Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Zabezpečení mesh IoT sítí

Marko Aćamović

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Marko Aćamović

Informatika

Název práce

Zabezpečení mesh IoT sítí

Název anglicky

Security of mesh networks for IoT

Cíle práce

Bakalářská práce je tématicky zaměřená na problematiku zabezpečení mesh sítí. Hlavním cílem je zhodnotit stávající zabezpečení mesh sítí a porovnat aktuální technologie.

Dílčí cíle práce jsou:
- charakterizovat IoT sítě a jejich zabezpečení,
- zhodnotit stávající bezpečnostní protokoly a mechanismy pro mesh sítě,
- identifikovat hlavní hrozby a slabiny mesh sítí,
- porovnat zabezpečení sítě Zigbee s jinou technologií.

Metodika

Teoretická část bakalářské práce bude založena na analýze a rešerši aktuálních odborných zdrojů.

V praktické části bakalářské práce budou na základě poznatků zjištěných v teoretické části zhodnoceny vybrané technologie mesh IoT sítí se zaměřením na problematiku bezpečnosti. Následně budou definovány nedostatky a jejich možná náprava.

Na základě syntézy teoretických a praktických poznatků budou zpracovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

IoT, Zigbee sítě, IEEE 802.15. 4, zabezpečení sítí, bezpečnostní protokoly, mesh IoT sítě

Doporučené zdroje informací

ANDRADE, Roberto Omar, Luis TELLO-OQUENDO a Iván ORTIZ, 2021. Cybersecurity Risk of IoT on Smart Cities. 1. vyd. Cham: Springer International Publishing, 95 s. ISBN 978-30-308-8523-6.

DAVOLI, Luca a Gianluigi FERRARI. 2022. Wireless Mesh Networks for IoT and Smart Cities: Technologies and Applications. 1. vyd. Stevenage: Institution of Engineering & Technology, 289 s. ISBN 978-18-395-3282-5.

CHAKI, Rituparna a Debdutta Barman ROY, 2021. Security in IoT: The Changing Perspective. 1. vyd. Boca Raton: Taylor & Francis Group, 136 s. ISBN 978-03-677-1141-2.

LELE, Chitra, 2022. Internet of Things (IoT) A Quick Start Guide: A to Z of IoT Essentials. 1. vyd. Indie: BPB Publications, 146 s. ISBN 978-93-898-4586-0.

NAYAK, Padmalaya, Souvik PAL a Sheng-Lung PENG, 2021. IoT and Analytics for Sensor Networks: Proceedings of ICWSNUCA 2021. 1. vyd. Singapur: Springer Singapore Pte. Limited, 244 s. ISBN 978-98-116-2918-1.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Michal Stočes, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 7. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 12. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zabezpečení mesh IoT sítí" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14. března 2024 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Michalu Stočesovi, Ph.D. za jeho odborné vedení a cenné rady, které byly pro mě klíčové při psaní této bakalářské práce.

Zabezpečení mesh IoT sítí

Abstrakt

Bakalářská práce se zaměřuje na zabezpečení mesh IoT sítí, klíčovou oblast v rostoucím odvětví IoT.

V teoretické části je charakterizována problematika IoT sítí, stávajících bezpečnostních protokolů a mechanismů specifických pro mesh sítě, a identifikaci hlavních hrozeb a slabých míst těchto sítí.

V praktické části jsou na základě teoretických poznatků hodnoceny vybrané technologie mesh IoT sítí, přičemž je kladen důraz na bezpečnostní aspekty. Na základě této analýzy jsou definovány nedostatky a navrženy možnosti jejich nápravy. Závěr práce představuje syntézu teoretických a praktických poznatků.

Klíčová slova: IoT, mesh sítě, zabezpečení, analýza, Zigbee, IQRF, Bluetooth Mesh

Security of mesh networks for IoT

Abstract

The bachelor's thesis is focused on the security of mesh IoT networks, a key area in the growing IoT industry.

In the theoretical part are characterized the issues of IoT networks, existing security protocols, and mechanisms specific to mesh networks along with the identification of main threats and weaknesses of these networks.

In the practical part, selected technologies of mesh IoT networks are evaluated based on theoretical knowledge, with an emphasis on security aspects. Based on this analysis, deficiencies are defined, and possibilities for their remediation are proposed. The conclusion of the thesis presents a synthesis of theoretical and practical knowledge.

Keywords: IoT, mesh networks, analysis, Zigbee, IQRF, Bluetooth Mesh

Obsah

1 Úvod **9**

2 Cíl práce a metodika **10**

3 Teoretická východiska **11**

3.1 Mesh sítě v IoT prostředí 11

3.1.1 Definice mesh sítí 11

3.1.2 Topologie sítě 12

3.1.3 Charakteristika mesh sítí v IoT 12

3.1.4 Charakteristika a architektura mesh IoT sítí 14

3.2 Zabezpečení v mesh IoT sítích 24

3.2.1 Bezpečnostní mechanismy 24

3.2.2 Bezpečnostní protokoly 26

3.3 Hrozby a slabiny mesh IoT sítí 27

3.3.1 Hrozby pro mesh IoT sítě 27

3.3.2 Slabiny v zabezpečení mesh IoT sítí 28

3.3.3 Důsledky nedostatečného zabezpečení v mesh sítích 29

4 Vlastní práce **31**

4.1 Výběr konkrétních technologií mesh IoT sítí pro analýzu 32

4.2 Definice kritérií 34

4.3 Stanovení cíle 35

4.4 Vytvoření hierarchie pro porovnání bezpečnosti mesh IoT sítí 36

4.5 Stanovení vah kritérií 36

4.6 Normalizace a výpočet vlastních vektorů 38

4.7 Kontrola konzistence 39

4.8 Aplikace vah na alternativy 40

5 Výsledky a diskuse **43**

5.1 Výsledky vícekriteriální analýzy 43

5.2 Diskuse 43

6 Závěr **47**

7 Seznam použitých zdrojů **48**

8 Seznam obrázků, tabulek, grafů a zkratek **54**

8.1 Seznam obrázků 54

8.2 Seznam tabulek 54

1 Úvod

V dnešní době je internet věcí neoddělitelnou součástí našich životů, přičemž jeho význam neustále roste s každým novým zařízením, které se připojuje k internetu. Od domácích spotřebičů po průmyslová čidla, IoT zařízení transformují způsoby, jakými interagujeme s naším okolím, automatizují procesy a zlepšují rozhodovací mechanismy ve všech sektorech. Tato revoluce přináší značné výhody, jako je optimalizace procesů, snížení nákladů a zlepšení kvality života, čímž se stává IoT nezbytným pro pokrok moderní společnosti.

Zabezpečení IoT sítí je proto nezbytně důležité pro zajištění bezpečného a spolehlivého prostředí v této stále více propojené době. S rostoucím počtem zařízení připojených k internetu se zvyšuje i riziko potenciálních bezpečnostních hrozeb, které mohou ohrozit soukromí uživatelů a celkovou integritu systémů. Ochrana těchto zařízení a dat, která generují a přenášejí, je zásadní.

V tomto kontextu se hlavním cílem této bakalářské práce stává zhodnocení stávajících technologií sítí typu mesh. Práce bude zaměřena na analýzu a posouzení různých síťových protokolů které jsou využívány v mesh IoT sítích. Cílem je poskytnout přehled o současném stavu zabezpečení v IoT prostředí a přispět k rozvoji efektivnějších a robustnějších bezpečnostních řešení, která dokáží čelit narůstajícím hrozbám v digitálním světě.

2 Cíl práce a metodika

Bakalářská práce je tematicky zaměřená na problematiku zabezpečení mesh sítí. Hlavním cílem je zhodnotit stávající zabezpečení mesh sítí a porovnat aktuální technologie.

Dílčí cíle práce jsou:

- charakterizovat IoT sítě a jejich zabezpečení,
- zhodnotit stávající bezpečnostní protokoly a mechanismy pro mesh sítě,
- identifikovat hlavní hrozby a slabiny mesh sítí,
- porovnat zabezpečení sítě Zigbee s jinou technologií.

Teoretická část bakalářské práce je založena na analýze a rešerši aktuálních odborných zdrojů. Tento průzkum je zaměřen především na nejnovější poznatky v oblasti mesh IoT sítí a bezpečnostních aspektů spojených s těmito technologiemi.

V praktické části práce je provedeno hodnocení vybraných technologií mesh IoT sítí, kde hlavním kritériem je bezpečnost. Toto hodnocení je založeno na aplikaci Saatyho metody vícekriteriální analýzy, což umožní objektivní srovnání a vyhodnocení jednotlivých technologií. Na základě syntézy teoretických a praktických poznatků jsou zpracovány závěry bakalářské práce, kde rovněž identifikuje nedostatky a navrhne možné jejich řešení

3 Teoretická východiska

3.1 Mesh sítě v IoT prostředí

Síť typu mesh je typ topologie místní lokální sítě (LAN), ve které jsou uzly nebo zařízení vzájemně propojeny nehierarchickým způsobem, což umožňuje efektivně spolupracovat a poskytovat širší pokrytí oblasti sítě, než jaké je možné u jiných topologií místních sítí, kde jsou uzly spojovány pomocí jediného centrálního prvku sítě, což je velmi důležitým aspektem v prostředí internetu věcí (IoT). (1)

3.1.1 Definice mesh sítí

Mesh síť je systém, který se skládá z více uzlů, které mohou být počítače, routery, switche a další zařízení napojená na danou síť. Každý uzel v síti vysílá své vlastní signály a díky tomu, že síť je decentralizovaná, tak přeposílání dat je možné pouze posíláním dat sousedním uzlům. Každý uzel v mesh síti je připojen k dalšímu uzlu pomocí vyhrazeného odkazu. Takové spojení umožňuje, aby data putovala od uzlu k uzlu bez zpoždění nebo selhání. (2) (3)

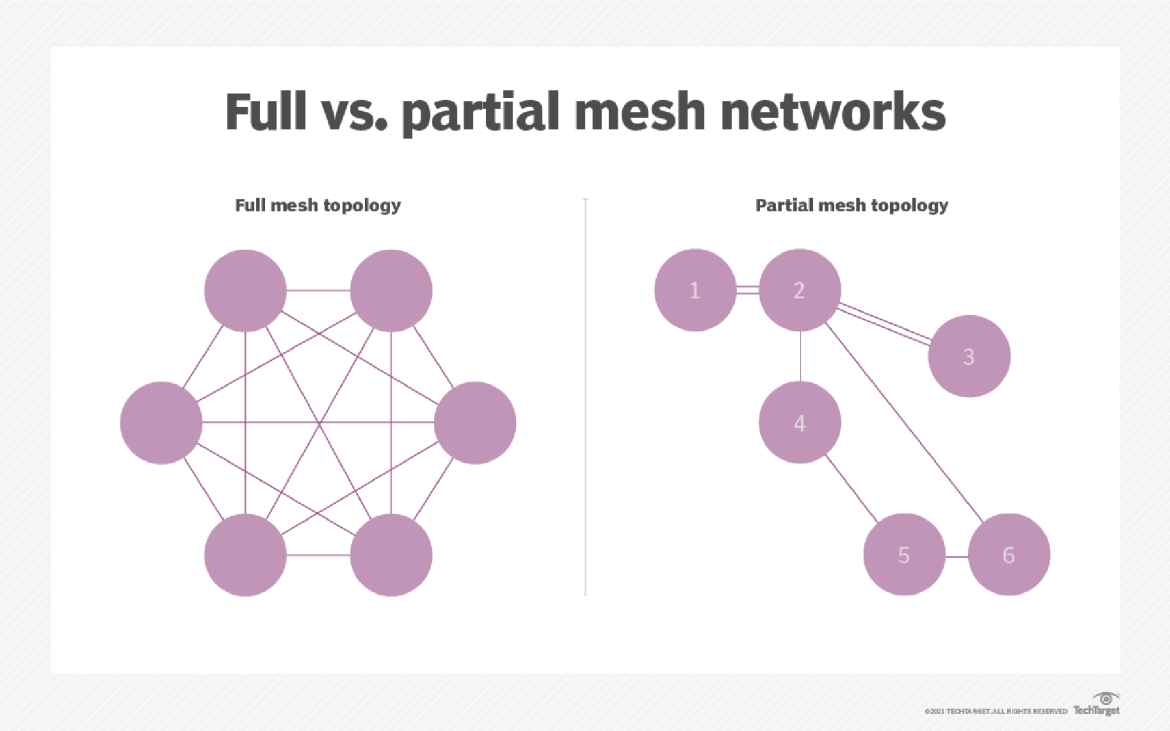
Koncovými zařízeními v mesh IoT sítích bývají typicky zařízení, která jsou vybavena senzory, které umožňují sběr dat a tato zařízení jsou později schopna sama pracovat s těmito daty bez závislosti na člověku, i když člověk může kdykoliv zasáhnout do jejich chodu. Dále se tato zařízení vyznačují nízkou spotřebou energie a spoluprací s cloudovými službami, které umožňují centralizovanou správu dat a přístup k nim z různých míst.

Brány (Gateways) jsou zařízení, která poskytují přístup k externím sítím prostřednictvím připojení, jako je internet. Brány mají za úkol provádět komunikaci mezi uzly a externím světem. (4) (5)

3.1.2 Topologie sítě

V úplné (full) mesh síti je každý uzel propojen se všemi ostatními uzly v síti viz obrázek 1, zatímco v částečné (partial) mesh síti jsou pouze některé uzly propojeny se všemi viz obrázek 1, takže některé uzly jsou propojeny s jinými skrze jiný uzel, který jim umožňuje komunikaci se zbytkem sítě. Rozhodnutí, zda využít úplnou mesh síť nebo pouze částečnou záleží na několika faktorech jako je celkový provoz a zatížení sítě, jaké uzly jsou ohroženy selháním a rozsah sítě. (6)

Obrázek 1 topologie úplné (full) mesh sítě a částečné (partial) mesh sítě



(6)

3.1.3 Charakteristika mesh sítí v IoT

Autoři odborného článku Hybrid Low-Power Wide-Area Mesh Network for IoT Applications identifikovali několik klíčových výhod spojených s použitím mesh IoT sítí v rámci rozsáhlých aplikací pro internet věcí. Výhody jsou následující:

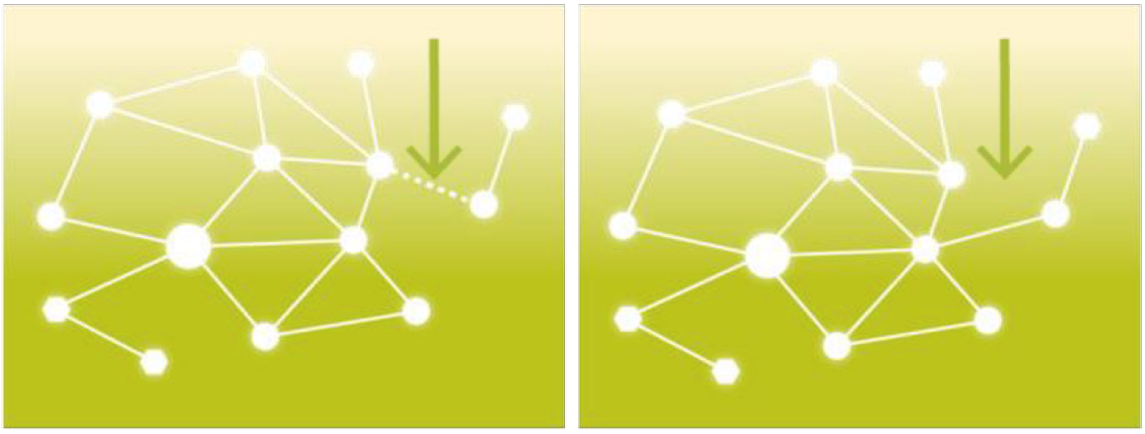
Spolehlivost komunikace: Redundantní cesty a více uzlů v síti zařizují, aby mesh IoT sítě fungovala spolehlivě a byla odolnější než jiné topologie, jelikož je nepravděpodobné, že dojde k přerušení komunikace, pokud jedna cesta selže.

Flexibilita a rozšiřitelnost: Mesh sítě jsou velmi flexibilní a snadno rozšiřitelné. Lze přidávat nová zařízení do sítě bez potřeby velkých úprav, což je velmi výhodné pro IoT prostředí, které se často rozrůstá.

Efektivní využití energie: Hlavní finanční výhodou pro obchodní závody, které chtějí implementovat mesh IoT sítě, je energetická efektivita, kdy mohou mesh sítě výrazně snížit spotřebu energie a náklady ve srovnání s podobně velkými sítěmi, kde se využívají tradiční topologie. Každý uzel v mesh síti spotřebovává méně energie oproti jiným technologiím, jelikož zařízení nemusí vydávat dostatečně silné signály, aby dosáhly na centrální server nebo cloud, aby dosáhly dalšího uzlu, kdežto v mesh síti uzly komunikují napřímo mezi sebou, pokud spolu sousedí. Výsledkem je úspora nákladů na výměnu baterií, spotřebu energie a životnost zařízení. (7) (8)

Samoregenerace sítě: Mesh síť je samoopravná pokud se dokáže automaticky opravit při změně prostředí. Pokud existující funkční spojení mezi dvěma uzly je blokováno nějakým objektem, který se mezi uzly nachází dočasně nebo trvale, síť automaticky bez zapojení jakéhokoliv uživatele změní svou topologii, aby mohla směrovat svůj provoz jinou cestou viz obrázek 2. Tato funkce je možná pouze u částečných mesh sítí, kdy nejsou všechny uzly propojeny, v případě úplné mesh sítě by byl signál přesměrován přes jiný uzel.

Obrázek 2 příklad samoregenerace mesh sítě



(9)

Škálovatelnost: Toto je klíčovou funkcí pro mesh IoT sítě. Síť se může automaticky rozšiřovat a může teoreticky obsahovat až neomezený počet koncových uzlů, takže síť může být velká, jak je potřeba. Díky zvýšenému dosahu je fyzické škálování jednodušší, protože signály se mohou šířit na velké vzdálenosti a zaznamenávat méně mrtvých míst. (9)

3.1.4 Charakteristika a architektura mesh IoT sítí

Zařízení internetu věcí jsou využívána jak v průmyslových, tak ve spotřebitelských aplikacích a jsou obvykle integrována do dalších zařízení, jako jsou mobilní zařízení, průmyslová zařízení a lékařská zařízení. Mohou být také v širokém rozsahu používána v chytrých městech. Následně jsou tato zařízení využívána k odesílání dat nebo k interakci s dalšími IoT zařízeními prostřednictvím sítě. (10)

Typy zařízení v mesh IoT sítích

Technologickou společností TechTarget, Inc. jsou IoT zařízení dělena na tři podskupiny. Mezi tyto podskupiny patří zařízení spotřebitelského IoT (CIoT/Customer IoT), zařízení IoT pro podniky (Enterprise IoT) a průmyslová IoT zařízení (IIoT/Industry IoT).

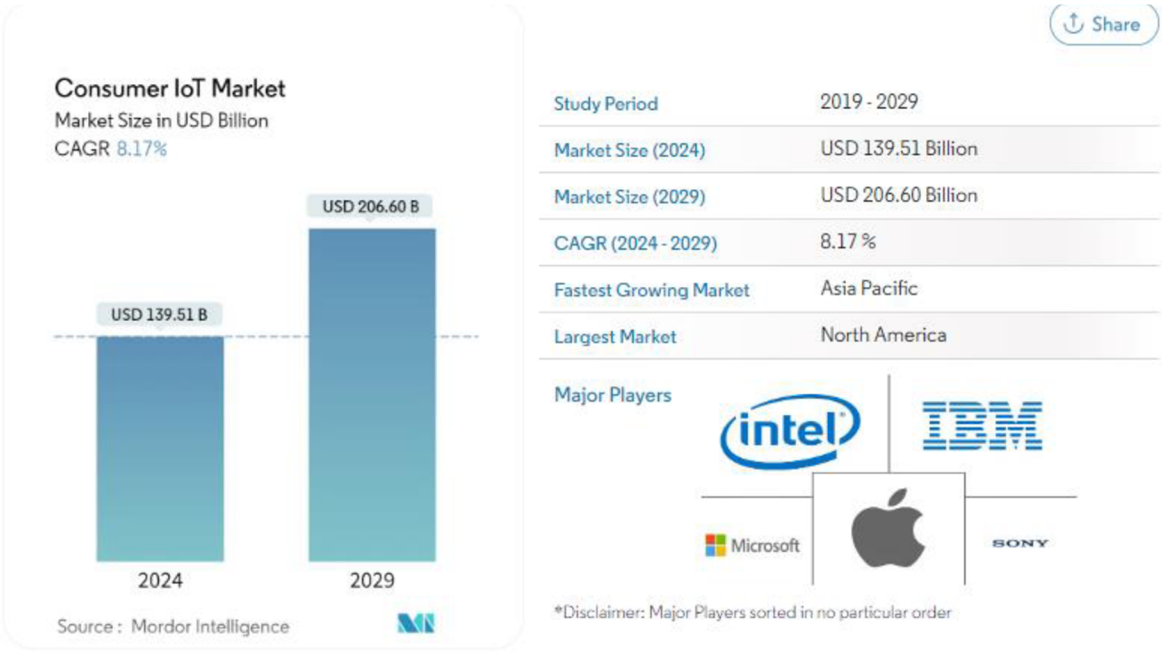
Spotřebitelské IoT

Ve světě internetu věcí je spotřebitelské IoT rozpoznáváno jako specifická podskupina s podstatnými odlišnostmi v aplikacích a zařízeních, která jsou pro přístup používána. Prostřednictvím internetu věcí jsou rozličné objekty, sítě a systémy spojovány, aby bylo usnadněno jejich používání a komunikace mezi nimi. Automatizace chytrého domova je považována za příkladnou ilustraci spotřebitelského internetu věcí v praxi, kde jsou všechna chytrá zařízení spojena do jedné sítě, což vede k zvýšené komunikaci a zjednodušení pro uživatele. S rostoucí inteligencí spotřební elektroniky jsou podniky vedeny k využívání různých řešení IoT ve spotřební elektronice pro účely monitorování, správy a přizpůsobení produktů.

Spojení mezi trhem IoT a spotřební elektronikou je charakterizováno širokým rozsahem funkcí, jako jsou snímání, ovládání a kontrola, což vede ke vzniku chytrých a energeticky účinných elektronických zařízení. Tyto zařízení jsou oceňována za schopnost snadno se propojit s výrobní sítí přes internet a za poskytování cenných informací, jako jsou údaje o výkonu produktu, trendy využívání a spotřeba energie, což je považováno za jeden z klíčových přínosů v průmyslu. (11) (12)

Zařízení a aplikace spotřebitelského IoT, která mají schopnost nevratně měnit běžný život jsou rychle integrována do každodenního života, zvlášť v Evropě, Americe a Asii. Dle analýzy trhu je v roce 2024 velikost trhu 139,51 mld USD a v roce 2029 je očekávána velikost trhu 206,60 mld USD se složeným ročním tempem růstu (CAGR) 8,17 % viz obrázek 3.

Obrázek 3 velikost trhu spotřebitelského IoT



(13)

Po vypuknutí COVID-19 byla zaznamenána změna v postoji spotřebitelů k technologiím IoT. Rostoucí poptávka po IoT zařízeních byla pozorována v různých sektorech, včetně domácností, kde jsou tato zařízení využívána pro automatizaci a efektivnější provádění domácích úkolů, maloobchodu, kde přispívají k logistice a zlepšení zákaznického servisu, výrobního průmyslu, kde podporují automatizaci výrobních procesů, zdravotnictví, kde jsou nasazovány pro dezinfekci, distribuci léků a asistenci pacientům, a v dalších oblastech, kde přinášejí zlepšení efektivity a bezpečnosti. (13)

<u>Oblasti využití CIoT</u>:

Domácí automatizace a zabezpečení:

Inteligentní zabezpečovací systémy jsou instalovány v domácnostech, aby umožňovaly majitelům na dálku monitorovat své domovy prostřednictvím dveřních a okenních senzorů, pohybových detektorů a kamer. Uživatelům jsou poskytována upozornění v reálném čase v případě zjištění neobvyklé aktivity.

Inteligentní zámky a přístupové systémy jsou implementovány pro poskytování bezpečnějšího a pohodlnějšího způsobu správy přístupu do domů. Umožňují vzdálené odemykání a zamykání dveří a sledování, kdo a kdy vstoupil nebo opustil dům.

Automatizace osvětlení je realizována tak, že umožňuje uživatelům dálkově ovládat osvětlení, nastavovat časovače a automatizovat osvětlení na základě denního světla nebo přítomnosti osob v místnosti. Tím je zvyšována energetická účinnost.

Inteligentní termostaty a systémy klimatizace jsou navrženy tak, aby uživatelům umožňovaly optimalizovat nastavení teploty v domě pro maximální komfort a energetickou účinnost. Systémy se mohou učit z uživatelských preferencí a automaticky se přizpůsobovat změnám počasí.

Energetické monitorování a správa jsou integrovány do systémů pro monitorování spotřeby energie v reálném čase, které uživatelům umožňují sledovat a řídit spotřebu energie svých zařízení. To vede k úsporám nákladů a snížení dopadu na životní prostředí. (11) (14)

Sledování majetku:

V rámci spotřebitelského IoT je umožněno a usnadněno sledování všeho, od chytrých telefonů, fotoaparátů, klíčů, přes domácí mazlíčky, až po zranitelné členy rodiny, jako jsou děti a starší osoby. Monitorování čehokoli, co podporuje IoT a je připojeno, je zajištěno i na delší vzdálenosti. (12)

Chytrá nositelná zařízení:

V oblasti nositelné technologie dochází k rychlému rozšiřování popularity zařízení vedle tradičně populárních chytrých hodinek a fitness trackerů. Zařízení určená pro spotřebitele, vybavená intuitivními aplikacemi s rozmanitou funkcionalitou, jsou nyní navrhována s cílem transformovat způsob, jakým spotřebitelé prožívají každodenní život. Kromě toho jsou vyvíjeny inteligentní boty, které monitorují chůzi uživatele, a chytré opasky pro nevidomé, vybavené kamerami a senzory, jež uživatelům poskytují informace o objektech v jejich bezprostředním okolí.

Monitorování zdraví:

Zdravotnictví v IoT je další významnou aplikační oblastí, kde spotřebitelský internet věcí roste rychlým tempem a zlepšuje zkušenosti pacientů a pečovatelů. Rozsah využití byl rozšířen od komplexního monitorování zdravotního stavu pacientů, přes aplikace inteligentních sluchadel, dohledu nad zdravotnickým zařízením, až po specializovanou péči o seniory. Tento trend ukazuje narůstající spojení mezi osobními zdravotními službami a technologiemi internetu věcí, což signalizuje změnu modelu sektoru zdravotní péče.

Osobní poradci:

Osobní asistenti, jako jsou Siri, Alexa a Google Assistant, jsou již dlouho součástí technologického prostředí a přispívají k významnému pokroku ve vývoji IoT. Integrace polohových senzorů, mapového softwaru, Bluetooth, GPS , aplikací pro chytré telefony, RFID tagů a sítí umožňuje dosažení úrovně přesnosti síťového snímání, jež napomáhá snadnému sledování položek. (11)

Podnikové IoT

Podnikové IoT je definováno jako následující fáze konceptu internetu věcí. Podnikům je umožněno navázat více spojení, což vede ke zvýšení využití, snížení manuální práce, škálování podnikových procesů a lepšímu plánování. Tím je dosaženo zvýšení operační efektivity, snížení provozních nákladů a zvýšení celkové efektivity. Z tohoto důvodu je stále více podniků motivováno k investování do fyzických produktů s integrovanými výpočetními zařízeními.

Lepší zákaznický zážitek a získávání detailnějších rozsáhlých datových sad k analýze mohou být také poskytnuty využitím podnikového IoT. Existuje mnoho způsobů, jak může být podnikové IoT využito k efektivnějšímu a produktivnějšímu provádění každodenních podnikových procesů a zvýšení produktivity zaměstnanců.

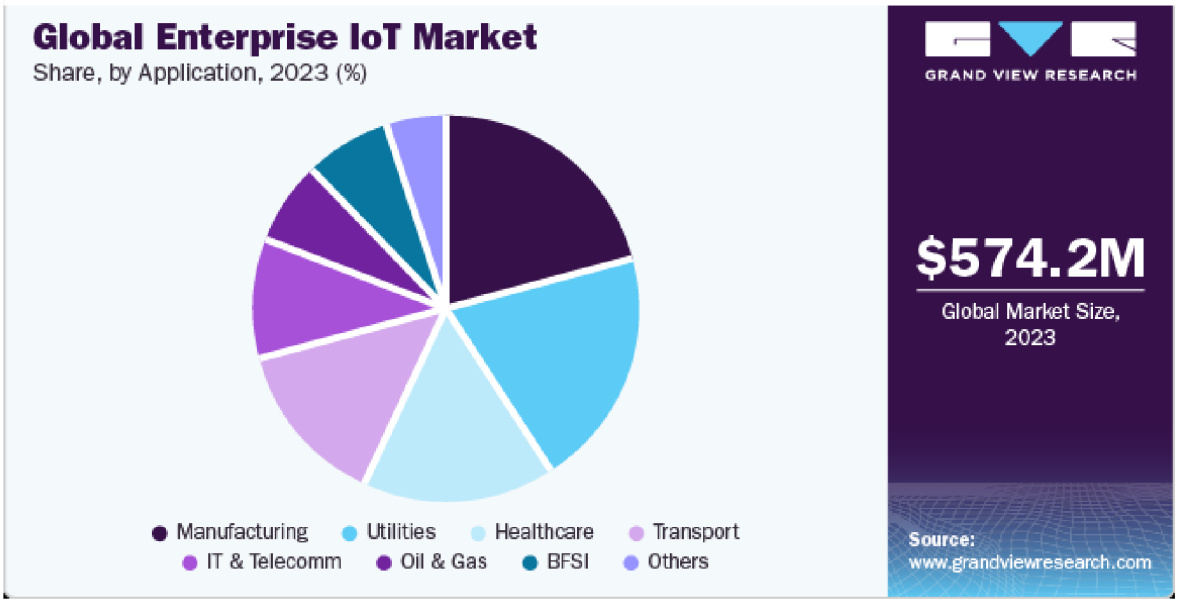
Automatizace podnikových procesů závislých na kontextových informacích poskytovaných naprogramovanými zařízeními, jako jsou stroje, vozidla, inteligentní zařízení a další vybavení, je dosažena využitím kombinace technologií včetně zařízení s vestavěnými senzory a aktuátory, internetové komunikace a cloudových platforem. Navíc mohou být těmto zařízením odeslány řídící instrukce na základě určitých podnikových pravidel prostřednictvím aplikací podnikového IoT. (15) (16)

Velikost globálního trhu podnikového internetu věcí byla v roce 2023 odhadnuta na 574,2 milionů USD a bylo očekáváno, že v období 2024 až 2030 poroste složenou roční mírou růstu 14,1 %. Očekává se, že růst trhu bude poháněn vývojem technologií jako Bluetooth, Wi-Fi, Insteon, Zigbee a další, které slouží jako základní infrastruktura pro implementace IoT a umožňují bezproblémovou konektivitu a komunikaci mezi zařízeními.

Největší podíl tržeb na globálním trhu podnikového internetu věcí byl v roce 2023 dosažen ve výrobním sektoru. Rozvojem koncepce Průmyslu 4.0 bylo výrobcům umožněno přijmout technologie IoT, což vedlo k podpoře změny v modelu výrobních procesů. Sektor dopravy je očekáván, že zaznamená významný růst na trhu, což je připisováno rostoucí

integraci technologií IoT, jež mají revoluční vliv na transport a logistiku. V sektoru dopravy bylo umožněno sledování v reálném čase, prediktivní údržba a optimalizace provozu prostřednictvím implementace řešení IoT. Finanční sektor a sektor těžby ropy a plynu byly identifikovány jako nejmenší ze zmíněných sektorů na globálním trhu podnikového internetu věcí v roce 2023 viz obrázek 4. (17) (18)

Obrázek 4 rozdělení dle sektorů ve využití podnikového IoT



(17)

<u>Oblasti využití podnikového IoT</u>:

Chytré kanceláře:

V chytrých kancelářích bylo zavedeno inteligentní řízení energie, což umožnilo zvýšení energetické účinnosti prostředí. Současně byly implementovány systémy pro zaznamenávání přístupu a kontrolu, poskytující vyšší úroveň bezpečnosti a regulace vstupů do objektu. Dále bylo využito vnitřní sledování zaměstnanců, aby se zefektivnil pohyb a lokalizace lidí uvnitř budovy. Monitorování obsazenosti zasedacích místností a toalet bylo zavedeno s cílem optimalizovat využívání prostor a snížit čekací doby. Kvalita vnitřního vzduchu a monitorování systémů topení, ventilace a klimatizace (HVAC) byly rovněž sledovány, zajišťujíc na pracovišti zdravé pracovní podmínky a efektivitu systémů. (19)

Prodej:

Pro řízení zásob jsou využívány technologie IoT, jako jsou RFID senzory a chytré štítky, které umožňují sledovat a řídit zásoby v reálném čase. Tím je snižována lidská chyba a minimalizován odpad, což zajišťuje, že správné produkty jsou vždy na skladě.

Při analýze prodeje mohou IoT zařízení sbírat informace o chování zákazníků, jejich preferencích a minulých nákupech. Tyto informace mohou být využity ke zlepšení prodejních a marketingových strategií. Získaná data pomáhají obchodníkům porozumět potřebám zákazníků a přizpůsobit své nabídky.

Pro prevenci ztrát mohou IoT kamery a senzory monitorovat aktivitu v obchodech za účelem odrazení krádeží a podvodů. To obchodníkům pomáhá zajistit bezpečnost jejich produktů a zákazníků, čímž snižují ztráty a zvyšují zisky.

V optimalizaci dodavatelského řetězce mohou IoT senzory sledovat zboží od výroby po dodání, zajišťujíc, že produkty jsou doručovány včas a ve vhodné kvalitě. To obchodníkům umožňuje zlepšit efektivitu svého dodavatelského řetězce, snížit náklady a zvýšit spokojenost zákazníků. (20)

Zdravotnictví:

Monitorování pacientů na dálku je identifikováno jako nejběžnější aplikace IoT zařízení ve zdravotnictví. Zdravotní metriky jako tepová frekvence, krevní tlak, teplota a další jsou automaticky sbírány od pacientů, kteří nejsou fyzicky přítomni v lékařském zařízení. Tím je odstraněna nutnost cestování pacientů k poskytovatelům zdravotní péče nebo samostatného sběru dat pacienty.

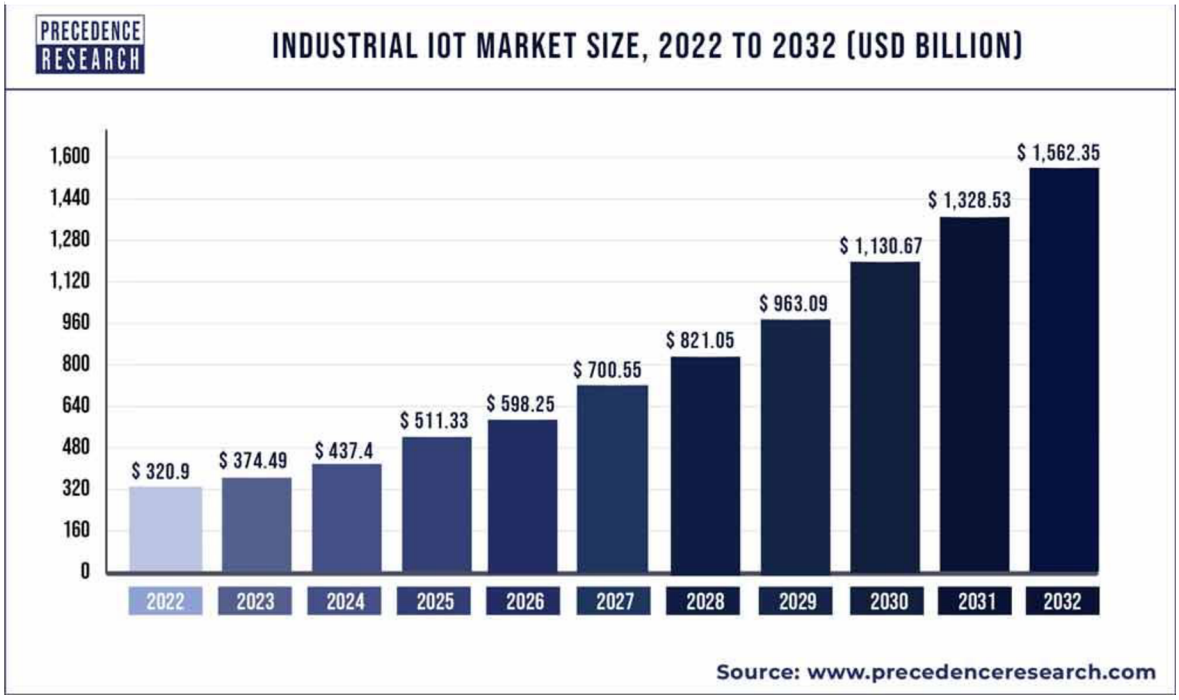
V nemocnicích a jiných zdravotnických zařízeních jsou používána IoT zařízení, aby byly osoby při vstupu do nemocničních pokojů upozorněny na nutnost dezinfekce rukou. Tato zařízení mohou dokonce poskytovat instrukce k nejlepšímu postupu dezinfekce s ohledem na snížení specifického rizika pro jednotlivé pacienty. Jedním z hlavních omezení je, že tato zařízení mohou pouze připomínat nutnost čištění rukou, nemohou provést dezinfekci za lidi. Přesto ve výzkumu bylo ukázáno, že používání těchto zařízení může v nemocnicích snížit míru infekce o více než 60 procent. (21)

Průmyslové IoT

Pro použití ve výrobních závodech nebo v průmyslových prostředích jsou určena zařízení IIoT, která jsou primárně tvořena senzory monitorujícími montážní linky nebo další výrobní procesy. Informace získané z těchto senzorů jsou odesílány do aplikací pro monitorování s cílem zajistit optimální průběh klíčových procesů. Současně tyto senzory umožňují předvídat potřebu výměny součástek a tím předcházet neplánovaným výpadkům. IIoT se používá v mnoha průmyslových odvětvích, včetně výroby, energetického managementu, veřejných služeb, ropy a zemního plynu. (22) (23)

V roce 2023 byla velikost trhu odhadnuta na 374,49 miliardy USD. Do roku 2032 se očekává, že velikost trhu dosáhne 1,562.35 miliardy USD. Růst trhu v období od roku 2023 do roku 2032 byl předpovězen s roční složenou mírou růstu 17,2 % viz obrázek 5. (24)

Obrázek 5 velikost trhu IIoT a jeho odhadovaný růst



(24)

<u>Oblasti využití průmyslové IIoT</u>:

Automobilový průmysl:

Do automobilů jsou začleňována zařízení IoT, zahrnující technologie jako senzory, cloud computing, aplikace a další prvky, které jsou spojeny do komplexního systému. Tento systém umožňuje vzájemné propojení automobilů, prediktivní údržbu, řízení vozového parku, pojištění a mnoho dalšího. Použitím internetu věcí v automobilovém průmyslu je výrobcům umožněna realizace inovací, které mají potenciál proměnit automobily v systémy s vlastnostmi přibližujícími se umělé inteligenci. (25)

Zemědělský průmysl:

V oblasti zemědělství jsou k posílení různých zemědělských metod používány drony, jak pozemní, tak vzdušné. Tyto metody zahrnují posouzení zdravotního stavu plodin, zavlažování, sledování růstu plodin, aplikaci postřiků, výsadbu a analýzu půdy a polních podmínek.

Pro sledování a geofencing hospodářských zvířat majitelé farem využívají bezdrátové aplikace IoT, které shromažďují informace o umístění, pohodě a zdraví jejich skotu. Tato data jsou využívána k prevenci šíření onemocnění a ke snížení nákladů na práci. (26)

Ropný a plynárenský průmysl:

Některé ropné společnosti provozují flotilu autonomních letounů, která pomocí vizuálního a infračerveného snímání identifikují možné problémy v ropovodech. Informace získané tímto způsobem jsou poté kombinovány s údaji z jiných typů senzorů, což slouží k zajištění bezpečnosti operací. (22)

Komunikační protokoly

Zigbee:

Skupinou Zigbee Alliance byla vytovřena technologie Zigbe, která je využívána v PAN (Persoanl Area Network) a je založena na základě standardu IEEE 802.14.4, což je standard pro bezdrátové sítě s nízkou rychlostí. Zigbee představuje otevřený standard, který je navržen pro aplikace s nízkým přenosem dat a nízkou spotřebou energie, to v teorii umožňuje vzájemné používání produktů různých výrobců, nicméně v důsledku úprav jednotlivými výrobci nastávají problémy s interoperabilitou. (27)

Standardem IEEE 802.15.4 jsou podporovány hvězdicové a peer-to-peer technologie. Technologií Zigbee je umožněno propojovat zařízení pomocí hvězdice nebo dvěma druhy peer-to-peer, mesh a cluster tree. V sítích technologie Zigbee jsou identifikovány tři druhy zařízení: koordinátor, router a koncové zařízení. Koncovým zařízením není umožněno směrovat provoz, tedy jejich účelem je odesílání informací. Mohou být napájeny bateriemi a často jsou konfigurovány do režimu spánku za účelem úspory energie, přičemž čekají na odpověď od rodičovského zařízení (routeru), skrze které je směrována příchozí komunikace. Routery mají za úkol směrování provozu v síti a uchovávání zpráv, které jsou předávány jejich potomkům (koncovým zařízením). Koordinátor, sloužící jako specifický typ routeru, umožňuje vytvoření sítě a konfiguraci různých síťových nastavení. V sítích Zigbee jsou data přenášena ve formě paketů a mohou být posílána buď unicastově nebo broadcastově. (28) (29)

Zigbee je využíváno mnoha společnostmi v oblasti kabelového a telekomunikačního průmyslu v jejich set-top boxech, satelitních přijímačích a domácích bránách pro nabídku služeb monitorování domovů a správy energie zákazníkům. Dále je Zigbee používáno poskytovateli, kteří nabízejí řešení propojeného osvětlení pro domácnosti a firmy. Produkty pro chytrý domov založené na Zigbee umožňují uživatelům ovládat LED dekorace, žárovky,

dálkové ovladače a vypínače jak lokálně, tak i na dálku, což umožňuje efektivnější správu spotřeby energie. (28)

Zigbee poskytuje škálovatelnost s podporou až 65,000 uzlů v jedné síti, jeden rodič dokáže podporovat maximálně 65 zařízení v síti. Pracováno je na frekvenčních pásmech 2.4 GHz, 868 MHz v Evropě a 915 MHz v USA, s maximálním dosahem, který může být až 100 metrů v interiéru a větším v exteriéru. Je dosahována přenosová rychlost dat 250 kbps na frekvenci 2.4 GHz. Díky nízké latenci, typicky menší než 15ms pro přímý přenos, a vysoké energetické účinnosti je tato technologie ideální pro domácí automatizaci a průmyslové řešení. (28) (30)

Zigbee využívá šifrování AES-128 pro zajištění bezpečnosti dat přenášených mezi zařízeními. Autentizace je zajištěna předáváním klíčů a osobní identifikací (PSK), což zvyšuje odolnost vůči neoprávněnému přístupu. Zigbee Alliance pravidelně aktualizuje bezpečnostní protokoly, přičemž technologie je v souladu s bezpečnostními standardy IEEE 802.15.4. (31)

Bluetooth Mesh:

Bluetooth mesh je technologie Bluetooth, která je vlastněna skupinou Bluetooth Special Interest Group (SIG). Byla spuštěna v červenci 2017. Mesh síťování funguje na Bluetooth Low Energy (LE) a je kompatibilní s hlavní specifikací verze 4.0 a vyšší. Síťování Bluetooth Mesh umožňuje komunikaci mezi mnoha zařízeními (m:m) a je optimalizováno pro vytváření sítí s velkým počtem zařízení. Je ideálně vhodné pro řešení kontrolního monitorování a automatizace, která vyžadují, aby desítky, stovky nebo tisíce zařízení komunikovaly mezi sebou. (32) (33)

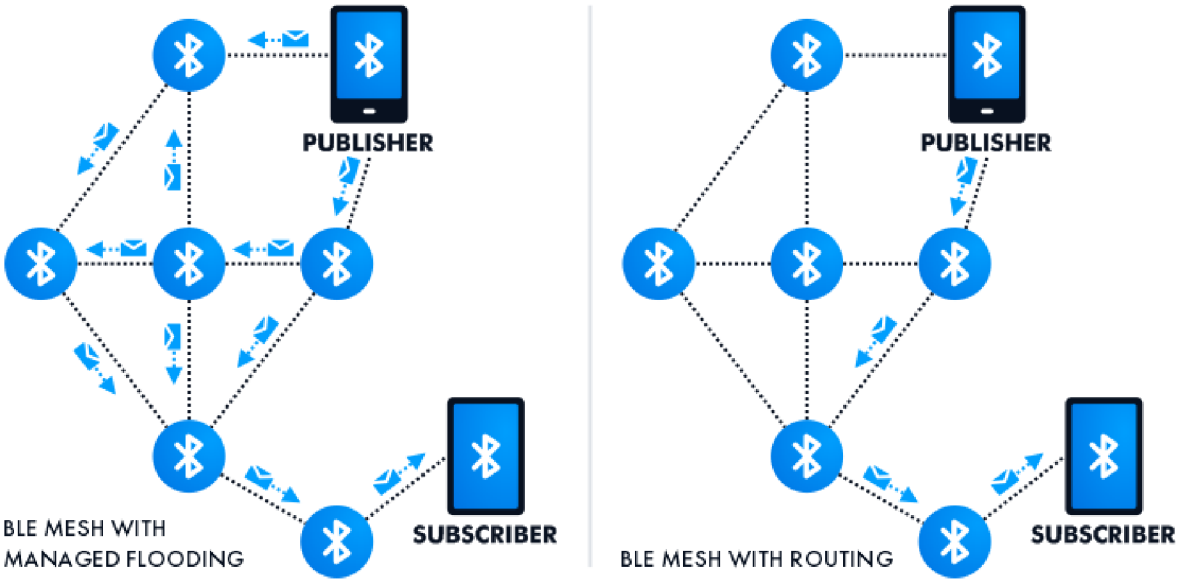
Rozlišujícím faktorem mezi sítí Bluetooth Mesh a Zigbee či jinými technologiemi je primárně metoda šíření zpráv. Na rozdíl od ostatních bezdrátových sítí, které jsou závislé na směrování, Bluetooth Mesh síť využívá princip zaplavení tzv. flooding viz obrázek 6. Tento přístup poskytuje model komunikace peer-to-peer, kde všechny uzly komunikují přímo mezi sebou. Princip zaplavení umožňuje efektivní přenos zpráv bez nutnosti využití složitých algoritmů pro směrování. Nezávislost uzlů společně s metodou šíření zpráv po více cestách podporuje škálovatelnost sítě Bluetooth Mesh. (34)

Bluetooth Mesh sítě jsou schopné podpory tisíců zařízení, což umožňuje jejich aplikaci v širokém spektru prostředí, včetně smart home systémů a průmyslových IoT řešení. Technologie je provozována na 2.4 GHz frekvenčním pásmu, což jí umožňuje dosahovat maximálního dosahu až 200 metrů. Jednou z charakteristik Bluetooth Mesh je schopnost dosáhnout vyšší rychlosti přenosu dat, která může dosahovat až 1 Mbps. Nicméně, tato

technologie může vykazovat proměnlivou latenci, která v některých situacích může dosáhnout až několika sekund. (35)

Bluetooth Mesh využívá šifrování AES-CCM a AES-CMAC a podporuje autentizaci pomocí předávání klíčů a PSK. Bezpečnostní protokoly jsou aktualizovány pravidelně skrze Bluetooth Special Interest Group, který zajišťuje, že technologie je v souladu s nejnovějšími bezpečnostními požadavky a standardy pro mesh sítě. (32)

Obrázek 6 porovnání floodingu a routingu v Bluetooth Mesh sítích



(34)

IQRF:

IQRF je bezdrátová mesh technologie fungující v sub-GHz ISM rádiových frekvenčních pásmech. Pro její použití není požadována infrastruktura od externích dodavatelů, ani licenční poplatky nebo poplatky operátorům. Obecnost funkčnosti transreceiverů je zajištěna softwarovým vybavením, které je možné do nich nahrát, ať už jde o již připravený, avšak rozšiřitelný síťový plugin nebo o aplikaci vytvořenou uživatelem v programovacím jazyce C. (36)

IQRF je specializováno na bezdrátovou komunikaci pro IoT a nabízí topologie hvězda, mesh, lineární a strom. Technologie je provozována na frekvencích 433, 868 a 916 MHz s maximálním dosahem až 600 metrů v exteriéru a rychlostí přenosu dat 19.8 kbps. S podporou až stovky zařízení v síti a latencí typicky menší než 100 ms. IQRF je považováno za vhodné pro domácí automatizaci, průmyslové IoT a smart city aplikace. Vyznačuje se vysokou energetickou účinností a je založeno na vlastních standardech, které jsou navrženy pro

kompatibilitu s mnoha běžnými technologiemi, což usnadňuje integraci do různorodých systémů. (37) (38)

IQRF poskytuje šifrování AES-128 a autentizaci prostřednictvím předávání klíčů a síťového hesla, což umožňuje vytvoření bezpečného komunikačního kanálu. Aktualizace bezpečnostních protokolů probíhají méně často než u jiných technologií. IQRF se snaží dodržovat vlastní bezpečnostní standardy s důrazem na robustní bezpečnostní funkce. (39)

3.2 Zabezpečení v mesh IoT sítích

V důsledku toho, že přes IoT zařízení protékají cenná a soukromá data, jsou vystavena riziku kybernetických útoků. Přidání každého nového zařízení do sítě zvyšuje digitální útočnou plochu, což je množství zranitelných bodů, které mohou neautorizovaní uživatelé využít k proniknutí do systému. Tato stálá hrozba krádeže dat a dalších narušení zdůrazňuje zásadní význam zabezpečení v oblasti IoT.

Propojení IoT zařízení, přestože přináší efektivitu, zároveň zvyšuje bezpečnostní rizika. Útočník může prostřednictvím jednoho napadeného zařízení získat přístup k celému systému. V podnikovém prostředí, kde jsou IoT zařízení implementována do sítě, získávají přístup k důvěrným datům a zásadním systémům firmy. Útočníci se často zaměřují na nezabezpečené tiskárny, inteligentní osvětlení a jiná kancelářská zařízení, aby se dostali do sítě a k jejím datům. (40)

3.2.1 Bezpečnostní mechanismy

Šifrování dat:

Šifrování je bezpečnostní opatření v kybernetické bezpečnosti, které převádí čitelný text na šifrovanou formu. Při šifrování je použit šifrovací algoritmus a šifrovací klíč k zakódování dat do šifrovaného textu. Jakmile je tento šifrovaný text přenesen příjemci, klíč je využit k dekódování šifrovaného textu zpět na původní hodnotu. Šifrovací klíče fungují podobně jako fyzické klíče, což znamená, že pouze uživatelé disponující správným klíčem mohou odemknout nebo dešifrovat šifrovaná data. Šifrování je děleno na symetrické a asymetrické šifrování.

U symetrických šifrovacích algoritmů dochází k využití identického klíče pro proces šifrování i dešifrování. To znamená, že subjekt, který provádí šifrování dat, je nucen tajný klíč sdílet se všemi autorizovanými stranami, aby bylo možné data dešifrovat. Vzhledem k své rychlosti a jednoduchosti implementace je symetrické šifrování obvykle upřednostňováno pro šifrování velkého objemu dat oproti asymetrickému šifrování. Příklady symetrického šifrování

jsou AES (Advanced Encryption Standard) a DES (Data Encryption Standard), který je předchůdcem AES.

Asymetrické šifrování využívá dva klíče, které jsou rozdílné, ale matematicky na sebe navázány, jedná se o veřejný a soukromý klíč. Veřejný klíč bývá běžně sdílen s širokou veřejností a je dostupný komukoli, kdežto soukromý klíč je chráněn před neoprávněným přístupem a je k dispozici pouze majiteli tohoto klíče. Šifrování veřejným klíčem zajišťuje, že zpráva může být dešifrována pouze zamýšleným příjemcem pomocí odpovídajícího soukromého klíče, i kdyby došlo k narušení informací během přenosu. Šifrování soukromým klíčem umožňuje příjemci informací ověřit identitu odesílatele, jelikož data, která byla pozměněna neautorizovaným uživatelem, nebudou moci být dešifrována. Často využívaným algoritmem je RSA. (41) (42)

Autentizace:

Autentizace je prováděna serverem, když je nutné přesně identifikovat, kdo přistupuje k poskytovaným informacím. Klient používá autentizaci za účelem ověření, že server je opravdu tím systémem, za který se vydává. V rámci autentizačního procesu je požadováno, aby uživatel nebo počítač prokázal svou identitu vůči serveru nebo klientu. Autentizace serverem se obvykle odvíjí od použití uživatelského jména a hesla, zatímco další metody mohou zahrnovat technologie jako jsou karty, skenování sítnice, rozpoznávání hlasu a otisky prstů. Server obvykle autentizuje klienta poskytnutím certifikátu, v němž důvěryhodná třetí strana, jako Verisign nebo Thawte, potvrzuje, že server náleží k očekávané entitě, například bance. Autentizace sama o sobě nespecifikuje, jaké akce může jednotlivec provádět nebo které soubory může prohlížet, slouží pouze k identifikaci a ověření identity osoby nebo systému. (43)

Monitorování a detekce hrozeb:

Monitorování hrozeb je charakterizováno jako metoda nebo proces zaměřený na kontinuální dohled nad sítěmi nebo koncovými body za účelem identifikace bezpečnostních rizik, jako jsou narušení bezpečnosti nebo úniky dat. Toto sledování umožňuje získat přehled o chování v síti a uživatelích, kteří ji využívají, což napomáhá lepší ochraně dat a zabraňuje nebo omezuje poškození způsobená bezpečnostními incidenty. Řešení pro monitorování hrozeb shromažďují informace ze senzorů sítě a zařízení, stejně jako z agentů koncových bodů a dalších bezpečnostních technologií, aby identifikovaly vzory naznačující potenciální hrozbu nebo bezpečnostní incident. (44)

Detekce hrozeb a reakce na ně představuje postup identifikace jakékoliv škodlivé aktivity, která by mohla ohrozit síť, následovaný vytvořením vhodné odpovědi k minimalizaci nebo neutralizaci hrozby předtím, než by mohla využít přítomné zranitelnosti. Při detekci

a zmírňování hrozeb je rychlost klíčová. Bezpečnostní programy musí být schopny rychle a efektivně identifikovat hrozby, aby útočníci neměli dostatek času prozkoumávat citlivá data. (45)

Aktualizace bezpečnostních protokolů:

Aktualizace protokolů síťového zabezpečení není důležitá pouze pro prevenci úniků dat, také přispívá k ochraně před jinými typy kybernetických útoků, jako jsou malware a ransomware. Dalším důvodem pro pravidelnou aktualizaci protokolů síťového zabezpečení je zajistit soulad s průmyslovými regulacemi a standardy. V závislosti na odvětví a umístění může být pro společnost nezbytné dodržovat konkrétní zákony nebo standardy, aby chránila citlivá data. V Evropské hospodářském prostoru je vyžadováno nařízení o ochraně osobních údajů (GDPR), aby organizace, které zpracovávají osobní údaje jednotlivců v Evropském hospodářském prostoru (EHP), přijaly určitá opatření k ochraně těchto dat. (46) (47)

3.2.2 Bezpečnostní protokoly

Transport Layer Security:

Transport Layer Security (TLS) je bezpečnostní protokol, který je široce využíván k ochraně soukromí a zabezpečení dat při komunikaci na internetu. Primárně je TLS využíván pro šifrování spojení mezi webovými aplikacemi a servery, například při načítání internetových stránek prostřednictvím webových prohlížečů.

Zahájení spojení TLS probíhá prostřednictvím procesu nazývaného TLS handshake. Při přístupu uživatele na webovou stránku, která TLS využívá, dochází k zahájení TLS handshake mezi klientem a webovým serverem. V průběhu TLS handshake dochází k výměně informací mezi klientem a webovým serverem, kde obě strany společně stanoví, jakou verzi protokolu TLS budou využívat pro komunikaci. Součástí procesu je také dohoda na specifických šifrovacích sadách pro zabezpečení přenosu dat. Identita serveru je během tohoto procesu ověřována pomocí TLS certifikátu serveru, což zaručuje klientovi, že komunikuje s autentickým serverem. Po úspěšném ověření a dohodě na parametrech spojení jsou vytvořeny relační klíče pro šifrování komunikace, čímž se zvyšuje bezpečnost přenášených zpráv. (48)

Datagram Transport Layer Security:

Datagram Transport Layer Security (DTLS) je protokol využívaný k zabezpečení komunikace založené na datagramech. Je založen na protokolu TLS a poskytuje podobnou úroveň zabezpečení. Jako datagramový protokol DTLS negarantuje pořadí doručení zpráv ani to, že budou zprávy vůbec doručeny. Nicméně, DTLS získává také výhody datagramových protokolů, zejména nižší režii a sníženou latenci. (49) (50)

3.3 Hrozby a slabiny mesh IoT sítí

V následující části budou zkoumány různé faktory, které mohou představovat bezpečnostní hrozby a slabiny v kontextu mesh IoT sítí. Zohlední se zde potenciální útoky, zranitelnosti a nedostatky v zabezpečení, které mohou ohrozit bezpečnost a funkčnost těchto sítí.

3.3.1 Hrozby pro mesh IoT sítě

Fyzické hrozby:

Od chvíle svého vzniku je každé fyzické zařízení vystaveno možnosti neautorizované manipulace, která neodpovídá záměrům výrobce nebo distributora. Zejména IoT zařízení přitahují pozornost lidí poháněných čistou zvědavostí, útočníků v hledání nových technických výzev, osob usilujících o získání obchodních informací o výrobcích a službách, jedinců usilujících o finanční prospěch a mnoho dalších s rozmanitými škodlivými úmysly. Přesně proto je důležité nahlížet i na fyzické zabezpečení zařízení v IoT sítích.

Pro získání přístupu k vnitřním komponentám zařízení může být využito fyzické otevření tohoto zařízení. Dalším krokem může být připojení konektoru k fyzickému portu na zařízení, což umožní přímý přístup k jeho funkcím. Kromě toho lze využít bezkontaktní technologie pro detekci aktivity vyzařované zařízením, jako je elektromagnetické záření, zvuky vysoké nebo nízké frekvence, či kolísání napájecího zdroje, což poskytuje další možnosti pro analýzu a interakci se zařízením bez nutnosti fyzického připojení. (51)

Man in the Middle:

V oblasti kryptografie a bezpečnosti informačních systémů je útok Man-in-the-Middle (MITM) typem útoku, kde útočník bez vědomí dvou komunikujících stran přenáší a potenciálně upravuje jejich vzájemnou komunikaci. Tyto strany přitom věří, že jsou ve spojení přímo mezi sebou. Útok MITM označuje situace, kdy se útočník vloží do komunikace mezi uživatelem a aplikací, a to buď pro účely skrytého odposlouchávání nebo pro předstírání identity jedné z komunikujících stran, což vede k narušení původně bezpečného informačního toku. (52)

Botnet:

Botnety jsou využívány pro způsobení přetížení cílených aplikací, webových stránek nebo služeb, čímž slouží jako nástroje pro provedení DDoS (Distributed Denial of Service) útoků, avšak mohou být také využity pro šíření spamu, adwaru, spywaru a podobně. Útočník získá kontrolu nad zařízením prostřednictvím malwaru. Vlastník takto ovlivněného zařízení si často není vědom toho, že jeho zařízení bylo infikováno a že se stalo součástí botnetu.

V rámci tradiční architektury botnetů se používá klient-server model, který botmasterům umožňuje ovládání celé sítě na dálku a skrytí komunikačního provozu. Infikovaná zařízení se připojují k předem určenému serveru, na kterém čekají na instrukce od botmastera. Tento botmaster instrukce odesílá na server, odkud jsou distribuovány klientům k provedení. Po dokončení úkolů klienti odesílají výsledky zpět botmasterovi. Alternativním modelem je peer-to-peer síť, kde není vyžadován centrální server pro komunikaci, což eliminuje běžný bod selhání při botnetových útocích. V tomto modelu každý bot funguje jako server pro rozšiřování příkazů, tak jako klient přijímající instrukce, což zvyšuje odolnost sítě proti vypnutí. (53)

DoS a DDoS:

Při útocích typu denial-of-service (DoS) dochází k zaplavení serveru nadměrným provozem, což má za následek nedostupnost webové stránky nebo jiného zdroje. Distribuovaný útok typu denial-of-service představuje DoS útok, kde je k zaplavení cílového zdroje využito rozsáhlé sítě počítačů nebo zařízení. Cílem obou typů útoků je přetížení serveru nebo webové aplikace za účelem narušení poskytovaných služeb.

V důsledku přetížení serveru větším objemem paketů z TCP nebo UDP, než je schopen efektivně zpracovat, může docházet k jeho selhání. To může vést k poškození dat, nesprávnému směrování zdrojů nebo jejich úplnému vyčerpání, což v konečném důsledku paralyzuje systém.

Existuje několik druhů útoků DoS, patří mezi ně útoky typu flooding nebo útoky na aplikační vrstvu. Útok typu flooding je DoS útok, při kterém jsou odesílány několikanásobné požadavky na spojení k serveru, ale následně nedochází k dokončení handshaku. Útok na aplikační vrstvu je druh DDoS útoku, který se zaměřuje na vrstvu 7 modelu OSI. Příkladem může být útok Slowloris, při němž útočník odesílá neúplné požadavky HTTP, ale nedokončí je. Pro každý požadavek jsou pravidelně odesílány HTTP hlavičky, což vede k zablokování síťových zdrojů. (54) (55) (56) (57)

3.3.2 Slabiny v zabezpečení mesh IoT sítí

Slabá hesla:

Slabá hesla představují pro útočníky nejjednodušší cestu ke kompromitaci IoT zařízení a k zahájení rozsáhlých botnetů a dalšího malware. Správa hesel v distribuovaném ekosystému IoT je časově náročná a obtížná povinnost, obzvláště když jsou IoT zařízení spravována bezdrátově.

Nezabezpečené síťové služby:

Útočníci se snaží zneužít nedostatky v komunikačních protokolech a službách, které běží na IoT zařízeních, s cílem nabourat se k citlivým nebo utajovaným datům přenášeným

mezi zařízením a serverem. Cílem útoků Man-in-the-Middle je využít těchto zranitelností k získání přístupových údajů, které jsou použity pro ověření pravosti koncových bodů, a následně tyto údaje použít pro provedení rozsáhlejších útoků. Z toho důvodu je klíčové chránit komunikaci IoT zařízení pomocí osvědčených postupů daného průmyslu.

Zastaralé komponenty:

Bezpečnost ekosystému IoT může být ohrožena zranitelnostmi v softwarových závislostech nebo zastaralých systémech. Využívání open-source komponent výrobci pro konstrukci jejich IoT zařízení vytváří složitý dodavatelský řetězec, který je obtížné sledovat. Tyto komponenty mohou zdědit zranitelnosti, které jsou útočníkům známé, čímž vzniká rozšířená hrozba, jež čeká na své využití. (58) (59)

Nekvalitní IoT zařízení:

Některá IoT zařízení jsou čím dál tím více rozpoznávána jako nebezpečná, a to ne kvůli jejich designu, ale kvůli nedostatkům ve výrobě. CISA, americká agentura pro kybernetickou ochranu, již upozornila na závažné bezpečnostní nedostatky v zařízeních s GPS vyrobených v Asii, které se používají v automobilech a motocyklech. Tyto přístroje obsahují přednastavená administrátorská hesla a další chyby, které by umožňují výrobcům vzdáleně sledovat polohu těchto zařízení a dokonce potenciálně přerušit dodávku paliva, když jsou vozidla v pohybu. (60)

3.3.3 Důsledky nedostatečného zabezpečení v mesh sítích

Únik dat:

Při získání přístupu k IoT síti mohou být citlivé informace, jako jsou osobní data, finanční záznamy nebo vizuální materiály zabezpečovacích kamer, odhaleny útočníkem. Tato kompromitace soukromí může mít za následek finanční ztráty pro jednotlivce, stejně jako psychologické dopady způsobené zneužitím osobních informací.

Škoda na infrastruktuře:

V případě, že jsou IoT zařízení integrována do systémů kritické infrastruktury, útočníkův přístup může vést k výpadkům služeb nebo manipulaci s funkcemi zařízení. To může mít za následek fyzické škody nebo dokonce ohrožení lidských životů, například pokud jsou zasaženy energetické sítě nebo systémy zdravotnické péče. Botnet Mirai v říjnu 2016 použil síť infikovaných IoT zařízení, včetně digitálních kamer a DVR přehrávačů, k provedení masivního DDoS útoku na poskytovatele služeb správy výkonu internetu Dyn, což vedlo k výpadku několika velkých webových stránek, jako jsou CNN, Netflix a Twitter.

Zneužití zařízení:

Zařízení IoT mohou být útočníkem zneužita pro různé účely, včetně zvýšení spotřeby energie nebo neoprávněného přístupu. Hack Jeep v červenci 2015, kdy skupina výzkumníků demonstrovala, jak mohou ovládat SUV Jeep prostřednictvím mobilní sítě Sprint využitím zranitelnosti při aktualizaci firmwaru. Útočníci mohli ovlivnit rychlost vozidla a dokonce ho vyvést z cesty, což poukazuje na riziko zneužití zařízení.

Narušení operací:

Kompromitace IoT zařízení může zasáhnout do běžných operací a procesů v organizaci, což vede k ztrátě produktivity a potenciálně i k finančním ztrátám. Zpomalení nebo přerušení služeb může mít vliv na schopnost organizace plnit své povinnosti a sliby vůči zákazníkům. (61)

4 Vlastní práce

Praktická část je zaměřena na konkrétní analýzu a hodnocení bezpečnosti těchto sítí. Hlavním cílem této praktické části je zhodnotit stávající zabezpečení mesh IoT sítí a provést porovnání mezi vybranými technologiemi.

Budou představeny následující kroky:

Výběr konkrétních technologií mesh IoT sítí pro analýzu:

Pro úspěšnou realizaci analýzy je klíčovým prvním krokem výběr konkrétních technologií mesh IoT sítí, které budou předmětem studie. Tento výběr vyžaduje zvážení relevantnosti a aktuálnosti každé technologie v rámci současného prostředí internetu věcí. Zohledníme faktory, jako je rozšířenost používání, kompatibilita, a přínos pro oblast zabezpečení.

Definice kritérií, které budeme používat k hodnocení bezpečnosti těchto technologií:

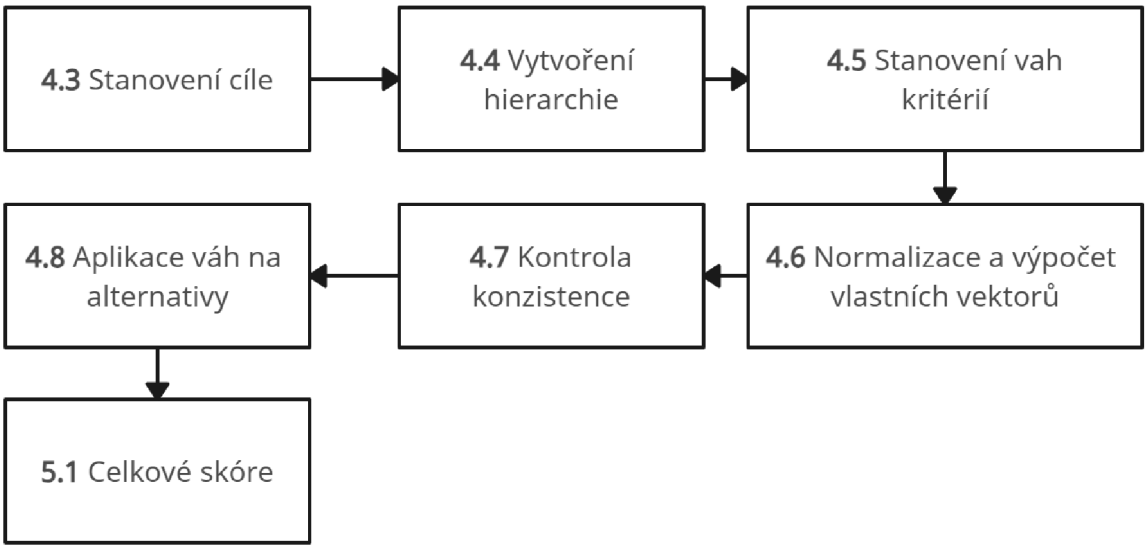
Kritéria pro hodnocení bezpečnosti technologií budou klíčovým prvkem Saatyho metody vícekriteriální analýzy. Stanovíme specifická kritéria, která zahrnou aspekty jako autentizace, šifrování dat, odolnost vůči různým typům útoků, a další bezpečnostní faktory. Každé kritérium bude definováno a váženo podle jeho významu v kontextu bezpečnosti sítí IoT.

Aplikace vícekriteriální analýzy a srovnání bezpečnosti technologie Zigbee s dalšími technologiemi:

Tato fáze práce bude zaměřena úsilí na porovnání technologie Zigbee s dalšími relevantními technologiemi v rámci IoT. Za účelem dosažení tohoto cíle bude využita Saatyho metoda vícekriteriální analýzy na vybrané technologie s důrazem na jejich bezpečnostní aspekty. Vícekriteriální analýza bude prováděna na základě předem stanovených kritérií. Hodnoty jednotlivých kritérií pro každou technologii budou kvantifikovány s cílem poskytnout objektivní a komplexní pohled na bezpečnostní úroveň každé z nich. V přiřazování vah k jednotlivým kritériím použijeme Saatyho metodu. Touto metodou bude umožněno strukturované a systematické hodnocení, což v konečném důsledku povede ke komparativní analýze bezpečnosti mezi Zigbee a ostatními technologiemi. Tímto metodologickým přístupem viz obrázek 7 bude zajištěno systematické a objektivní hodnocení bezpečnosti technologie Zigbee ve srovnání s ostatními relevantními technologiemi v oblasti IoT. (62)

Identifikace nedostatků a navrhnutí možných opatření pro zvýšení bezpečnosti:
Na základě výsledků analýzy bude možné identifikovat konkrétní nedostatky v bezpečnosti každé technologie. Tato identifikace bude sloužit jako výchozí bod pro navržení konkrétních opatření a doporučení, která mohou být implementována k zvýšení celkové bezpečnosti technologií.

Obrázek 7 schéma postupu Saatyho metody vícekriteriální analýzy



Zdroj: vlastní zpracování

4.1 Výběr konkrétních technologií mesh IoT sítí pro analýzu

Jedním z hlavních kritérií výběru byl významný podíl těchto technologií na trhu. Technologie Zigbee byla vybrána kvůli jejímu tržnímu objemu, který v roce 2023 dosáhl 4,59 miliardy USD, a jejímu složenému ročnímu růstu, odhadovanému mezi 6 a 9 % podle různých studií. Bluetooth Mesh byl zvolen z podobných důvodů, s tržním objemem 4,1 miliardy USD v roce 2022 a CAGR kolem 11 %. (63) (64)

Výběr české technologie IQRF pak přispěl k různorodosti a specifičnosti analýzy. IQRF, jako zástupce na českém trhu IoT, měl v roce 2022 obrat 9 944 tis. Kč. Začleněním této méně známé, ale významné technologie se práce snaží poskytnout širší pohled na dynamický a rychle se rozvíjející trh IoT. Tento diverzifikovaný výběr technologií umožňuje práci hlouběji zkoumat různé aspekty a trendy v oblasti IoT, zatímco poskytuje konkrétní příklady z významných segmentů trhu. (65)

Zdůvodnění výběru těchto technologií, včetně jejich relevance pro současný kontext IoT a zabezpečení:

Každá z vybraných technologií byla vybrána na základě jejich širokého využití, relevance v současném kontextu IoT a specifických aspektů zabezpečení, které nabízejí.

Zigbee: Zařazení technologie Zigbee do analýzy bylo motivováno jeho rozšířeností a častým využitím v průmyslových a domácích prostředích. Tato technologie se dlouhodobě etablovala v průmyslových a výrobních odvětvích, kde je považována za spolehlivou volbu pro rozsáhlé IoT sítě. Díky své historii a osvědčenému výkonu je Zigbee klíčovým příkladem technologie schopné zvládnout náročné podmínky průmyslového prostředí. Jedním z klíčových důvodů pro výběr Zigbee byla také jeho schopnost poskytovat stabilní a spolehlivou komunikaci, což je nezbytné pro kritické aplikace v rámci IoT, jako jsou automatizované průmyslové procesy. Tato schopnost je zásadní pro zajištění kontinuity a bezpečnosti v dynamických a náročných prostředích IoT.

IQRF: V případě IQRF byla volba zdůvodněna jeho flexibilitou a škálovatelností mesh topologie. IQRF se vyznačuje adaptabilitou, která umožňuje efektivní implementaci v různých prostředích IoT, od malých domácích sítí až po rozsáhlé průmyslové aplikace. Jeho schopnost přizpůsobit se sítím s proměnným počtem zařízení a dynamicky se měnícím prostředím je zásadní pro efektivní využití v různorodých IoT aplikacích. IQRF rovněž přináší inovativní bezpečnostní prvky, které jsou klíčové pro ochranu dat a zabezpečení v prostředích, kde je bezpečnost kritickým faktorem pro úspěšnou implementaci IoT sítí. Tato schopnost poskytovat vysoce bezpečné řešení je nezbytná vzhledem k narůstajícím hrozbám v oblasti kybernetické bezpečnosti v IoT.

Bluetooth Mesh: Zahrnutí technologie Bluetooth Mesh do studie je motivováno jejím rostoucím přijetím v oblasti IoT a schopností rozšířit tradiční Bluetooth o mesh síťování. Tato technologie přináší nové možnosti pro IoT aplikace, zejména v kontextu smart home a průmyslových aplikací. Bluetooth Mesh se zaměřuje na poskytování robustních a bezpečných mesh sítí, které jsou klíčové pro distribuci a správu dat v IoT prostředích. Jeho schopnost poskytovat spolehlivé a zabezpečené komunikační schopnosti v mesh topologii přináší důležitý pohled na výzvy a řešení spojené s bezpečností v IoT.

Výběr těchto tří technologií reflektuje rozmanitost a komplexnost současného IoT prostředí. Každá z nich představuje jiný přístup k vytváření a zabezpečení mesh sítí, což je klíčové pro pochopení široké škály výzev a řešení v oblasti zabezpečení IoT. Tato diverzita

umožňuje komplexní přehled o tom, jak různé technologie řeší bezpečnostní hrozby a jaký dopad mají tyto řešení na praktické nasazení v reálných scénářích IoT.

4.2 Definice kritérií

Přehled kritérií:

Úroveň šifrování:

Toto kritérium se zaměřuje na typ a sílu šifrovacích algoritmů, které jsou používány v dané technologii. Zahrnuje posouzení používaných šifrovacích standardů, jejich robustnosti a odolnosti vůči pokročilým dešifrovacím technikám.

Kvantitativní hodnocení úrovně šifrování je klíčové pro určení, jak dobře jsou data chráněna během přenosu v síti. Toto hodnocení poskytuje objektivní základ pro porovnání bezpečnosti dat přenášených mezi různými technologiemi, umožňuje identifikovat potenciální slabiny v ochraně dat a poskytuje směr pro zlepšení zabezpečení.

Mechanismy autentizace:

Toto kritérium se věnuje analýze typů a složitosti mechanismů autentizace, které technologie využívají. Zahrnuje hodnocení různých metod ověřování identity uživatelů a zařízení, jako jsou hesla, digitální certifikáty, biometrická data nebo multifaktorová autentizace.

Mechanismy autentizace jsou zásadní pro zajištění, že přístup k síti a k datům mají pouze oprávněné entity. Kvantitativní srovnání těchto mechanismů poskytuje cenné informace o tom, jak efektivně technologie chrání proti neautorizovanému přístupu a jakým hrozbám může být vystavena.

Odolnost vůči útokům:

Toto kritérium hodnotí míru odolnosti technologie vůči běžným typům kybernetických útoků, jako jsou DoS, Man-in-the-Middle, replay útoky a další.

Odolnost vůči útokům je klíčová pro zachování funkčnosti a bezpečnosti sítě. Toto kritérium poskytuje kvantifikovatelný základ pro srovnání, jak dobře jsou jednotlivé technologie připraveny čelit těmto hrozbám, což je nezbytné pro vytvoření robustních a odolných síťových řešení.

Aktualizace bezpečnostních protokolů:

Zde se hodnotí frekvence a rozsah, s jakým technologie aktualizují své bezpečnostní protokoly a software.

Schopnost pravidelně aktualizovat a adaptovat bezpečnostní protokoly je zásadní pro reakci na nově vznikající hrozby a zranitelnosti. Toto kritérium umožňuje kvantitativní hodnocení schopnosti technologie udržet krok s neustále se měnícím bezpečnostním prostředím, což je nezbytné pro dlouhodobou ochranu sítě.

Dodržování bezpečnostních standardů:

Toto kritérium se zaměřuje na míru, do jaké technologie splňuje mezinárodní bezpečnostní standardy a získává příslušné certifikace.

Dodržování bezpečnostních standardů a získání certifikací poskytuje důležitý ukazatel kvality a spolehlivosti bezpečnostních prvků technologie. Toto kritérium umožňuje kvantifikovat a srovnat, do jaké míry se technologie řídí osvědčenými postupy a normami v oblasti bezpečnosti, což je klíčové pro zajištění důvěry a spolehlivosti v IoT prostředí.

4.3 Stanovení cíle

Byl stanoven cíl, který určuje směr a rozsah analýzy. Jeho stanovení je nezbytné pro zaměření výzkumu a poskytuje jasný rámec pro posouzení a porovnání alternativ.

Pro Saatyho metodu byl definován následující cíl: „Určit nejbezpečnější mesh IoT síť“. Tento cíl byl zvolen vzhledem k rostoucí důležitosti bezpečnosti v oblasti internetu věcí, kde mesh sítě hrají klíčovou roli. V kontextu IoT je bezpečnost považována za kritický faktor, protože rizika spojená s nebezpečnými síťovými řešeními mohou mít vážné následky, od narušení soukromí až po ohrožení fyzické bezpečnosti.

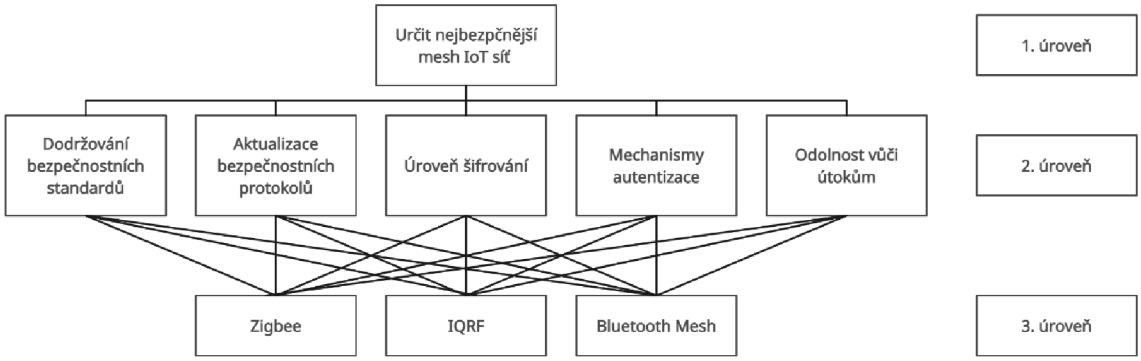
4.4 Vytvoření hierarchie pro porovnání bezpečnosti mesh IoT sítí

V této části práce aplikujeme metodu Analytického Hierarchického Procesu (AHP) pro objektivní a strukturované porovnání tří významných bezdrátových komunikačních technologií: Zigbee, IQRF a Bluetooth Mesh. Naším cílem je identifikovat, která z těchto technologií nejlépe vyhovuje stanoveným kritériím.

Hierarchie AHP pro tento výzkum je rozdělena do tří úrovní viz obrázek 8:

1. úroveň: Cíl
2. úroveň: Kritéria pro hodnocení
3. úroveň: Varianty

Obrázek 8 hierarchie AHP



Zdroj: vlastní zpracování

4.5 Stanovení vah kritérií

Cílem tohoto procesu je stanovení relativní důležitosti jednotlivých kritérií, která jsou použita pro hodnocení a porovnání technologických alternativ v oblasti bezpečnosti mesh IoT sítí. Proces je zásadní pro zajištění, že analýza odráží přesné priority a potřeby v kontextu hodnocení bezpečnostních aspektů zvolených technologií.

Postup pro hodnocení:

Vytvoření matice porovnání: Nejdříve byla vytvořena matice porovnání, v níž každé kritérium zastupuje jak řádek, tak sloupec. Tato matice slouží jako základ pro následné porovnávání a hodnocení významu jednotlivých kritérií.

Použití Saatyho škály: Pro hodnocení významu každého kritéria vzhledem k ostatním byla použita Saatyho škála, která se pohybuje od 1 (stejná důležitost) až po 9 (extrémní důležitost)

viz tabulka 1. Tato škála umožňuje kvantitativní vyjádření stupně, do jakého je jedno kritérium považováno za důležitější než jiné.

Tabulka 1 Saatyho škála

1	rovnocenná kritéria i a j
3	slabě preferované kritérium i před j
5	silně preferované kritérium i před j
7	velmi silně preferované kritérium i před j
9	absolutně preferované kritérium i před j

Zdroj: vlastní zpracování

Příklad hodnocení: Jako příklad, v analýze bylo kritérium „Úroveň šifrování“ hodnoceno jako slabě preferováno než „Odolnost vůči útokům“. Na základě literatury byla tomuto páru kritérií přiřazena hodnota 3 na Saatyho škále, což naznačuje, že úroveň šifrování je považována za relativně důležitější.

Konzistence hodnocení: Důraz byl kladen také na konzistenci v hodnocení. Saatyho metoda poskytuje mechanismus pro kontrolu konzistence hodnocení, což je klíčové pro zajištění spolehlivosti a validnosti výsledků analýzy.

Výsledky tohoto hodnocení viz tabulka 2 hrají zásadní roli ve výpočtu vah pro každé kritérium, které následně ovlivňují celkovou analýzu a výběr mezi technologickými alternativami. Správné a pečlivé hodnocení kritérií je tak nezbytným krokem pro zajištění objektivity a přesnosti vícekriteriální analýzy.

Tabulka 2 výsledná tabulka po provedení stanovení vah

	Úroveň šifrování	Mechanismy autentizace	Odolnost vůči útokům	Aktualizace bezpečnostních protokolů	Dodržování bezpečnostních standardů
Úroveň šifrování	1	1	3	5	9
Mechanismy autentizace	1	1	2	5	9
Odolnost vůči útokům	0,33333	0,33333	1	3	5
Aktualizace bezpečnostních protokolů	0,2	0,2	0,33333	1	3
Dodržování bezpečnostních standardů	0,11111	0,11111	0,2	0,33333	1

Zdroj: vlastní zpracování

4.6 Normalizace a výpočet vlastních vektorů

V této části je popsán proces, během kterého byla normalizována matice porovnání a byly vypočítány vlastní vektory s využitím geometrického průměru pro stanovení vah preferencí. Tento krok je nezbytný pro transformaci subjektivních hodnocení významu kritérií na kvantitativní váhy, které jsou klíčové pro další fáze vícekriteriální analýzy.

Normalizace vektorů za pomoci geometrického průměru:

Výpočet geometrického průměru: Pro každý řádek matice porovnání byl vypočítán geometrický průměr. Geometrický průměr byl zvolen z důvodu jeho schopnosti efektivně shrnout množství hodnocení v jednom řádku a redukovat vliv extrémních hodnot. Proces výpočtu zahrnoval násobení všech hodnot v řádku a následné odmocnění výsledku n-tou odmocninou, kde n je počet kritérií.

Normalizace vektorů: Po výpočtu geometrického průměru pro každý řádek byly tyto průměry normalizovány. Normalizace byla provedena vydělením každého geometrického průměru

součtem všech geometrických průměrů. Takto byly získány normalizované váhy preferencí pro každé kritérium.

Výsledné normalizované váhy viz tabulka 3 reprezentují relativní význam každého kritéria v rámci celkového hodnocení. Tyto váhy jsou klíčové pro další analýzu, neboť určují, jaký důraz je kladen na jednotlivá kritéria při hodnocení a porovnání technologických alternativ.

Tabulka 3 normalizovaná tabulka s váhami

	Geometrický průměr	Váha (preference)
Úroveň šifrování	2,6673	0,370
Mechanismy autentizace	2,6673	0,370
Odolnost vůči útokům	1,1076	0,154
Aktualizace bezpečnostních protokolů	0,5253	0,073
Dodržování bezpečnostních standardů	0,2416	0,034
Součet	7,2090	1,000

Zdroj: vlastní zpracování

4.7 Kontrola konzistence

Pro potvrzení konzistence hodnocení v rámci procesu vícekriteriálního rozhodování byla provedena kontrola konzistence pomocí nástroje Citlivostní analýza, konkrétně funkce „Hledání řešení“ (Goal Seek) v aplikaci Microsoft Excel. Tento přístup umožnil automaticky upravit hodnoty v matici porovnání tak, aby výsledná maximální vlastní hodnota (lambda) byla co nejblíže velikosti matice, což je indikátorem konzistence hodnocení.

Použití Citlivostní Analýzy:

Nastavení cílové hodnoty: Do funkce „Cílová hodnota“ byl zadán požadavek na nalezení takové hodnoty v matici, při které bude determinant matice co nejbližší nule, což je podmínka konzistence.

Výsledek citlivostní analýzy: Procesem hledání řešení byl determinant matice upraven na hodnotu -0,0001615 a maximální vlastní hodnota (lambda) dosáhla hodnoty 5,084. Tento výsledek naznačuje, že matice je dostatečně konzistentní a že subjektivní hodnocení významu kritérií může být považováno za spolehlivé.

Zjištěná hodnota lambda a hodnota determinantu signalizují, že hodnocení kritérií v matici porovnání jsou v souladu s požadavky na konzistentní rozhodovací matrici. Tento výsledek potvrzuje, že zvolený přístup může být použit pro výpočet vah kritérií.

4.8 Aplikace vah na alternativy

Proces aplikace vah na alternativy byl proveden s využitím geometrického průměru pro určení dílčích vah a následného výpočtu vážených dílčích vah jednotlivých alternativ. Tento krok umožňuje kvantitativní porovnání alternativ na základě kritérií definovaných v rámci hodnotícího modelu. Kontrola konzistence byla zajištěna prostřednictvím funkce „Hledání řešení“ v aplikaci Microsoft Excel, což zajistilo uspořádanost mezi výpočty a stanovenými preferencemi.

Výpočet dílčích a vážených dílčích vah:

Stanovení geometrického průměru: Pro každou alternativu byl vypočítán geometrický průměr hodnocení přiřazených dle literatury. Tento průměr byl použit pro stanovení dílčích vah, které odrážejí relativní přednost dané alternativy ve vztahu k ostatním.

Aplikace dílčích vah: Na základě dílčích vah byly pro každou alternativu vypočítány vážené dílčí váhy. Tento výpočet byl proveden vynásobením dílčích vah příslušnými váhami kritérií, které byly získány v předchozím kroku vícekriteriální analýzy.

Kontrola konzistence: Během výpočtů byla konzistence kontrolována funkcí Citlivostní analýza – hledání řešení. Tato funkce byla aplikována s cílem zajistit, že dílčí váhy jsou uspořádané a odpovídají výslednému hodnocení významu kritérií. Výsledky viz tabulka 4 dokazují, že matice jsou dostatečně konzistentní.

Tabulka 4 kontrola konzistence jednotlivých variant

	Λ (vlastní hodnota)	Determinant
Úroveň šifrování	3	-0,000182254
Mechanismy autentizace	3	-0,000182254
Odolnost vůči útokům	3,039	-0,000118096
Aktualizace bezpečnostních protokolů	3,029	-0,00013147
Dodržování bezpečnostních standardů	3,039	-0,000118096

Zdroj: vlastní zpracování

Z výpočtů viz tabulka 5, 6, 7, 8 a 9 vyplynuly vážené dílčí váhy pro každou alternativu, které jsou zásadní pro jejich vzájemné porovnání a pro finální výběr nejvhodnější alternativy.

Tabulka 5 výpočet vážených dílčích vah u úrovně šifrování

Úroveň šifrování	Zigbee	IQRF	Bluetooth Mesh	Geometrický průměr	Dílčí váhy	Vážené dílčí váhy
Zigbee	1	1	3	1,442	0,429	0,159
IQRF	1	1	3	1,442	0,429	0,159
Bluetooth Mesh	0,333	0,333	1	0,481	0,143	0,053

Zdroj: vlastní zpracování

Tabulka 6 výpočet vážených dílčích vah u mechanismů autentizace

Mechanismy autentizace	Zigbee	IQRF	Bluetooth Mesh	Geometrický průměr	Dílčí váhy	Vážené dílčí váhy
Zigbee	1	1	0,333	0,693	0,200	0,074
IQRF	1	1	0,333	0,693	0,200	0,074
Bluetooth Mesh	3	3	1	2,080	0,600	0,222

Zdroj: vlastní zpracování

Tabulka 7 výpočet vážených dílčích vah u odolnosti vůči útokům

Odolnost vůči útokům	Zigbee	IQRF	Bluetooth Mesh	Geometrický průměr	Dílčí váhy	Vážené dílčí váhy
Zigbee	1	3	0,333	1,000	0,258	0,040
IQRF	0,333	1	0,2	0,405	0,105	0,016
Bluetooth Mesh	3	5	1	2,466	0,637	0,098

Zdroj: vlastní zpracování

Tabulka 8 výpočet vážených dílčích vah u aktualizace bezpečnostních protokolů

Aktualizace bezpečnostních protokolů	Zigbee	IQRF	Bluetooth Mesh	Geometrický průměr	Dílčí váhy	Vážené dílčí váhy
Zigbee	1	9	3	3,000	0,672	0,049
IQRF	0,111	1	0,2	0,281	0,063	0,005
Bluetooth Mesh	0,333	5	1	1,186	0,265	0,019

Zdroj: vlastní zpracování

Tabulka 9 výpočet vážených dílčích vah u dodržování bezpečnostních standardů

Dodržování bezpečnostních standardů	Zigbee	IQRF	Bluetooth Mesh	Geometrický průměr	Dílčí váhy	Vážené dílčí váhy
Zigbee	1	5	3	2,466	0,637	0,021
IQRF	0,2	1	0,333	0,405	0,105	0,004
Bluetooth Mesh	0,333	3	1	1,000	0,258	0,009

Zdroj: vlastní zpracování

5 Výsledky a diskuse

5.1 Výsledky vícekriteriální analýzy

Pro stanovení celkového skóre jednotlivých alternativ byly použity vážené dílčí váhy, které vznikly aplikací předem stanovených vah kritérií na hodnocení alternativ. Tento proces výpočtu umožňuje sloučení jednotlivých hodnotících faktorů do jediného ukazatele, který odráží celkovou preferenci nebo výkonnost každé zvažované alternativy.

Tabulka 10 výsledná tabulka se syntézou preferencí a pořadím

	Syntéza preferencí	Pořadí
Zigbee	0,343	2.
IQRF	0,257	3.
Bluetooth Mesh	0,401	1.

Zdroj: vlastní zpracování

Alternativa Bluetooth Mesh byla vyhodnocena jako nejlepší s celkovým skóre 0,401, což ji staví na první místo. Zigbee následuje s celkovým skóre 0,343, umisťujíc se na druhou pozici. Alternativa IQRF obdržela skóre 0,257, což ji řadí na třetí místo.

Je důležité poznamenat, že ačkoliv Saatyho metoda poskytuje strukturovaný a systematický přístup k hodnocení a rozhodování, výsledky jsou v zásadě ovlivněny subjektivním úsudkem autora. Výběr kritérií, jejich relativní váhy a interpretace výsledků jsou formovány individuálním pohledem a preferencemi, což může ovlivnit konečná rozhodnutí.

5.2 Diskuse

Na základě výsledků vícekriteriální analýzy bylo navrženo zlepšení zabezpečení mesh IoT sítí, a to zvýšením frekvence a pravidelnosti aktualizací bezpečnostních protokolů. Bylo zjištěno, že aktualizace bezpečnostních protokolů v současných mesh IoT sítích probíhají nepravidelně a nejsou dostatečně časté, což může vést k nedostatečné obraně proti nově vznikajícím kybernetickým hrozbám a bezpečnostním rizikům.

Důraz byl kladen na zavedení systematického a pravidelného procesu aktualizací, který by zajistil, že bezpečnostní protokoly budou v souladu s nejnovějšími vývojovými trendy a požadavky na kybernetickou bezpečnost.

V této souvislosti byla zdůrazněna důležitost pravidelné revize a aktualizace bezpečnostních protokolů, zahrnující implementaci nových technologických vylepšení

a zajištění kompatibility s nejnovějšími standardy v oblasti IoT. Tyto aktualizace by měly probíhat systematicky a v pravidelných intervalech, aby byla zajištěna stále aktuální ochrana proti hrozbám.

Navíc bylo doporučeno, aby se v rámci procesu aktualizace věnovala pozornost vzdělávání uživatelů a správců sítí o důležitosti a významu bezpečnostních protokolů, včetně školení zaměřených na nejnovější trendy v kybernetické bezpečnosti a nejlepší praktiky pro jejich implementaci v mesh IoT sítích.

Závěrem bylo zdůrazněno, že systematické a pravidelné aktualizace bezpečnostních protokolů jsou nezbytné pro zajištění dlouhodobé bezpečnosti mesh IoT sítí a ochrany před neustále se vyvíjejícími hrozbami. Tyto kroky by měly být považovány za nedílnou součást správy a údržby mesh IoT sítí, aby bylo zajištěno jejich bezpečné a efektivní fungování.

Identifikace hlavních hrozeb a slabin mesh Iot sítí:

Bezpečnostní chyby jsou považovány za značnou slabinu těchto sítí. Vzhledem k různým úrovním zabezpečení a rozmanitosti zařízení v mesh IoT sítích je snadné vniknout do těchto systémů pomocí slabých hesel, zastaralého softwaru nebo nezabezpečených komunikačních kanálů. Tyto zranitelnosti mohou být zneužity útočníky k neoprávněnému přístupu nebo šíření malwaru. Různé úrovně zabezpečení mezi zařízeními v síti mohou vést k vytvoření bezpečnostních mezer, což je zvláště problematické v případě, že jsou napadeny klíčové systémové funkce nebo citlivá data.

Problematika škálovatelnosti a výkonu je také často zdůrazňována. Se zvyšujícím se počtem zařízení v síti narůstá náročnost na koordinaci, komunikaci mezi těmito zařízeními a zabezpečením všech těchto zařízení. Bylo zjištěno, že to může vést k zpomalení a snížení efektivity systému, zejména když je nutné přidávat nová zařízení nebo upravovat síťovou infrastrukturu, dle analytických reportů z prvního kvartálu roku 2023 počet koncových zařízení narostlo o 18 % na 14,4 miliardy koncových IoT zařízení. V roce 2023 byl očekáván růst 16 % na 16,7 miliardy koncových zařízení. (66)

Nedostatečná správa a aktualizace softwaru a hardwaru jsou rovněž považovány za významné slabiny. Systémy, které nejsou pravidelně aktualizovány, jsou náchylné k bezpečnostním hrozbám. Nedostatečná správa také může vést k tomu, že systémy nejsou optimálně konfigurovány nebo obsahují zastaralé komponenty, což zvyšuje riziko bezpečnostních incidentů.

Fyzická zranitelnost IoT zařízení je často zmiňována jako kritická slabost. Zařízení umístěná v méně zabezpečených prostředích jsou náchylná k poškození, krádeži nebo

manipulaci, což je obzvláště problematické v případě, že zařízení shromažďují nebo zpracovávají citlivá data.

Energetická efektivnost je klíčovým aspektem, zejména vzhledem k tomu, že mnoho IoT zařízení je napájeno bateriemi. Efektivní správa energie je nezbytná pro udržení dlouhodobého provozu zařízení, přičemž vysoká spotřeba energie může omezit jejich funkčnost a spolehlivost.

Co se týče hrozeb, fyzický přístup k zařízením je považován za značné bezpečnostní riziko. Je zaznamenáno, že útočníci mají možnost provádět různé škodlivé aktivity v případě, že získají fyzický přístup k zařízením. Toto riziko je obzvláště závažné v prostředích, kde jsou zařízení veřejně přístupná nebo nedostatečně zabezpečená. V případě fyzických útoků na IoT mesh sítě je možné, že do zařízení bude nainstalován malware nebo škodlivý software útočníkem, což umožňuje dálkovou kontrolu zařízení, shromažďování dat a provádění škodlivých aktivit v síti. Fyzická manipulace nebo sabotáž zařízení mohou být také provedeny, což by narušilo jejich funkčnost. Provádění úprav na hardwarové úrovni by mohlo vést k nesprávnému fungování zařízení nebo jejich zneužití. Únos zařízení, při kterém je získána kontrola nad zařízením a využito jej k provádění neautorizovaných akcí, jako je odesílání falešných dat nebo útoky na další zařízení v síti, může být rovněž realizován. Při fyzickém přístupu k zařízení může dojít k extrakci uložených dat, včetně osobních informací, přihlašovacích údajů nebo jiných citlivých dat. Toto může vést k závažným následkům, jako je krádež identity nebo neoprávněné použití informací.

Útoky typu Man-in-the-Middle jsou identifikovány jako další hrozba pro tyto sítě. Během těchto útoků může dojít k odposlechu nebo manipulaci s komunikací mezi zařízeními, což může vést k ztrátě citlivých informací nebo narušení funkčnosti sítě. Bezpečná komunikace a autentizace jsou klíčové pro ochranu proti těmto útokům.

DoS a DDoS útoky jsou uznávány jako běžné hrozby pro mesh IoT sítě. Tyto útoky, které zahrnují záměrné přetížení sítě, mohou znemožnit normální provoz a komunikaci mezi zařízeními, omezujíce tak funkčnost sítě.

Botnety, tedy sítě kompromitovaných zařízení, jsou také identifikovány jako značná hrozba. Tyto sítě mohou být použity pro řadu škodlivých aktivit, včetně šíření malware a provádění DDoS útoků. Bylo zaznamenáno, že počet IoT zařízení (botů) zapojených do DDoS útoků řízených botnety se zvýšil z přibližně 200 000 před rokem na zhruba 1 milion zařízení, která dnes generují více než 40 % veškerého DDoS provozu. (67)

Tyto hrozby a slabiny ukazují na významné výzvy, které stojí před mesh IoT sítěmi. Je zásadní, aby byly tyto problémy řešeny s maximální prioritou, což zahrnuje implementaci robustních bezpečnostních protokolů, pravidelné aktualizace a pečlivou správu sítě, aby byla zajištěna jejich bezpečnost a spolehlivost.

6 Závěr

Tato bakalářská práce se zabývala tématikou zabezpečení mesh IoT sítí, s hlavním cílem zhodnotit technologie používané v mesh IoT sítích. Předmětem bylo posouzení různých aspektů zabezpečení, včetně identifikace slabých míst a potenciálních hrozeb, které tyto sítě mohou ohrožovat. Cílem bylo poskytnout ucelený pohled na stav zabezpečení v oblasti mesh IoT sítí a nabídnout doporučení pro jejich zlepšení.

V teoretické části byly popsány základní principy mesh IoT sítí, architektura a jejich typické využití. Kromě charakteristiky těchto sítí byla pozornost věnována také popisu bezpečnostních prvků, které jsou zásadní pro ochranu sítí a udržení integrity a důvěrnosti přenášených dat. Tento popis poskytuje pevný základ pro pochopení bezpečnostního kontextu mesh IoT sítí a představuje důležitý krok k identifikaci potřebných zlepšení a opatření pro zvýšení celkové bezpečnosti.

Praktická část práce byla zaměřena na hodnocení síťových protokolů používaných v mesh IoT sítích na základě vybraných kritérií s využitím Saatyho metody vícekriteriální analýzy. Byly hodnoceny technologie Zigbee, IQRF a Bluetooth Mesh. Součástí praktické části byla také identifikace slabin a hrozeb, kterým mesh IoT sítě čelí. Mezi tyto slabiny patří chyby uživatelů a administrátorů, které často vedou k nevhodné konfiguraci systémů a jejich zranitelnosti vůči útokům, problematika škálovatelnosti, používání nekvalitních IoT zařízení s nedostatečnými bezpečnostními funkcemi. Mezi největší hrozby byly zařazeny typy útoků, jako jsou Man-in-the-Middle, DoS a DDoS útoky, a využití botnetů.

Výsledky práce ukázaly, že ačkoliv technologie Zigbee, IQRF a Bluetooth Mesh dosahují v kontextu vybraných kritérií podobných úrovní zabezpečení, Bluetooth Mesh byla hodnocena jako nejbezpečnější volba. Toto zjištění poukazuje na význam správného výběru a konfigurace technologií pro zajištění optimálního zabezpečení mesh IoT sítí. Kromě toho bylo v práci navrženo opatření pro zvýšení bezpečnosti, které zahrnuje častější aktualizace bezpečnostních protokolů a lepší proškolení uživatelů a administrátorů. Tyto kroky jsou klíčové pro minimalizaci rizik spojených s chybami v konfiguraci a používání sítí.

7 Seznam použitých zdrojů

1. MALLICK, Chiradeep Basu. What Is a Mesh Network? Meaning, Types Working, and Applications in 2022. *Spiceworks* [online]. 2022-08-12. [cit: 2023-12-18]. Dostupné z: https://www.spiceworks.com/tech/networking/articles/what-is-mesh-network/.

2. KHATIB, Mutamed. *Wireless Mesh Networks - Security, Architectures and Protocols.* Tulkarm : IntechOpen, 2020. 180 s. ISBN 978-1-78985-485-5.

3. DAVOLI, Luca a FERRARI, Gianluigi. *Wireless Mesh Networks for IoT and Smart Cities : Technologies and Applications.* Stevenage : Institution of Engineering & Technology, 2022. 289 s. ISBN 978-1-83953-283-2.

4. GILLIS, Alexander. What is the internet of things (IoT)? *TechTarget* [online]. 2023. [cit: 2023-12-18]. Dostupné z: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT.

5. WZOREK, Mariusz, BERGER, Cyrille a DOHERTY, Patrick. Router and gateway node placement in wireless mesh networks for emergency rescue scenarios. Springer. [online]. (PDF). 2021-12-02. [cit: 2023-12-18]. Dostupné z: https://link.springer.com/article/10.1007/s43684-021-00012-0.

6. GILLIS, Alexander. mesh network topology (mesh network). *TechTarget.* [online]. 2021. [cit: 2023-12-18]. Dostupné z: https://www.techtarget.com/iotagenda/definition/mesh-network-topology-mesh-network.

7. Thingsquare. 5 Reasons to Use IoT Mesh Networks. *IoT For All. Thingsquare* [online]. 2024. [cit: 2023-12-19]. Dostupné z: https://www.iotforall.com/5-reasons-to-use-iot-mesh-networks.

8. NURLAN, Zhanserik, a kol. Wireless Sensor Network as a Mesh: Vision and Challenges. *IEEE Access.* [online]. 2022. [cit: 2023-12-19]. Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9656902.

9. Insights. 8 things you should know about wireless mesh networks. *Lumen radio.* [online]. 2020-03-12. [cit: 2023-12-19]. Dostupné z: https://lumenradio.com/stories/8-things-you-should-know-about-wireless-mesh-networks/.

10. GILLIS, Alexander. IoT devices (internet of things devices). *TechTarget.* [online]. 2023. [cit: 2023-12-19]. Dostupné z: https://www.techtarget.com/iotagenda/definition/IoT-device.

11. OLIYNYK, Kostiantyn. Internet of Things in Consumer Electronics Market: Use Cases + Future Prospects. *WebbyLab.* [online]. 2023-11-08. [cit: 2023-12-19]. Dostupné z: https://webbylab.com/blog/iot-in-consumer-electronics-market/.

12. Amantya. Consumer IoT – What it is | Prominent Use Cases. *Amantya.* [online]. 2022-06-07. [cit: 2023-12-19]. Dostupné z: https://www.amantyatech.com/consumer-iot-what-it-is-prominent-use-cases.
13. Mordor Intelligence. Consumer IoT Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029) [online]. 2023. [cit: 2023-12-19]. Dostupné z: https://www.mordorintelligence.com/industry-reports/consumer-iot-market.
14. VIGDERMAN, Aliza a TURNER, Gabe. What Is Home Automation and How Does It Work? *security.org.* [online]. 2024-01-30. [cit: 2024-02-12]. Dostupné z: https://www.security.org/home-automation/.
15. IPera. What is Enterprise Internet of Things (IoT)? *IPera.* [online] 2022-12-08. [cit: 2024-02-12]. Dostupné z: https://ipera.ai/what-is-enterprise-internet-of-things-iot/#2_What_is_Enterprise_IoT.
16. Famark. ENTERPRISE INTERNET OF THINGS (ENTERPRISE IOT). *famark.* [online] 2023. [cit: 2024-02-12]. Dostupné z: https://www.famark.com/IoT/enterprise-internet-of-things.htm.
17. Grand View Research. Enterprise IoT Market Size, Share & Trends Analysis Report By Component (Hardware, Software & Solutions, Services), By Enterprise Type (SMEs, Large Enterprise), By Application, By Region, And Segment Forecasts, 2024 - 2030. *Grand View Research.* [online]. 2022. [cit: 2024-02-13]. Dostupné z: https://www.grandviewresearch.com/industry-analysis/enterprise-iot-market-report.
18. LELE, Chitra. *Internet of Things (IoT) A Quick Start Guide: A to Z of IoT Essentials (English Edition).* BPB Publications, 2022. 146 s. ISBN 978-9-38984-586-0.
19. ThingsBoard. Smart office solutions. *ThingsBoard.* [online]. [cit: 2024-02-14]. Dostupné z: https://thingsboard.io/use-cases/smart-office/.
20. NØDSKOV, Nemi. How IoT in Retail Is Changing the Global Retail Industry. *onomondo.* [online]. 2023-01-30. [cit: 2024-02-15].
21. Ordr. A Whole Hospital Approach To Securing Patient Care . *Ordr.* [online]. [cit: 2024-02-15]. Dostupné z: https://ordr.net/solutions/healthcare.
22. GILLIS, Alexander. industrial internet of things (IIoT). *TechTarget.* [online]. 2023. [cit: 2024-02-15]. Dostupné z: https://www.techtarget.com/iotagenda/definition/Industrial-Internet-of-Things-IIoT.
23. CHAKI, Rituparna a ROY, Debdutta Barman. *Security in IoT : The Changing Perspective.* Taylor & Francis Group, 2021. 136 s. ISBN 978-1-00053-129-9.

24. Precedence Research. Industrial IoT Market (By Component: Solution, Services, Platform; By End-Use: Manufacturing, Energy & Power, Oil & Gas, Healthcare, ogistics & Transport, Agriculture, Others) - Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook. *Precedence Research.* [online]. 2023. [cit: 2024-02-17]. Dostupné z: https://www.precedenceresearch.com/industrial-iot-market.
25. NØDSKOV, Nemi. IoT: The Future of Technology in the Automotive Industry. *onomondo.* [online]. 2022-08-12. [cit: 2024-02-17]. Dostupné z: https://onomondo.com/blog/iot-the-future-of-technology-in-the-automotive-industry/.
26. IoT Solutions World Congress. *IoT Solutions Congress.* [online]. [cit: 2024-02-17]. Dostupné z: https://www.iotsworldcongress.com/iot-transforming-the-future-of-agriculture/.
27. ROSENCRANCE, Linda. Zigbee. *TechTarget.* [online]. červen 2017. [cit: 2024-02-17]. Dostupné z: https://www.techtarget.com/iotagenda/definition/ZigBee.
28. Geeks for geeks. Introduction of ZigBee. *Geeks for geeks.* [online]. 2023-02-22. [cit: 2024-02-17]. Dostupné z: https://www.geeksforgeeks.org/introduction-of-zigbee/.
29. Silicon Labs. What is the difference between an end device, a router, and a coordinator? *Silicon Labs.* [online]. 2023-01-23. [cit: 2024-02-18]. Dostupné z: https://community.silabs.com/s/article/what-is-the-difference-between-an-end-device-a-router-and-a-coordinator-do-i?language=en_US#:~:text=In%20ZigBee%2C%20there%20are%20three,network%20in%20the%20first%20place.
30. Mvava. How Many Devices Can Zigbee Support? *Mvava.* [online]. 2022-05-17. [cit: 2024-02-18]. Dostupné z: https://www.mvava.com/blog/188-How-Many-Devices-Can-Zigbee-Support.
31. Connectvity Standard Alliance. Zigbee Direct 1.0. *CSA-IoT.org.* [online] 2023. [cit: 2024-02-18]. Dostupné z: https://csa-iot.org/developer-resource/specifications-download-request/.
32. Bluetooth. General market questions. *Bluetooth.* [online]. [cit: 2024-02-19]. Dostupné z: https://www.bluetooth.com/learn-about-bluetooth/feature-enhancements/mesh/mesh-faq/.
33. Moko Blue. What Is Bluetooth Mesh? *Moko Blue.* [online]. 2021-03-19. [cit: 2024-02-19]. Dostupné z: https://mokoblue.com/what-is-bluetooth-mesh/.
34. SOLOVEV, Andrey a PETROVA, Anna. Bluetooth Mesh: Technology Overview, Examples, Alternatives, and First-Hand Experience. *Integra Sources.* [online]. 2024-02-19. [cit: 2024-02-23]. Dostupné z: https://www.integrasources.com/blog/bluetooth-mesh-network-tutorial/.

35. Silicon Labs. Benchmarking Bluetooth Mesh, Thread, and Zigbee Network Performance. *Silicon Labs.* [online]. [cit: 2024-02-23]. Dostupné z: https://www.silabs.com/wireless/multiprotocol/mesh-performance.

36. IQRF. What is IQRF? *IQRF.* [online]. [cit: 2024-02-25]. https://www.iqrf.org/what-is-iqrf.

37. IQRF. Technology. *IQRF.* [online]. [cit: 2024-02-26]. Dostupné z: https://www.iqrf.co.uk/technology.html.

38. IQRF. Frequently Asked Questions. *IQRF.* [online]. [cit: 2024-02-26]. Dostupné z: https://www.iqrf.org/support/faq.

39. IQRF. IQRF security. *IQRF.* [online]. [cit: 2024-02-26]. Dostupné z: https://www.iqrf.org/technology/security.

40. IEEE. The Importance of IoT Security in a Connected World. *IEEE Innovation at work.* [online]. [cit: 2024-02-27]. Dostupné z: https://innovationatwork.ieee.org/the-importance-of-iot-security-in-a-connected-world/.

41. STOUFFER, Clare. What is encryption? How it works + types of encryption. *Norton.* [online]. 2023-07-18. [cit: 2024-02-28]. Dostupné z: https://us.norton.com/blog/privacy/what-is-encryption.

42. Opentext. What is Encryption? *opentext.* [online]. [cit: 2024-02-28]. Dostupné z: https://www.opentext.com/what-is/encryption.

43. Boston University. Understanding Authentication, Authorization, and Encryption. *BU TechWeb.* [online]. [cit: 2024-02-28]. Dostupné z: https://www.bu.edu/tech/about/security-resources/bestpractice/auth/#:~:text=In%20authentication%2C%20the%20user%20or,%2C%20voice%20recognition%2C%20and%20fingerprints.

44. LORD, Nate. What is Threat Monitoring? *Digital Guardian.* [online]. 2020-09-29. [cit: 2024-02-28]. Dostupné z: https://www.digitalguardian.com/blog/what-threat-monitoring.

45. Rapid7. Threat Detection and Response. *Rapid7.* [online]. [cit: 2024-02-28]. Dostupné z: https://www.rapid7.com/fundamentals/threat-detection/.

46. PrimaSecure. The Importance of Regularly Updating Your Network Security Protocols. *PrimaSecure.* [Online]. 2023-03-02. [cit: 2024-03-01]. Dostupné z: https://primasecure.com/the-importance-of-regularly-updating-your-network-security-protocols/.

47. EUR-Lex. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. *EUR-Lex.* [online] 2016-04-04. [cit: 2024-03-01]. Dostupné z: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

48. CloudFare. What is TLS (Transport Layer Security)? *CloudFare.* [online]. [cit: 2024-03-01]. Dostupné z: https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/.

49. Microsoft. Datagram Transport Layer Security protocol. *Microsfot Learn.* [online]. 2023-02-14. [cit: 2024-03-02]. Dostupné z: https://learn.microsoft.com/cs-cz/windows-server/security/tls/datagram-transport-layer-security-protocol.

50. Mozilla. DTLS (Datagram Transport Layer Security). *Mozilla Developer.* [online]. 2023-06-08. [cit: 2024-03-02]. Dostupné z: https://developer.mozilla.org/en-US/docs/Glossary/DTLS.

51. IoT Security Foundation. Physical Security. *IoT Security Foundation.* [online]. [cit: 2024-03-02]. Dostupné z: https://iotsecurityfoundation.org/best-practice-guide-articles/physical-security/.

52. MALLIK, Avijit. *MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING IN SIMPLE.* Rajshahi, Bangladéš : Rajshahi University of Engineering & Technology, [online]. 2018. [cit: 2024-03-02]. Cyberspace: Jurnal Pendidikan Teknologi Informasi. ISSN 2597-9671. Dostupné z: https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453.

53. Eset. Botnet. *Eset.* [online]. [cit: 2024-03-02]. https://www.eset.com/cz/botnet/.

54. Fortinet. DoS Attack vs. DDoS Attack. *Fortinet.* [online]. [cit: 2024-03-02]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/dos-vs-ddos.

55. OSANAIYE, Opeyemi, CHOO, Kim-Kwang Raymond a DLODLO, Mqhele. *Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework.* Journal of Network and Computer Applications, vol. 67. [online]. [cit: 2024-03-02]. ISSN 1084-8045. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1084804516000023.

56. ANDRADE, Roberto, TELLO-OQUENDO, Luis a ORTIZ, Iván. *Cybersecurity Risk of IoT on Smart Cities.* Springer International Publishing AG, 2021-12-01. ISBN 978-3-03088-524-3.

57. NAYAK, Padmalaya, PAL, Souvik a PENG, Sheng-Lung. *IoT and Analytics for Sensor Networks : Proceedings of ICWSNUCA 2021.* Singapur : Springer Singapore Pte. Limited, 2021-09-12. 224 s. ISBN 978-9-81162-919-8.

58. BAHIRAT, Tanuja. Top 9 IoT Vulnerabilities to Enhance IoT Security in 2023. *G2.* [online]. 2023-06-16. [cit: 2024-03-04]. Dostupné z: https://www.g2.com/articles/iot-vulnerabilities.

59. ARAMPATZIS, Anastasios. Top 10 Vulnerabilities that Make IoT Devices Insecure. *Venafi.* [online]. 2023-06-27. [cit: 2024-03-04]. Dostupné z: https://venafi.com/blog/top-10-vulnerabilities-make-iot-devices-insecure/.

60. DREW, Alexi. Chinese technology in the 'Internet of Things' poses a new threat to the west. *Financial Times.* [online]. 2022-08-10. [cit: 2024-03-04]. Dostupné z: https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117.

61. Cyber Management Alliance. IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities. *Cyber Management Alliance.* [online]. 2022-09-25. [cit: 2024-03-04]. Dostupné z: https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities.

62. BROŽOVÁ, Helena a HOUŠKA, Milan. *Základní metody operační analýzy.* 1. Praha : Česká zemědělská univerzita v Praze, 2008. 224 s. ISBN 978-80-213-0951-7.

63. Polaris Market Research. Bluetooth 5.0 Market Share, Size, Trends, Industry Analysis Report, By Component; By Application By End-Use; By Region; Segment Forecast, 2022 - 2030. *Polaris Market Research.* [online]. 2022. [cit: 2024-01-16]. Dostupné z: https://www.polarismarketresearch.com/industry-analysis/bluetooth-5.0-market.

64. Mordor Intelligence. Zigbee Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029) Source: https://www.mordorintelligence.com/industry-reports/zigbee-market. *Mordor Intelligence.* [online]. 2022. [cit: 2024-01-16]. Dostupné z: https://www.mordorintelligence.com/industry-reports/zigbee-market.

65. IQRF Tech s.r.o. PŘÍLOHA K ÚČETNÍ ZÁVĚRCE. *Veřejný rejstřík a Sbírka listin.* [online]. 2023-06-26. [cit: 2024-01-17]. Dostupné z: https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=77405819&subjektId=982248&spis=1087425.

66. SINHA, Satyajit. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally. *IoT Analytics.* [online]. 2023-05-24. [cit: 2024-01-18]. Dostupné z: https://iot-analytics.com/number-connected-iot-devices/.

67. Nokia. Nokia Threat Intelligence Report finds malicious IoT botnet activity has sharply increased. *Nokia.* [online]. 2023. [cit: 2024-01-18]. Dostupné z: https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

Obrázek 1 topologie úplné (full) mesh sítě a částečné (partial) mesh sítě 12
Obrázek 2 příklad samoregenerace mesh sítě....13
Obrázek 3 velikost trhu spotřebitelského IoT....15
Obrázek 4 rozdělení dle sektorů ve využití podnikového IoT....18
Obrázek 5 velikost trhu IIoT a jeho odhadovaný růst 20
Obrázek 6 porovnání floodingu a routingu v Bluetooth Mesh sítích 23
Obrázek 7 schéma postupu Saatyho metody vícekriteriální analýzy 32
Obrázek 8 hierarchie AHP....36

8.2 Seznam tabulek

Tabulka 1 Saatyho škála 37
Tabulka 2 výsledná tabulka po provedení stanovení vah 38
Tabulka 3 normalizovaná tabulka s váhami 39
Tabulka 4 kontrola konzistence jednotlivých variant....40
Tabulka 5 výpočet vážených dílčích vah u úrovně šifrování....41
Tabulka 6 výpočet vážených dílčích vah u mechanismů autentizace....41
Tabulka 7 výpočet vážených dílčích vah u odolnosti vůči útokům....41
Tabulka 8 výpočet vážených dílčích vah u aktualizace bezpečnostních protokolů....42
Tabulka 9 výpočet vážených dílčích vah u dodržování bezpečnostních standardů....42
Tabulka 10 výsledná tabulka se syntézou preferencí a pořadím 43