží bloky a transakcie. Transakcia v tomto prípade predstavuje komunikáciu medzi dvomi zariadeniami. Jedno zariadenie ide komunikovať s iným zariadením, tak sa pomocou blockchain technológie overia zariadenia a komunikácia môže prebiehať. Problém v týchto riešeniach je ťažiaci stroj, ktorý potenciálne predstavuje bod zlyhania. Ak zlyhá ťažiaci stroj, tak komunikácia dvoch zariadení nie je overená a je nezabezpečená.

IDS riešenia využívajúce blockchain technológiu na zdieľanie informácií [16] sú riešenia, kde viac IDS systémov spolupracuje ako jeden systém. Pri tejto spolupráci si tieto IDS systémy potrebujú vymieňať informácie, nové pravidlá, logy o útokoch a ďalšie údaje. Na

bezpečné zdieľanie týchto všetkých informácií využívajú blockchain technológiu. Vďaka tomu vedia potom všetky spolupracujúce IDS systémy lepšie vyhodnocovať útoky z vonkajšieho prostredia a následne im zabráňovať alebo im predchádzať. Nevýhodou je, že stále nedostatočne ochraňujú sieť voči útoku z vnútra siete.

Z analýzy týchto nástrojov nám vyplynulo, že existujúce nástroje a existujúce výskumné riešenia poskytujú ochranu siete voči útočníkom útočiacich z vonkajšieho prostredia. Identifikovali sme, že vnútorné napadnutie siete tieto riešenia nevedia efektívne zachytiť a je to problém, ktorý sme v rámci výskumu dizertačnej práce riešili.

3 Ciele dizertačnej práce

Na základe uvedeného stavu poznania sme zistili, že pre kvalitnú komunikáciu v prostredí Internetu vecí potrebujeme zaistiť bezpečnosť komunikácie a poskytovanie QoS služieb. Následne v hlbšej analýze poskytovania QoS a bezpečnosti sme zistili, že poskytovanie QoS a bezpečnosť komunikácie a siete sú hlboko prepojené. V rámci toho sme analyzovali existujúce možnosti zabezpečenia siete, ktoré ochraňujú sieť voči útokom z vonkajšieho prostredia. Zistili sme, že tieto riešenia neposkytujú dostatočnú ochranu voči útokom z vnútra siete. Existujúce prístupy pre zabezpečenie IoT siete sú častokrát energeticky náročné a neprispôsobené pre prácu v IoT sieti, čo takisto znižuje dostupnosť. Preto naším hlavným cieľom v dizertačnej práci je zlepšiť poskytovanie QoS služieb v prostredí Internetu vecí. To dosiahneme priamo pomocou toho, že urýchlíme zotavenie siete po útoku z vnútra siete. Výsledkom je, že dostupnosť služieb je zvýšená, čím je priamo dosiahnuté zlepšenie poskytovania QoS služieb v sieti. Preto na naplnenie hlavného cieľa dizertačnej práce, chceme upraviť existujúce bezpečnostné prístupy a technológie pre IoT prostredie, aby sme zlepšili poskytovanie QoS služieb v IoT sieťach. Zároveň pre naplnenie hlavného cieľa práce je potrebné vytvoriť aj nové bezpečnostné procesy pre zabezpečenie IoT siete.

Ciele a úlohy dizertačnej práce sú rozdelené na nasledujúce časti:

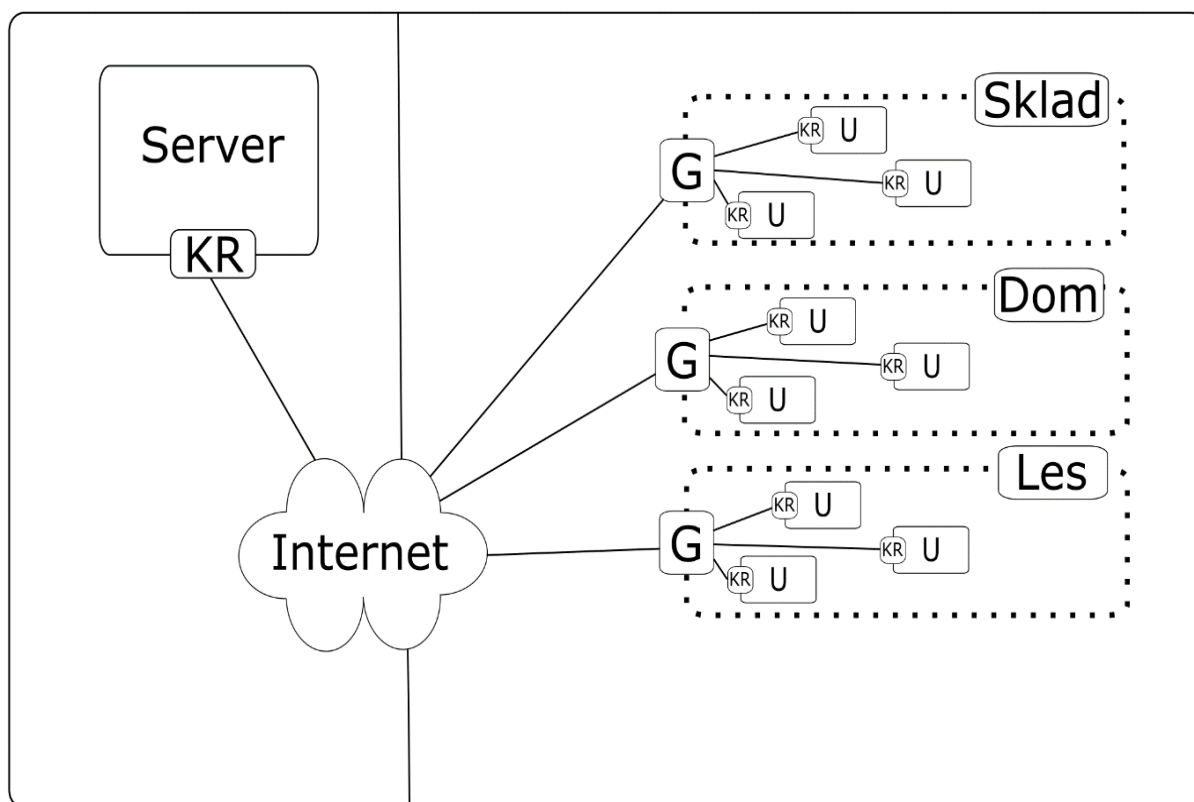
- Navrhnutie úprav v rámci existujúcich prvkov, ktoré sa používajú v rámci rôznych riešení na zabezpečenie alebo zlepšenie komunikácie a využitie týchto upravených existujúcich prvkov v rámci navrhovanej bezpečnostnej architektúry. Vytvorenie ďalších bezpečnostných procesov pre lepšie zabezpečenie siete – ukladanie kľúčov na zariadenie a pod.
- Vytvorenie architektúry pre zabezpečenie siete na zvýšenie dostupnosti siete a poskytovanie služieb v rámci IoT senzorovej siete. Navrhnutá architektúra využije vlastnosti IDS systémov a blockchain-ovej technológie na lepšiu detekciu hrozieb a útočníkov v sieti.
- Implementovanie navrhovanej architektúry do programového riešenia a testovanie výsledného riešenia. Následne overenie vlastností architektúry z pohľadu časovej náročnosti (rýchlosť odhalenia útoku, vytvorenie, overenie a vloženie bloku do siete), odhaľovania útokov a komunikačná spôsobilosť siete (aké zahltenie siete je generované v rámci bezpečnostných procesov).
- Porovnanie dosiahnutia konsenzu v rámci blockchain technológie a zhodnotenie, ktorý z testovaných konsenzuálnych algoritmov je najviac spôsobilý pre IoT sieť. Testovanie bezpečnostných princípov (či je lepšie generovanie kľúča na zariadení, distribuovaný výpočet kľúča v sieti, alebo generovanie kľúča na serveri) a ich spôsobilosť pre IoT zariadenia, aby sme zistili, ktorý z daných riešení zaťažuje IoT zariadenia najmenej. Porovnanie navrhovanej architektúry voči analyzovaným výskumným riešeniam, najmä porovnanie voči riešeniam, ktoré implementujú IDS systémy pomocou blockchain technológie.

4 Bezpečnostná architektúra

Za účelom vyriešenia identifikovaného problému spojeného s poskytovaním QoS služieb v IoT prostredí bola vytvorená **bezpečnostná architektúra**. Táto architektúra (obr. 2) pozostáva z dvoch častí, ktoré komunikujú cez Internet. Tieto časti sú:

- **sieťová časť** – zodpovedná za manažovanie siete, udržiavanie blockchain siete, zbieranie údajov z prostredia pomocou senzora, obojsmerná šifrovaná komunikácia so serverom,
- **serverová časť** – zodpovedná za nastavovanie siete, prístup k uloženým údajom, ktoré boli prijaté zo siete, fungovanie bezpečnostného procesu, manažovanie kľúčov.

Obidve časti využívajú už existujúce prístupy na zabezpečenie siete. Niektoré z týchto procesov a prístupov boli upravené pre potrebu optimalizácie pre IoT prostredie. V rámci architektúry boli navrhnuté aj nové procesy. Za najdôležitejšie procesy a prístupy pre fungovanie bezpečnostnej architektúry považujeme bezpečnostný proces na identifikáciu útočníka v sieti a upravený blockchain, ktorý udržiava v sieti záznamy potrebné na odhalenie útočníka.



Legenda:

KR - komunikačné rozhranie

G - Gateway

U - Uzol

Obr. č. 2 – Celkový pohľad na navrhovanú architektúru

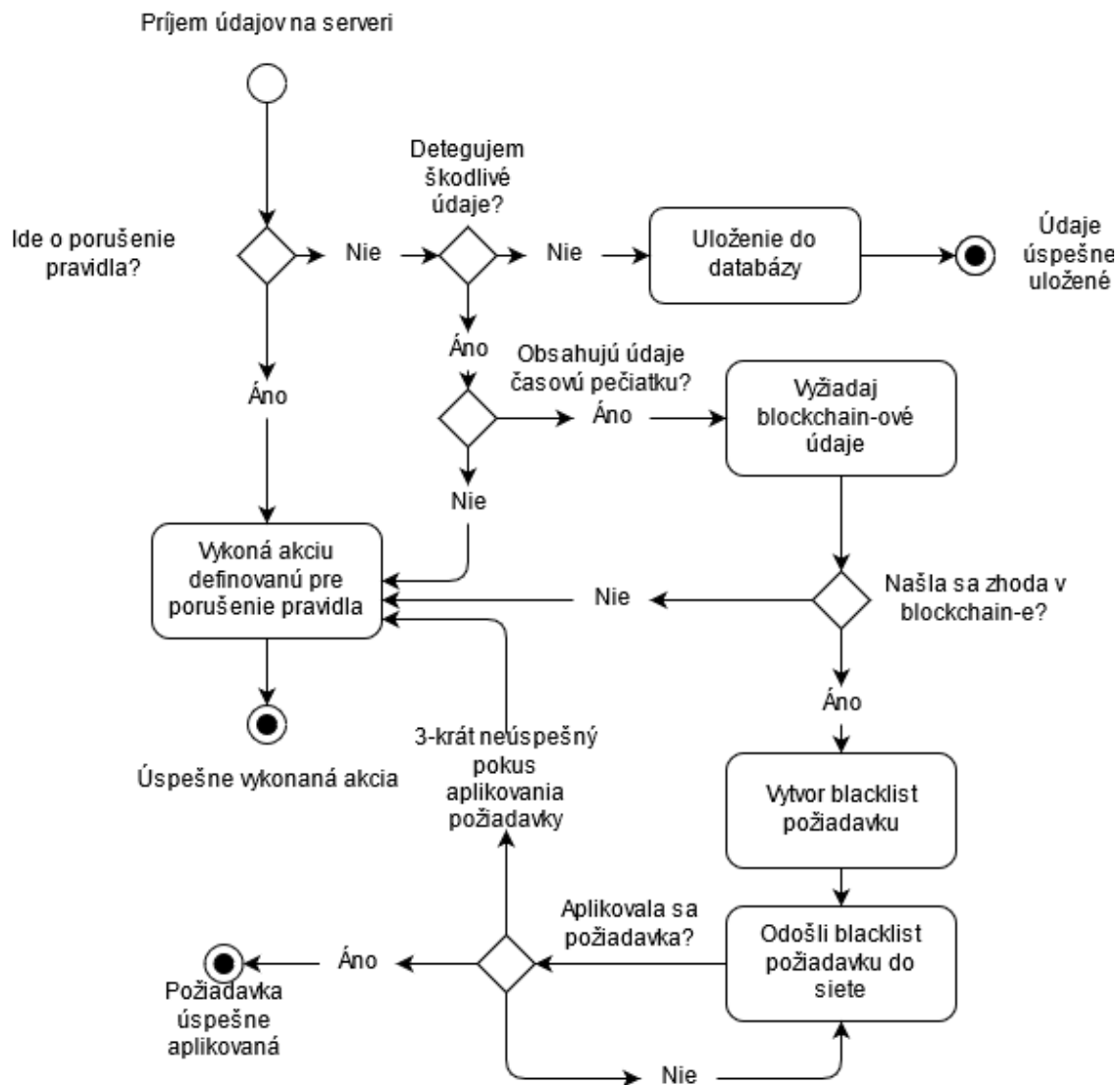
4.1 Dôležité bezpečnostné prvky

Ako sme uviedli vyššie, za najdôležitejšie prvky navrhovanej bezpečnostnej architektúry považujeme upravený blockchain a bezpečnostný proces. Tieto dva prvky tvoria základ celej bezpečnosti v rámci architektúry. Boli navrhnuté tak aby brali ohľad na nízko výkonové zariadenia v IoT prostredí a generovali čo najmenšiu sieťovú premávku.

Upravený blockchain v rámci našej architektúry slúži na udržiavanie histórie komunikácie medzi serverom a IoT senzorovou sieťou. Jedná sa o to, že pomocou blockchain technológie sú všetky záznamy distribuované na všetkých zariadeniach a je veľmi nízka šanca ďalšej kompromitácie záznamov. Blockchain v rámci použitia sme museli upraviť. Upravenie blockchain technológie spočíva v nasledujúcich technikách:

- **dynamická veľkosť bloku** – blok má veľkosť n transakcií, kde n reprezentuje počet uzlov v sieti. Ak je v sieti 50 uzlov, tak jeden blok má veľkosť 50 transakcií. Pri overení bloku je potom nutné iba overiť jeden blok a následne šíriť v sieti iba jeden blok. Následkom je nižšie výpočtové zaťaženie z pohľadu overovania jedného bloku a následného šírenia bloku v sieti.
- **časová synchronizácia** – pridaním časovej synchronizácie sa zníži záťaž na sieť pri overovaní a validovaní transakcií a blokov. Uzly odosielať transakcie jednému uzlu, ktorý overuje transakcie, vkladá ich do bloku a následne overuje blok. Toto odosielanie transakcií je synchronizované pomocou rozvrhu vysielania. Tým zaistíme aby overovací uzol nebol zahltený x transakciami, ale prijme jednu transakciu za určitý čas. Tým znižujeme zahltenia uzla a počet výpadkov pri odosielaní transakcií za účelom overenia a vloženia do blockchain-u.
- **obsah a veľkosť transakcie** – transakcia v tomto prípade predstavuje záznam o komunikácii medzi serverom a sieťou. Tento záznam (veľkosť 20 bajtov) predstavuje históriu komunikácie. Pomocou tejto histórie vieme jednoznačne identifikovať útočníka v sieti.

Bezpečnostný proces (obr. č. 3) sa spúšťa vtedy, keď server vyhodnotí škodlivé údaje alebo porušenie bezpečnostných pravidiel a následne vykoná akciu. Za škodlivé údaje v tomto prípade pokladáme všetky údaje, ktoré nie sú v určenej forme. Napríklad očakávame prijatie teplotných údajov v JSON formáte. Hodnota teploty má byť v rozmedzí od 100 do – 100 stupňov Celzia. Ako náhle je hodnota iná, ako je definovaná, spustí sa bezpečnostný proces. Pri detekcii týchto škodlivých údajov sa spustí bezpečnostný proces, kedy proces spustí dožiadanie všetkých historických komunikačných záznamov uložených v blockchain-e. V momente prijatia údajov na serveri sa spustí prehľadávanie týchto záznamov za účelom identifikácie útočníka. V prípade, že útočník je nájdený tak sa vytvorí „blacklist záznam“, ktorý je odoslaný do siete kde sa aplikuje a ostatné uzly nebudú komunikovať so škodlivým uzlom. Ak nastane udalosť, že uzol ďalej odosiela škodlivé údaje, tak sa musí proces zopakovať. V prípade tretieho spustenia bezpečnostného procesu pre rovnakú udalosť sa spustí obnovenie siete. Toto obnovenie siete, je realizované pomocou bezpečnostných kľúčov, ktoré boli do zariadenia vložené pri inicializácii – to je kvôli tomu aby neboli prenášané a vymieňané bezdrôtovou komunikáciou a tak by mohli byť kompromitované. V prípade, že aj po obnovení siete je škodlivý uzol stále aktívnym členom siete, tak bezpečnostný proces identifikuje toto narušenie bezpečnosti a nariadi obnovenie siete s tým, že tentokrát už danému uzlu neodošle požiadavku na obnovenie siete.



Obr. č. 3 – Bezpečnostný proces

4.2 Dôkaz funkčnosti bezpečnostného procesu

Na dokázanie základnej funkčnosti bezpečnostného procesu sme použili konečný stavový automat. V rámci tohto dôkazu sme ukázali, že proces je konečný a má nejakú zložitosť. Funkčnosť ako takú sme overovali pomocou programového riešenia.

Automat **bezpečnostného procesu** (obr. č. 4) reprezentuje konečný stavový automat. Týmto automatom je reprezentovaný matematický dôkaz toho, že sa proces nedostane do mŕtveho bodu ale dostane sa do konečného stavu. Z pohľadu automatu vieme rozdeliť výsledný jazyk automatu ako slová z jazyka, ktoré nám hovoria o bezpečnosti údajov a slová z jazyka, ktoré nám hovoria o škodlivosti údajov. V rámci automatu, slová, ktoré patria do jazyka a vyhodnocujeme ich ako bezpečné sa končia v stave *u*. Slová, ktoré patria do jazyka a vyhodnocujeme ich ako škodlivé končia v stavoch *va* a *cz*. Slová, ktoré do jazyka nepatria reprezentujú neautorizovaný prístup do siete alebo na server a takéto slová (v ponímaní procesu údaje) sa ani nespracujú. Konečný automat (obr. č. 3) pre bezpečnostný proces definujeme nasledovne:

- Σ – vstupná abeceda: {a, d, z, c, e, s, v, o};

- K – konečná množina stavov: $\{p, u, k, b, va, kp, o1, o2, o3, cz\}$;
- p – počiatočný stav;
- $\delta - Q \times \Sigma \rightarrow Q$ je prechodová funkcia (tabuľka 2);
- F – množina akceptačných (konečných) stavov: $\{u, va, cz\}$.

Q	Σ	$\rightarrow Q$
-	prijmiData	p
p	dataOK	u
p	dataZle	k
p	zlaSprava	va
k	dataZle	b
k	chybajuData	va
B	dataZle	kp
B	chybajuData	va
kp	posliP	o1
o1	posliP	o2
o1	OK	cz
o2	posliP	o3
o2	OK	cz
o3	vytvorA	va
o3	OK	cz

Tabuľka č. 2 – Tabuľka prechodových stavov pre automat bezpečnostného procesu

Význam jednotlivých stavov:

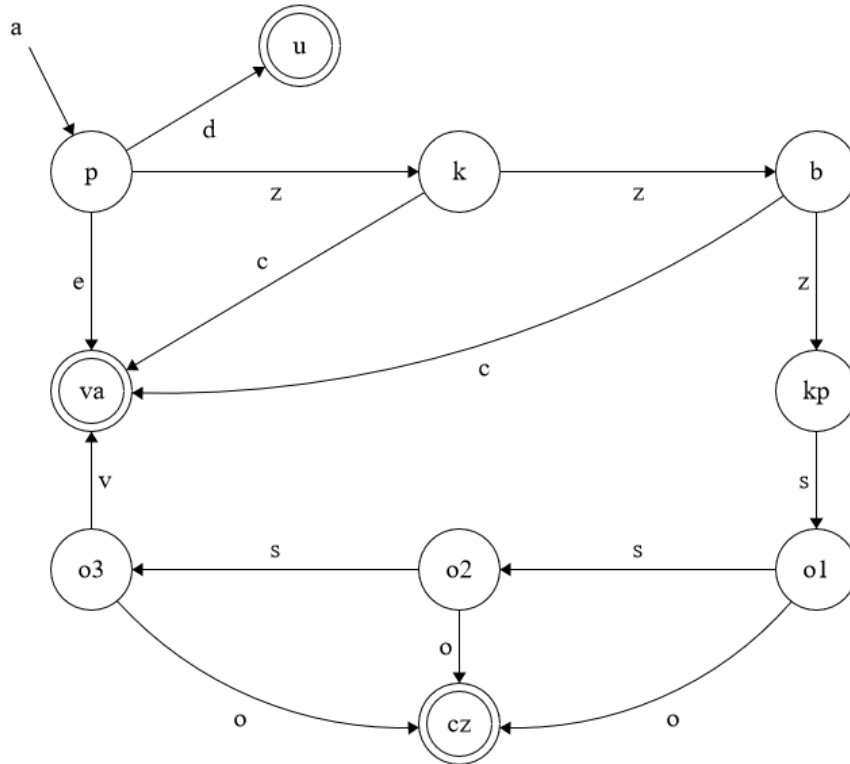
- p – príjem údajov;
- u – uloženie údajov;
- k – kontrola časovej pečiatky;
- b – spustenie bezpečnostného procesu;
- va – vykonaj akciu;
- kp – vytvor požiadavku;
- o1 – odosielanie požiadavky prvýkrát;
- o2 – odosielanie požiadavky druhýkrát;
- o3 – odosielanie požiadavky tretíkrát;
- cz – aplikovanie požiadavky do čierneho zoznamu.

Význam abecedy:

- a – prijatie údajov;
- d – údaje sú v poriadku;
- z – škodlivé údaje;
- c – chýbajúce údaje (bez časovej pečiatky, nenašla sa zhoda v záznamoch z blockchain-u);
- e – nesprávny formát správy zo siete;
- v – vytvor akciu;
- s – odošli požiadavku;
- o – požiadavka úspešne odoslaná.

Funkčnosť procesu sme dokazovali v rámci implementovaného prototypu.

Zložitosť tohto procesu je kvadratická. Stavy p a u predstavujú jednotkové operácie, ktoré sa v rámci procesu opakujú iba raz. Zložitý stav je stav b . Tento stav reprezentuje zozbieranie všetkých blockchain-ových záznamov z IoT siete a kontrolu údajov. Samotné zbieranie údajov predstavuje číslo n , pretože zbierame údaje od n uzlov. Kontrola údajov predstavuje násobok $x*n$, kde x predstavuje počet transakcií a blokov, ktoré musíme skontrolovať a n je počet blokov. Aplikácia požiadaviek cez stavy va , kp , $o1$, $o2$, $o3$ a cz predstavuje konštantu 7. Preto zložitosť tohto procesu je $2 + x*n + n + 7$ operácií v najhoršom prípade.



Obr. č. 4 – Bezpečnostný proces vyjadrený konečným stavovým automatom

4.3 Dôkaz bezpečnosti blockchain technológie

Čo sa týka použitia blockchain-u v rámci práce, tak sme vychádzali z článku [17], ktorý opisuje, prečo je blockchain technológia bezpečná. Tento článok hovorí o bezpečnosti blockchain-u to, že ak chce útočník meniť blockchain, tak zo štatistického hľadiska je to takmer nemožné. V rámci článku je na výpočet tejto pravdepodobnosti použitá Poissonová distribúcia (iný názov Poissonovo rozdelenie). Podľa definícií ([19][20]) Poissonová distribúcia (obr. č. 5) opisuje pravdepodobnosť javu, kedy nájdeme r udalostí za nejaký čas s tým, že udalosti sa dejú pravidelne opakujú v rozsahu u . Pre rôzne štatistické výpočty sú použité rôzne Poissonové rozdelenie. Pre výpočet pravdepodobnosti útoku na blockchain použili autori [17] Poissonovu kumulatívnu distribúciu (obr. č. 6), ktorou sa rekurzívne spočítajú pravdepodobnosti.

$$p(r; \mu) = \frac{\mu^r e^{-\mu}}{r!}$$

Obr. č. 5 – Poissonova distribúcia

$$P(r) = \sum_{k=0}^r \frac{\mu^k e^{-\mu}}{k!}$$

Obr. č. 6 – Poissonova kumulatívna distribúcia

Za názorný príklad použili proces náhodnej binomickej prechádzky (Binomial Random Walk), kedy sa snaží útočník dohnať poctivé uzly pri vkladaní bloku do blockchain-u. V rámci tohto príkladu je určené, že ak vloží do blockchain-u blok útočník, tak skóre sa zníži o 1, v prípade, že vloží blok poctivý účastník, tak sa skóre zvýši o 1. Toto skóre reprezentuje náskok v blokoch z . Na základe tohto príkladu vieme vypočítať pravdepodobnosť udalosti, kedy útočník dobehne poctivý blockchain.

$$g_z = \{ 1 \text{ ak } p \leq q \} \text{ a } q_z = \{ (q/p)^z \text{ ak } p > q \}$$

p – pravdepodobnosť, že nový blok vytvorí poctivý blockchain

q – pravdepodobnosť, že nový blok vytvorí útočník

q_z – pravdepodobnosť, že útočník dobehne poctivý blockchain s tým, že zaostáva o z blokov

Pri predpoklade, že $p > q$ vieme odvodiť nasledujúce vzťahy. Na základe vyššie spomenutého vzorca vieme pomocou Poissonovej distribúcie určiť útočníkov postup pri dobíhaní nasledujúcim vzťahom:

$$\lambda = z * (q / p)$$

Teraz zoberieme tento vzťah útočníkovho postupu a vynásobíme to Poissonovou hustotou, aby sme dostali finálnu pravdepodobnosť na to, či útočník dobehne poctivý blockchain. Prvý vzťah (obr. č. 7) je pre nekonečno blokov, druhý vzťah (obr. č. 8) je pre konečný počet náskoku vyjadrený ako počet blokov z .

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

Obr. č. 7 – Výpočet pravdepodobnosti, že útočník dobehne blockchain pre nekonečný náskok

$$1 - \sum_{k=0}^z \frac{\lambda^k e^{-\lambda}}{k!} (1 - (q/p)^{(z-k)})$$

Obr. č. 8 – Výpočet pravdepodobnosti, že útočník dobehne blockchain pre konečný náskok²

Výsledky v uvedenom článku hovoria, že čím je vyššia pravdepodobnosť q , tak tým potrebujú poctivé uzly väčší náskok pri blokoch z , aby sme vedeli blockchain, chrániť pred útočníkom. Pravdepodobnosť q silne závisí na tom, koľko uzlov v blockchain-ovej sieti vlastní útočník.

² obrázky 5 a 6 sú z článku **Chyba! Nenašiel sa žiaden zdroj odkazov.** a obrázky 7 a 8 sú z článku **Chyba! Nenašiel sa žiaden zdroj odkazov.**

5 Experimentálne výsledky

Na overenie funkčnosti navrhovanej bezpečnostnej architektúry sme vytvorili viacero prototypov pomocou, ktorých sme overovali vlastnosti tejto architektúry a funkčnosť navrhovaných úprav a nových procesov. Následne sme použili prototypy aj v rámci experimentov na vyhodnotenie dôležitých parametrov – zahltenie siete, časová záťaž zariadení, šifrovacia záťaž zariadení.

5.1 Opis prototypov

V rámci práce boli implementované nasledujúce štyri prototypy implementácie:

- prototypy na overenie blockchain-ových vlastností – týmito prototypmi sme overovali použitie blockchain technológie najmä v súvislosti s tým, koľko sieťovej a výpočtovej záťaže vytvárajú pri použití blockchain technológie v IoT sieti. V rámci blockchain technológie sme použili aj viac konsenzuálnych algoritmov (Proof of Work, Proof of Stake, practical Byzantine Fault Tolerance) aby sme zistili, ktorý z nich je najvhodnejší na použitie v IoT,
- prototypy na testovanie šifier – v rámci týchto prototypov sme overovali čas potrebný na šifrovanie a dešifrovanie a porovnávali rozdiely v šifrovaní a dešifrovaní medzi symetrickými a asymetrickými šiframi,
- prototypy na distribuované vytvorenie šifrovacích kľúčov – v rámci týchto prototypov sme sledovali, ako zaťažuje distribuované generovanie kľúčov zariadenia v IoT sieti,
- prototypy na testovanie bezpečnostného modulu – v rámci týchto prototypov sme sledovali časovú odozvu bezpečnostného procesu, ako rýchlo dokáže identifikovať útočníka v sieti.

Z pohľadu testovania prototypov sme otestovali prototypy štandardne pomocou jednotkových, integračných, regresných a aplikačných testov.

5.2 Experimentálne merania

Vykonané experimentálne merania boli realizované pomocou prototypov. Na základe týchto meraní sme interpretovali zistené výsledky, kde sme z týchto výsledkov určili aké vlastnosti má navrhovaná bezpečnostná architektúra z pohľadu zachytávania útokov, sieťového zahltenia a šifrovacia réžia.

5.2.1 Sieťové zahltenie

V rámci týchto experimentálnych meraní, sme pozorovali, aké sieťové zahltenie produkuje blockchain technológia, ktorú sme využili na odhaľovanie útočníkov. V rámci testovania sme použili tieto konsenzuálne algoritmy:

- Proof of Work (PoW),
- Proof of Stake (PoS),
- practical Byzantine Fault Tolerance (pBFT).

V rámci týchto algoritmov sme sledovali ako rýchlo dokážeme prijať konsenzus a overiť blok a druhú vlastnosť sme sledovali, koľko sieťového zahltenia generujú jednotlivé konsenzuálne

algoritmy, pri dosiahnutí konsenzu. Jednotlivé konsenzuálne algoritmy vytvárajú sieťové zahltenie v nasledujúcej miere:

- PoW generuje 3 až 6 správ: požiadavka, odpoveď, distribúcia bloku + potvrdzovanie správ (*min.*: $3*n$; *max.*: $6*n$);
- PoS generuje 4 až 8 správ: požiadavka, stávka, vrátenie stávky, distribúcia bloku + potvrdzovanie správ (*min.*: $4*n$; *max.*: $8*n$);
- pBFT generuje $n*(n-1)$: každé zariadenie dostane blok, aby ten blok overil a po overení odošle blok všetkým ostatným zariadeniam na kontrolu.

Meranie z pohľadu časovej odozvy je reprezentované v tabuľke 3. Oproti klasickým algoritmom pri tomto meraní boli realizované menšie zmeny. Aby sme vedeli odmerať potenciál PoW algoritmu, tak sme použili iba 20 bitové hash-e (štandardne 256-bitové). V rámci testovania sa vyskytol menší problém s testovaním pBFT algoritmu, kde sme nemali potrebný počet zariadení na otestovanie a tým nebola splnená nutná matematická podmienka $3k + 1$. Výsledky prezentované v tabuľke 3 prezentujú naplnenie bloku, kedy sme pri tomto testovaní naplňovali blok piatimi transakciami – 3 uzly naplnia blok rýchlejšie ako dva preto je tam časový rozdiel. Na základe toho sa určil čas potrebný na dosiahnutie konsenzu.

Konsenzuálny algoritmus	počet uzlov 2	počet uzlov 3	Predpokladaná réžia blockchain-u
POS	3.636 s	2.757 s	650 – 750 ms
POW	4.029 s	3.001 s	1000 ms
PBFT	3.495 s	2.673 s	500 – 670 ms

Tabuľka č. 3 – Porovnanie konsenzuálnych algoritmov a rýchlosť vytvorenia bloku

Pri výpočte a následného zahltenia siete, časového zaťaženia siete a výpočtového zaťaženia uzla treba vziať do úvahy aj charakteristiku jednotlivých použitých algoritmov. Pri sieťovom zahltení PoS a PoW algoritmus generujú lineárne zaťaženie siete, zatiaľ čo pBFT generuje kvadratické zaťaženie siete. Z výpočtového pohľadu PoS a pBFT negenerujú extrémne výpočtové zaťaženie, nakoľko PoS iba vyhodnotí stávky a pBFT skontroluje ostatné prijaté správy a na základe nich overí blok. Pri PoW je nutné vypočítať hash. Zložitosť výpočtu hash-u stále rastie, tak výpočtové zaťaženie sa zvyšuje. Z pohľadu časového zaťaženia je PoS najjednoduchší, lebo sa iba odošlú stávky a tie sa vyhodnotia. PoW je časovo náročný nakoľko výpočet hash-u prebieha dlho. pBFT musí v rámci dosiahnutia konsenzu čakať na x správ od n uzlov. Z veľkosťou siete preto narastá časové zaťaženie siete. Z predchádzajúcich meraní preto vieme určiť vzťahy pre výpočet časovej záťaže, zahltenia siete a pamäťovej záťaže.

Vzťah pre výpočet časovej záťaže siete s využitím blockchain-u

Nech v IoT senzorovej sieti využívame blockchain na zabezpečenie siete. Potom vzťah pre zahltenie siete spočítame ako:

$$t = (n * s) * t_r + b$$

kde,

n – počet uzlov;

s – počet správ v sieti -> PoW <3,4>, PoS <4,7>, pBFT = $n*(n-1)$;

t_t – časové rozostupy vo vysielaní a priemerná odozva komunikácie;

b – réžia blockchain-u.

Tento vzorec nám reprezentuje vysielaciu časovú záťaž na celú sieť. Ak chceme vypočítať vysielaciu záťaž pre jeden uzol, tak treba vziať do úvahy aj to, že v rámci vkladania informácií do blockchain-u, musí každý uzol aspoň raz za čas t byť ten, čo vytvára blok – v ideálnom prípade sa za čas t pri vytváraní bloku a vkladaní do blockchain-u vystrieda presne n uzlov. Preto časové zaťaženie uzla spočítame takto:

$$t_n = s * t_r + t/n$$

kde,

t – celkový čas na vloženie informácií do blockchain-u,

s, t_r, n – vysvetlené v predchádzajúcom vzorci.

Vzťah pre výpočet zahltenia siete

Vzťah zahltenia siete v závislosti od premávky v sieti vieme spočítať nasledovne:

$$z = b_r * p_{vs} * p_n$$

kde,

z – počet správ v sieti,

b_r – blockchain-ová réžia,

p_{vs} – počet vysielaní za sekundu,

p_n – počet uzlov v sieti,

Tento vzorec nám hovorí o tom, že čím častejšie odosielame senzorové údaje na server, tým viac máme zahltenú sieť.

Vzťah pre výpočet pamäťového zahltenie uzla

Z pohľadu pamäťového zahltenia uzla našou upravenou blockchain technológiu zahlcujeme zariadenie rozumne preto, lebo transakcie majú veľkosť 20 bajtov a veľkosť blokov je dynamicky určená v závislosti od počtu uzlov. Na základe týchto údajov vypočítame pamäťové zaťaženie nasledovne:

$$p_z = (v_t * x + p_{br}) * p_b$$

kde,

p_z – výsledné pamäťové zahltenie,

v_t – veľkosť transakcie (v našom prípade 20 bajtov),

x – počet transakcií v bloku (priamo závisí od počtu uzlov v sieti),

p_b – počet blokov uložených za deň,

p_{br} – pamäťová réžia blockchain technológie.

5.2.2 Odozva bezpečnostného modulu

Tieto merania sa sústreďujú na odozvu bezpečnostného modulu pri odhaľovaní škodlivých uzlov v sieti. Pre tieto merania sme použili 2 PC, kde na jednom PC reprezentoval sieť s x uzlami a druhé PC reprezentovalo server. Odozvu pri odosielaní sme nastavili na 150 ms – je to odozva ktorú sme reálne namerali medzi sieťou a serverom, za použitia IoT senzorových zariadení a realizáciou prenosu cez Internet. V rámci testu sme odosielať údaje, ktoré sme označili ako škodlivé. Ako náhle sa na PC zariadení reprezentujúcom server prijali tieto škodlivé údaje, tak sa spustil bezpečnostný proces. Jednotlivé merania sú zaznamenané v tabuľke 4. Z týchto údajov je jasne vidieť, že najväčší dopad na časovú odozvu má *Prijímanie záznamov zo siete*. Toto odosielenie bolo synchronizované podľa časového rozvrhu kde sme nastavili rozostup odosielení na 150 mili sekúnd. Je to kvôli tomu, aby sme zbytočne nevyčerpávali sieť a zároveň aby sme nezaťažovali server. Druhý dôležitý riadok je *Spracovanie Blockchain histórie*. Vidíme, že s rastúcim počtom uzlov v sieti rastie aj čas potrebný na spracovanie blockchain-ových údajov.

	Priemerný čas	Priemerný čas	Priemerný čas	Priemerný čas	Priemerný čas
Veľkosť siete	10 uzlov	20 uzlov	30 uzlov	40 uzlov	50 uzlov
Spracovanie škodlivých údajov	1.07 ms	1.10 ms	1.10 ms	1.14 ms	1.14 ms
Odoslanie Blockchain požiadavky	153.13 ms	155.23 ms	153.56 ms	153.78 ms	154.83 ms
Spracovanie Blockchain požiadavky	16.84 ms	33.22 ms	49.26 ms	67.58 ms	123.92 ms
Prijímanie záznamov zo siete	2.95 s	6.05 s	9.15 s	12.25 s	23.11 s
Spracovanie Blockchain histórie	186.86 mikro s	758.80 mikro s	1.44 ms	3.22 ms	7.97 ms
Vytvorenie blacklist požiadavky	1.28 ms	1.52 ms	1.55 ms	1.62 ms	1.68 ms
Odoslanie blacklist požiadavky	152.48 ms	149.80 ms	148.57 ms	149.45 ms	146.35 ms
Spracovanie blacklist požiadavky	1.07 ms	1.09 ms	1.09 ms	1.12 ms	1.12 ms
Blacklist požiadavka úspešne aplikovaná	152.66 ms	154.95 ms	154.19 ms	153.55 ms	152.43 ms
Celkový čas	3.57 s	6.67 s	9.77 s	12.87 s	23.73 s

Tabuľka č. 4 – Testovanie bezpečnostného modulu s oneskorením 153 ms

V rámci odozvy bezpečnostného modulu sme ešte merali aj počet správ (tabuľka 5), ktoré sú odoslané na server pri dožiadaní jedného bloku. V rámci bloku sme použili 60 bajtové transakcie namiesto pôvodne navrhovaných 20, a bloky sa skladali z n transakcií (n je počet uzlov). Transakcie sme zväčšili preto, lebo pri 50 správach by mal jeden blok 1000 bajtov a to by sa pri použití Wi-Fi technológií stále zmestilo do jednej správy. Z toho vyplynula nutnosť odosielať bloky viacerými správami (fragmentácia bloku a znovu vyskladanie na serveri). Týmto meraním sme zisťovali, aké veľké je sieťového zaťaženie a ako rýchlo rastie. Z merania vyplynulo, že počet paketov závisí od veľkosti blokov.

Veľkosť siete	Počet paketov
10 uzlová sieť	10
20 uzlová sieť	20
30 uzlová sieť	60
40 uzlová sieť	80
50 uzlová sieť	150

Tabuľka č. 5 – Sieťové zaťaženie pri odosielaní blockchain-ových záznamov

5.2.3 Dopady šifrovania na IoT zariadenia

V rámci týchto meraní sme riešili aký dopad má šifrovanie z pohľadu výpočtového zaťaženia, ktoré sme určili ako čas trvania výpočtu. Porovnávali sme dopad šifrovania a dešifrovania pomocou symetrických a asymetrických šifier. Pri porovnaní rôznych symetrických šifírov sme šifrovali údaje v rozmedzí 1 až 5000 bajtov na zariadeniach RaspberryPi. Následne sme merali čas potrebný na šifrovanie a dešifrovanie údajov uvedené v tabuľke 6. Na základe týchto meraní je vidno, že rozdiel medzi šifrovaním a dešifrovaním nie je veľký. Naproti tomu, ak sa pozrieme na tabuľku 8, tak je vidno, že pri použití asymetrickej šifry RSA je rozdiel medzi šifrovaním a dešifrovaním značný s narastajúcou dĺžkou šifrovacieho kľúča (samozrejme kľúče o veľkosti 8 až 64 bitov pre RSA sú nepostačujúce, merali sme ako dlho trvá šifrovanie na RaspberryPi zariadeniach). V rámci tabuľky 7 je ešte urobené ďalšie porovnanie z pohľadu veľkosti kľúča, kde je vidno, že pri použití symetrickej šifry AES s lineárne rastúcou dĺžkou kľúča nám lineárne rastie a čas potrebný na šifrovanie správy. Rovnaký trend je možné vidieť aj v tabuľke 8, ale tam je ukázané, že čas potrebný na dešifrovanie rastie exponenciálne. Preto z uvedených meraní v tabuľkách 6,7 s 8 môžeme konštatovať, že na šifrovanie a dešifrovanie komunikácie na IoT zariadeniach je z toho pohľadu vhodnejšie použitie symetrických šifírov.

Šifrovací algoritmus	Priemerný čas zašifrovania (mikro s)	Priemerný čas dešifrovania (ms)
AES	107,52	106,11
3DES	468,85	445,1
HIGHT	362,97	350,13
SEED	172,78	157,71
LEA	238,56	78,32
RC6	95,84	77,47
CHAM128	124,75	100,88
SIMECK64	152,52	131,31
SIMON128	197,03	101,79
SPECK128	88,93	52,03
TEA	148,98	122,74
XTEA	175,4	153,76

Tabuľka 6 – Časové porovnanie šifrovania a dešifrovania pomocou symetrických šifírov

Číslo merania	Priemer v ms
AES ECB 96	8,56
AES CBC 96	10,37
AES ECB 128	11,10
AES CBC 128	13,27
AES ECB 192	13,28
AES CBC 192	16,55

Tabuľka 7 – Časové porovnanie šifrovania s rôzne veľkými kľúčmi

Dĺžka kľúča v bitoch	Šifrovanie	Dešifrovanie
RSA 8	836 mikro s	309 mikro s
RSA 16	6,94 ms	88,64 mikro s
RSA 32	1,14 ms	9,7 s
RSA 64	9,21 ms	65,35 s

Tabuľka 8 – Časové porovnanie šifrovania a dešifrovania pomocou asymetrických šifier z rôznymi veľkosťami kľúčov

5.3 Porovnanie

Existujúce riešenia na zvýšenie bezpečnosti v IoT senzorovej sieti sme rozdelili na Smart Home riešenia a IDS riešenie. Smart Home riešenia na zabezpečenie komunikácie v sieti využívajú blockchain technológiu. Zabezpečenie komunikácie pri Smart Home riešeniach je realizované tak, že každá komunikácia medzi dvoma zariadeniami sa overuje pomocou ťažiaceho stroja. V prípade, že tento stroj zlyhá, tak komunikácia už nie je overovaná a tým pádom aj nezabezpečená. V našom riešení, ak zlyhá jeden uzol, sieť funguje ďalej. Výhodou nášho riešenia je, že sme odstránili potencionálny bod zlyhania. Výhodou Smart Home riešení je, že IoT zariadenia sú menej zaťažené výpočtami. Pri IDS riešeniach použili blockchain technológiu na zabezpečenie a verifikáciu IDS pravidiel a zdieľanie informácií. Vďaka tomu vedie IDS riešenia lepšie detegovať útoky zvonku na sieť. Naše riešenie je lepšie navrhnuté na zachytávanie útokov z vnútra siete. Výsledné merania sme porovnali ešte voči riešeniu [18] kde môžeme konštatovať, že naše riešenie je pomalšie v niektorých časových meraniach. Faktom pomalosti je najmä rozdiel vo výkone v použitých zariadeniach. Ak však výsledky porovnáme z pohľadu zložitosti, tak naše riešenie a riešenie [18] majú pri konkrétnych časových porovnaníach lineárnu zložitosť. V porovnaní voči ostatným analyzovaným riešeniam sme naše výsledne riešenie vytvorili tak, aby bola zaťaž na jednotlivé komponenty architektúry rozložená viac rovnomerne.

6 Zhodnotenie

Dizertačná práca sa zameriava na problém poskytovania kvality služieb v prostredí Internetu vecí, konkrétne v senzorových sieťach so zariadeniami s nízkym výkonom. Analýza prostredia Internetu vecí nám ukázala, že poskytovanie služieb v IoT prostredí je problémové z viacerých hľadísk – nízke zabezpečenie zariadení, heterogénne technologické prostredie (rôzne zariadenia, komunikačné technológie, a i.), nízko výkonové zariadenia napájané externým elektrickým zdrojom, mobilita zariadení, rušenie bezdrôtového spojenia. Hlavný prínos predloženej dizertačnej práce spočíva v návrhu bezpečnostnej architektúry, založenej na technológií blockchain. Navrhovaná bezpečnostná architektúra je založená na využití blockchain technológie pri procese odhaľovania útoku, kde blockchain technológia vystupuje ako databáza histórie prenosu údajov medzi serverom a IoT senzorovou sieťou. Aby bolo možné technológiu blockchain využívať na zachycovanie útokov, bol vytvorený bezpečnostný proces, ktorý využíva čítanie histórie prenosu údajov z blockchain záznamov, následne zabraňuje konkrétnym útokom a tým vytvorí priestor na zotavenie siete a služieb, ktoré poskytuje. Navrhnutá architektúra využíva existujúce bezpečnostné prístupy na šifrovanie komunikácie, vytvorenie bezpečného prístupu do IoT siete a bezpečné obnovenie zariadenia. Nakoniec boli použité metódy na zníženie zahltenia v sieti, kde sme použili rozvrh vysielania ako synchronizačný prvok pre komunikáciu siete so serverom a pre komunikáciu uzlov v blockchain-ovej sieti. Hlavnými prínosmi predloženej dizertačnej práce sú:

- bezpečnostná architektúra – je teoretický prínos, kde táto architektúra predstavuje umiestnenie bezpečnostných prvkov a procesov tak, aby sa výpočtová a komunikačná záťaž rovnomerne rozložila medzi server a sieť. Výsledným efektom je predĺženie životnosti siete, zlepšenie priepustnosti servera a IoT siete, zvýšenie bezpečnosti a zlepšenie poskytovania QoS služieb.
- bezpečnostný proces – je teoretický prínos, pomocou ktorého vieme rýchlo reagovať a zneškodniť útok, ktorý prichádza zvnútra siete.
- upravená blockchain technológia – je praktický prínos, pomocou ktorého vieme znížiť zaťaženie blockchain-ovej siete a zariadení používajúcich blockchain a urýchliť schvaľovanie transakcií a blokov v blockchain technológií.
- história prenosu údajov – je praktický prínos, ktorý využíva upravenú blockchain technológiu. Pomocou uchovania histórie prenosu údajov medzi serverom a sieťou vieme efektívne a jednoznačne odhaliť útočníka vnútri siete. Tento prínos spolu s upravenou blockchain technológiou môžeme použiť ako rozširujúci prvok pre IDS, IPS a SIEM systémy.

Vďaka týmto prínosom je IoT sieť lepšie zabezpečená voči útokom z vnútra siete. Jednotlivé prínosy takisto pomáhajú sieti k rýchlemu zotaveniu sa po útoku a sú optimalizované tak, aby výpočtová záťaž zariadení a sieťová záťaž z pohľadu odosielaných správ bola čo najmenšia.

Porovnanie voči existujúcim riešeniam

Existujúce riešenia na zvýšenie bezpečnosti v IoT senzorovej sieti sme rozdelili na Smart Home riešenia a IDS riešenie. Smart Home riešenia na zabezpečenie komunikácie v sieti využívajú blockchain technológiu. Zabezpečenie komunikácie pri Smart Home riešeniach je realizované tak, že každá komunikácia medzi dvoma zariadeniami sa overuje pomocou ťažiaceho stroja. V prípade, že tento stroj zlyhá, tak komunikácia už nie je overovaná a tým

pádom je nezabezpečená. V našom riešení, ak zlyhá jeden uzol, sieť funguje ďalej. Výhodou nášho riešenia je, že sme odstránili potencionálny bod zlyhania. Výhodou Smart Home riešení je, že IoT zariadenia sú menej zaťažené výpočtami. Pri IDS riešeniach použili blockchain technológiu na zabezpečenie a verifikáciu IDS pravidiel a zdieľanie informácií. Vďaka tomu vedia IDS riešenia lepšie detegovať útoky zvonku na sieť. Naše riešenie je lepšie navrhnuté na zachytávanie útokov z vnútra siete. Výsledné merania sme porovnali ešte voči riešeniu [18] kde môžeme konštatovať, že naše riešenie je pomalšie v niektorých časových meraniach. Faktom pomalosti je najmä rozdiel vo výkone v použitých zariadeniach. Ak však výsledky porovnáme z pohľadu zložitosti, tak naše riešenie a riešenie [18] majú pri konkrétnych časových porovnaníach lineárnu zložitosť. V porovnaní s ostatnými riešeniami z podkapitoly 2.4 sme naše výsledne riešenie vytvorili tak, aby bola záťaž na jednotlivé komponenty architektúry rozložená viac rovnomerne.

7 Použitá literatura

- [1] Mashal, I., Alsaryrah, O., Chung, Yang, T. Y., C. Z., Kuo, W. H., Agrawal, D. P.: Choices for interaction with things on Internet and underlying issues. *Ad Hoc Networks*, (2015), vol. 28, pp. 68–90.
- [2] Said, O., Masud, M.: Towards internet of things: survey and future vision. *International Journal of Computer Networks*, (2013), vol. 5, no. 1, pp. 1–17.
- [3] Sethi, P., Sarangi, S. R.: Internet of Things Architectures, Protocols, and Applications. *Journal of Electrical Computer Engineering*, (2017), vol. 2017, pp. 1-25.
- [4] Atzori, L., Iera, A., Morabito, G.: The Internet of Things A survey. *Computer Networks*, (2010), vol. 54, no. 15, pp. 2787-2805.
- [5] Porkodi, R., Bhuvaneswari, V.: The Internet of Things (IoT) Applications and Communication Enabling Technology Standards An Overview. In: 2014 International Conference on Intelligent Computing Applications, IEEE, (2014), pp. 324-329.
- [6] Rabaiei, K. A. A., Harous, S.: Internet of Things: Applications and Challenges. In: 2016 12th International Conference on Innovations in Information Technology (IIT), IEEE, (2016), pp. 212-217.
- [7] Elkarash, H., H., Elshennawy, N., M., Sallam, E., A.: Evaluating QoS using scheduling algorithms in MPLS/VPN/WiMAX networks. In: 2017 13th International Computer Engineering Conference (ICENCO), IEEE, (2017), pp. 14-19.
- [8] M. Daud, R. Rasiah, M. George, D. Asirvatham, A. F. A. Rahman and A. A. Halim, "Denial of service: (DoS) Impact on sensors," 2018 4th International Conference on Information Management (ICIM), Oxford, UK, 2018, pp. 270-274.
- [9] J. Chen, C. Hu, H. Zeng and J. Zhang, "Impact of Security on QoS in Communication Network," 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing, 2009, pp. 40-43.
- [10] Kizza J.M. (2009) Firewalls. In: Kizza J.M. (eds) A Guide to Computer Network Security. The Computer Communications and Networks. Springer, London.
- [11] A. Mairh, D. Barik, K. Verma, and D. Jena, "Honeypot in network security: a survey," in Proceedings of the 2011 international conference on communication, computing & security. ACM, 2011, pp. 600–605.
- [12] J. Inns, "The evolution and application of SIEM systems," *Network Security*, vol. 2014, no. 5, pp. 16–17, 2014.
- [13] LIAO, Hung-Jen, et al. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 2013, 36.1: 16-24.
- [14] Dabbagh M., Kakavand M., Tahir M. (2020) Towards Integration of Blockchain and IoT: A Bibliometric Analysis of State-of-the-Art. In: Prieto J., Das A., Ferretti S., Pinto A., Corchado J. (eds) Blockchain and Applications. BLOCKCHAIN 2019.
- [15] E. S. Kang, S. J. Pee, J. G. Song and J. W. Jang, "A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid," 2018 3rd International Conference on Computer and Communication Systems (ICCCS), Nagoya, Japan, 2018, pp. 472-476.
- [16] A. M. Krishna and A. K. Tyagi, "Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1-8.

- [17] Nakamoto, S.: Bitcoin A peer-to-peer electronic cash system. [Online; accessed April 17, 2021]. Available at: <https://bitcoin.org/bitcoin.pdf>.
- [18] F. Zhang, W. Li, T. Li, Y. Wang and Z. Li, "RuleChain: A Novel Intrusion Rules Distribution Method Based on Blockchain," 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2019, pp. 60-66.
- [19] Winkelman, R.: Econometric Analysis of Count Data. Springer-Verlag 5th edition, (2008), ISBN 978-3-540-77648-2.
- [20] Walck, Ch.: Hand-book on statistical distributions for experimentalists. University of Stockholm, (1996), [Online: accessed May 14, 2021]. Available at: <http://www.stat.rice.edu/~dobelman/textfiles/DistributionsHandbook.pdf>.
- [21] Basagni, S., Conti, M., Giordano, S., Stojemenovic, I.: Mobile Ad Hoc Networking. New Jersey: IEEE Press, (2004), ISBN 0-471-37313-3.

8 Publikačná činnosť

ADC Vedecké práce v zahraničných karentovaných časopisoch

- ADC01 ERDELYI, Jaroslav - MACKO, Dominik - JELEMENSKÁ, Katarína. PESL: System-Level Estimation of Power-Management Effect on Dynamic Energy Consumption. In *Electronics*. Vol. 9, iss. 8 (2020), pp. 1-13. ISSN 2079-9292 (2019: 2.412 - IF, Q2 - JCR Best Q, 0.303 - SJR, Q2 - SJR Best Q). V databáze: SCOPUS: 2-s2.0-85090259036 ; WOS: 000564636100001 ; DOI: 10.3390/electronics9081313.

AFD Publikované príspevky na domácich vedeckých konferenciách

- AFD01 ERDELYI, Jaroslav - ČIČÁK, Pavel. Survey on communication in internet of things environment. In *ICETA 2018 : 16th IEEE International Conference on Emerging eLearning Technologies and Applications. November 15-16, 2018, Starý Smokovec, Slovakia : Proceedings*. 1. vyd. Danvers : IEEE, 2018, S. 149-156. ISBN 978-1-5386-7912-8. V databáze: WOS: 000457680400022 ; SCOPUS: 2-s2.0-85060311125.
- AFD02 LENICKÝ, Ján - HRADSKÝ, Martin - KALINA, Martin - ERDELYI, Jaroslav - ČIČÁK, Pavel. E-Health device for remote health monitoring. In *ICETA 2020 : proceedings, 18th IEEE International conference on emerging elearning technologies and applications, November 12-13, 2020, virtual conference Košice, Slovakia*. 1. vyd. Danvers : IEEE, 2020, S. 382-387. ISBN 978-0-7381-2366-0. V databáze: SCOPUS: 2-s2.0-85103738645 ; DOI: 10.1109/ICETA51985.2020.9379268.
- AFD03 ŠIRKA, Stanislav - ERDELYI, Jaroslav - ČIČÁK, Pavel - JELEMENSKÁ, Katarína. Survey on security threats and algorithms in Internet of Things environment. In *ICETA 2019 : 17th IEEE International conference on emerging elearning technologies and applications : Information and communication technologies in learning. Starý Smokovec, Slovakia. November 21-22, 2019*. Danvers : IEEE, 2019, S. 721-726. ISBN 978-1-7281-4967-7. V databáze: SCOPUS: 2-s2.0-85082994216 ; IEEE: 9039994.

AGJ Autorské osvedčenia, patenty, objavy

- AGJ01 ERDELYI, Jaroslav - ČIČÁK, Pavel - MACKO, Dominik - JELEMENSKÁ, Katarína. Zariadenie na zaznamenávanie a zber údajov zo senzorov prostredníctvom siete internetu vecí. Banská Bystrica Úrad priemyselného vlastníctva SR 2020. 5 s. Dostupné na internete: <<https://wbr.indprop.gov.sk/WebRegistre/UzitkovyVzor/Detail/197-2019>>.