Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Srovnání přenosových protokolů pro IoT a jejich použití pro konkrétní aplikace

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Artem Bornusov

Informatika

Název práce

Srovnání přenosových protokolů pro IoT a jejich použití pro konkrétní aplikace

Název anglicky

Comparison of IoT transmission protocols and their use for specific applications

---

Cíle práce

Bakalářská práce je tématicky zaměřena na problematiku přenosových bezdrátových sítí pro zařízení internetu věci.
Hlavním cílem práce je zhodnotit vybrané přenosové protokoly pro IoT.

Vedlejší cíle:

1. Charakterizovat vybrané bezdrátové protokoly pro přenos dat v oblasti IoT.

2. Analyzovat vybrané IoT aplikace.

3. Návrh modelu využitý IoT bezdrátových protokolů pro vybrané aplikace.

Metodika

Teoretická část bakalářské práce se bude zakládat na analýze a rešerši odborných zdrojů v rámci oblasti bezdrátových protokolů pro přenos dat z IoT zařízení.

V praktické části budou vybrány a zhodnoceny vybrané IoT aplikace. Následném kroku budou definovány požadavky na přenos dat. V dalším kroku budou zhodnoceny vybrané IoT bezdrátové protokoly na základě požadavků aplikací.

Na základě syntézy těchto poznatků budou zpracovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 stran

Klíčová slova

IoT, Protokoly, Bluetooth, ZigBee, NB-IoT, Wi-Fi

Doporučené zdroje informací

HANES, David, Gonzalo SALGUEIRO, Patrick GROSSETETE, Rob BARTON a Jerome HENRY. IoT fundamentals: networking technologies, protocols, and use cases for the Internet of things. Indianapolis, IN: Cisco press, [2017]. ISBN 978-1587144561.

SALAM, Abdul. *Internet of things for sustainable community development : wireless communications, sensing, and systems.* Cham: Springer, 2020. ISBN 978-3030352905.

The Internet of Things : Foundation for Smart Cities, eHealth, and Ubiquitous Computing. [elektronický zdroj] /. ARMENTANO, Ricardo.; BHADORIA, Robin Singh.; CHATTERJEE, Parag.; DEKA, Ganesh Chandra.

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 20. 02. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Srovnání přenosových protokolů pro IoT a jejich použití pro konkrétní aplikace" jsem vypracoval(a) 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 15. 3. 2024 _____

Poděkování

Rád(a) bych touto cestou poděkoval(a) vedoucímu práce Ing. Michalu Stočesovi za pomoc a cenné rady při psaní mé bakalářské práce.

Srovnání přenosových protokolů pro IoT a jejich použití pro konkrétní aplikace

Abstrakt

Bakalářská práce se zaměřuje na srovnání přenosových protokolů pro internet věcí (IoT) a jejich aplikaci v konkrétních scénářích. Teoretická část práce analyzuje a charakterizuje vybrané bezdrátové protokoly pro přenos dat v oblasti IoT. V praktické části jsou identifikovány a zhodnoceny klíčové IoT aplikace, přičemž jsou definovány požadavky na přenos dat. Vybrané bezdrátové protokoly, konkrétně Wi-Fi, Zigbee a Bluetooth, jsou důkladně analyzovány v kontextu těchto aplikací. Výsledky srovnání slouží k vytvoření modelu pro efektivní využití IoT bezdrátových protokolů v průmyslovém a městském prostředí. Práce poskytuje komplexní pohled na výkon a vhodnost těchto protokolů pro specifické aplikace v rámci internetu věcí.

Klíčová slova: IoT, Protokoly, Bluetooth, ZigBee, NB-IoT, Wi-Fi

Comparison of IoT transmission protocols and their use for specific applications

Abstract

This bachelor thesis focuses on the comparison of transmission protocols for the Internet of Things (IoT) and their application in specific scenarios. The theoretical part of the thesis analyzes and characterizes selected wireless protocols for data transmission in IoT. In the practical part, key IoT applications are identified and evaluated, while data transmission requirements are defined. The selected wireless protocols, namely Wi-Fi, Zigbee and Bluetooth, are thoroughly analyzed in the context of these applications. The results of the comparison are used to develop a model for the effective use of IoT wireless protocols in industrial and urban environments. The work provides a comprehensive view of the performance and suitability of these protocols for specific applications within the IoT.

Keywords: IoT, Protocols, Bluetooth, ZigBee, NB-IoT, Wi-Fi

Obsah

1 Úvod

V aktuálním prostředí technologického progresu je koncept internetu věcí (IoT) nedílnou součástí našich životů. Je tak pohonnou sílou inovací, zatímco bezdrátové přenosové protokoly hrají důležitou roli v provázání a umožňují účinnou výměnu dat.

Tato bakalářská práce se zaměřuje na srovnání tří důležitých bezdrátových protokolů, které hrají klíčovou roli ve fungování dnešního světa, jsou jimi Bluetooth, Wi-Fi, Zigbee, s důrazem na jejich využití v jednotlivých scénářích.

Ve svém výzkumu si budeme rozebírat otázky, jak tyto protokoly plní určité potřeby různých IoT aplikací, jak se odlišují v technických popisech a jaké jsou výhody a nevýhody. Podíváme se do světa vybraných průmyslových aplikací, abychom lépe porozuměli výzvám a přínosům těchto protokolů.

Cílem této bakalářské práce není pouze poskytnout technickou analýzu protokolů, ale předvést je v souvislosti reálných scénářů a uživatelských potřeb. Jak nám mohou být nápomocni Wi-Fi, Zigbee a Bluetooth v průmyslových pokrocích nebo při vytváření Smart Cities (chytrých měst). Na konci této bakalářské práce je zaměření na překonání pouze technické analýzy protokolů. Namísto toho se snaží ukázat, jakým způsobem mohou být Wi-Fi, Zigbee a Bluetooth využity v reálných scénářích a jak mohou splnit uživatelské potřeby. Výzkum se rozšiřuje i do konkrétních odvětví, jako jsou průmyslové aplikace a vytváření chytrých měst.

Tímto přístupem se usiluje o poskytnutí komplexnějšího pohledu na problematiku, který není omezen pouze technickými specifikacemi, ale zkoumá i praktické využití v různých kontextech. Věříme, že práce přispěje k širšímu pochopení významu těchto bezdrátových protokolů a jejich potenciálu v současném technologickém prostředí.

2 Cíl práce a metodika

2.1.1 Cíl práce:

Bakalářská práce je tematicky zaměřena na problematiku přenosových bezdrátových sítí pro zařízení internetu věci. Hlavním cílem práce je zhodnotit vybrané přenosové protokoly pro IoT, dále charakterizovat vybrané bezdrátové protokoly pro přenos dat v oblasti IoT, analyzovat vybrané IoT aplikace a navrhnout model využití IoT bezdrátových protokolů pro vybrané aplikace.

2.1.2 Metodika:

Teoretická část bakalářské práce se bude zakládat na analýze a rešerši odborných zdrojů v rámci oblasti bezdrátových protokolů pro přenos dat z IoT zařízení.

V praktické části budou vybrány a zhodnoceny vybrané IoT aplikace. Následném kroku budou definovány požadavky na přenos dat. V dalším kroku budou zhodnoceny vybrané IoT bezdrátové protokoly na základě požadavků aplikací.
Na základě syntézy těchto poznatků budou zpracovány závěry bakalářské práce.

3 Teoretická východiska

V této části práce se bude zakládat na analýze a rešerši odborných zdrojů v rámci oblasti bezdrátových protokolů pro přenos dat z IoT zařízení.

3.1 Internet věcí

„Představte si svět, ve kterém je téměř vše, na co si vzpomenete, online a komunikuje s dalšími věcmi a lidmi, aby bylo možné poskytovat nové služby, které zlepšují náš život. Od samořídících dronů, které vám doručí objednávku potravin, až po senzory ve vašem oblečení, které monitorují vaše zdraví – svět, který znáte, čeká velký technologický posun vpřed. Tento posun se souhrnně nazývá internet věcí (IoT).“ (Hanes a další, str. 30, 2017).

Internet věcí jako koncept byl poprvé objeven v 90. letech a stává se jednou z mnoha výzev které otevírají obzory vědeckému a technologickému rozvoji

Internet věcí se dnes využívá nejvíce v oblastech, jako např. automatizace domácností. Jeho hlavní přínosy jsou různorodé, ať už z pohledu uživatelů, či firem, které nejvíce zajímá úspora energie, efektivita a spolehlivost.

Označuje síť objektů (věcí) které mohou komunikovat mezi sebou nebo vnějšími subjekty, a vnímat opravdový svět a spojovat se s ním. (Elhadi a další, 2018)

Internet věcí rapidně roste, protože se počet zařízení silně zvyšuje, v různých odvětvích bylo vyvinuto spoustu aplikací, například řízení dopravy, zdravotnictví či mobilita.

Tyto aplikace mají různé omezení a požadavky (pokrytí, energetická efektivita, škálovatelnost), které vyvolávají globální heterogenitu internetu věcí.

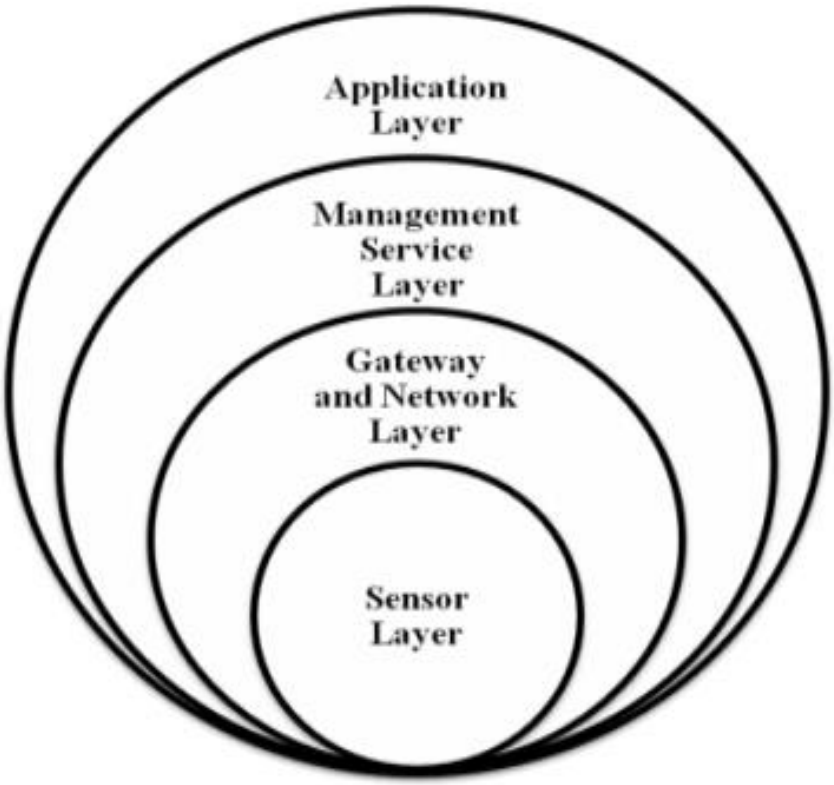
(Tournier a další, 2021)

Internet věcí je zaměřen hlavně na aplikační protokoly a síťové vrstvy. (Elhadi a další, 2018)

3.2 IoT architektura

Internetem věcí je poskytováno řešení založené na integraci informačních technologií, týkající se softwaru a hardwaru používaného k ukládání, zpracování a průběžného ukládání dat. Je navrženo mnoho standardů internetu věcí, které mají za úkol zjednodušit a usnadnit programátorům aplikací, a poskytovatelům služeb jejich práci. (Elhadi a další, 2018)

Architektura internetu věcí je všeobecně rozdělena do 4 vrstev.



Obrázek 1 - Vrstvy internetu věcí

3.2.1 Senzorová vrstva

Je to nejnižší vrstva IoT architektury (viz obr. 1), skládá se z vestavěných systému, senzorových sítí, čteček, RFID tagů nebo jiných forem snímačů rozmístěných v terénu, každý z těchto jednotlivých senzorů musí mít identifikaci a ukládání informací (například RFID tagy), sběr informací (např. senzorové sítě). (Soumyalatha, a další, 2016)

3.2.2 Přístupová brána a síťová vrstva

Je to 2 nejnižší vrstva, je zodpovědná za přesun informací, které jsou získané senzory do další vrstvy, podporuje flexibilní, škálovatelný, univerzální protokol podle standardů pro přenos dat z různých zařízení. Vrstva by měla mít výkonnou, vysokou a vytrvalou síť, zároveň by měla podporovat, aby mohlo více organizací komunikovat nezávisle. (Soumyalatha, a další, 2016)

3.2.3 Vrstva služeb pro správu

Tato vrstva funguje jako rozhrání mezi Přístupovou bránou a síťovou vrstvou a Aplikační vrstvou ve vzájemném směru. Zodpovídá za řízení informací a správu zařízení a zodpovídá za registraci velkých množství nezpracovaných dat a získání podstatných informací z ukládaných dat i z dat v reálném čase, zabezpečení a soukromí dat by mělo být zajištěno. (Soumyalatha, a další, 2016)

3.2.4 Aplikační vrstva

Jedná se o nejvyšší vrstvu internetu věcí (viz. obr. 1), která poskytuje uživateli rozhrání pro přístup k různým aplikacím pro různorodé uživatele. Aplikace mohou být využívány v rozmanitých sektorech jako Doprava, zdravotnictví, zemědělství, dodavatelský řetězec, vláda či maloobchod. (Soumyalatha, a další, 2016)

3.3 Normy

Při diskusi o normách je důležité nejprve pochopit záměr a účel jejich zavedení.
Primárním cílem normy je systematizovat používání pokynů. Normy, které vznikly na základě výzkumů a jsou schváleny odborníky z oboru, jsou autoritativní a jsou velmi důvěryhodné. Cílem normy je tedy normalizovat dohodnutý způsob provádění určité činnosti, měření objektu, vývoje výrobku nebo poskytování služby. Tímto způsobem mohou normy pomoct organizacím prosazovat příkazy jednotně a soudržně ve všech oblastech, v pozdější fázi také mohou tyto standardy organizaci umožnit měření dodržování původních pokynů. (Saleem, a další, 2018).

3.3.1 IEEE 802.15.4

Tento standard je nejpoužívanějším standardem v IoT pro MAC (Media Access Control), definuje formáty jak rámců, tak hlavičky počítaje cílových a zdrojových adres a také způsob, jakým mohou uzly mezi sebou komunikovat.
Formáty rámců využívané v obvyklých sítích nejsou vhodné pro nízkoenergetické sítě s více směry v internetu věcí kvůli své režii.
V roce 2008 byl vytvořen standard který nese název IEEE 802.15.4e který doplňuje a rozšiřuje standard IEEE 802.15.4 a podporuje komunikaci s nízkou spotřebou energie.

Využívá časovou synchronizaci a přeskakování kanálů, aby umožnila značnou spolehlivost, malé náklady a aby byly splněny požadavky na komunikaci v internetu věcí. (Salman, 2017)

3.3.2 IEEE 802.11ah

Tento standard je odlehčená (nízkoenergetická) verze původního standardu IEEE 802.11 (Wi-Fi). Byla navržena s nižší režií, aby splňovala požadavky IoT, standardy IEEE 802.11 jsou nejpoužívanějšími bezdrátovými standardy, jsou velmi široce používány a přijaty pro všechna elektronická zařízení včetně mobilních telefonů, notebooků, tabletů či digitálních televizorů. Původní standardy Wi-Fi však nejsou tolik vhodné pro aplikace internetu věcí kvůli své vysoké spotřebě a rámcové režii.
Pracovní skupina IEEE 802.11 proto začala pracovat na vzniku standardu 802.11ah, který má za úkol podporovat komunikaci s nízkou spotřebou energie a nízkou režií, vhodnou například pro senzory a motory. (Salman, 2017)

3.4 IoT protokoly

Byly navrženy mnohé standardy pro internet věcí, které měli za cíl zjednodušit a usnadnit práci programátorů a poskytovatelů služeb. Protokoly soupeří o postavení hlavního výběru pro připojené objekty, ale pro různé aplikace mohou být považovány za vhodnější různé protokoly. (Elhadi a další, 2018).
Upozorňují, že technologie používaná v bezdrátovém prostředí není jednoznačnou volbou, neboť každá technologie má své výhody a nevýhody.
V důsledku toho jsou vytvářeny nové protokoly s různorodými vlastnostmi přizpůsobenými potřebám připojených objektů jako je rozsah dosahu, snadná implementace, bezpečnost, spotřeba energie a další. (Elhadi a další, 2018)
Síť Gateway je zodpovědná za směrování dat z/do sítě s nízkou ztrátou výkonu do/z internetu nebo blízké místní sítě (LAN). (viz obrázek 3).
Mezi tyto protokoly patří Ethernet, 3G/4G/5G atd. (Mrabet a další, 2020)

Standard	Bluetooth	UWB	Zigbee	Wi-Fi
IEEE spec..	802.15.1	802.15.3a	802.15.4	802.11a/b/g
Frequency band	2.4GHz	3.1-10.6 GHz	868/915 MHz; 2.4 GHz	2.4 GHz; 5 GHz
Max signal rate	1 Mb/s	110Mb/s	250kb/s	54Mb/s
Nominal range	10 m	10 m	10-100 m	100 m
Nominal TX power	0 - 10 dBm	-41.3 dBm/MHz	(-25) - 0 dBm	15 - 20 dBm
Number of RF channels	79	(1-15)	1/10;16	14(2.4GHz)
Channel bandwidth	1MHZ	500MHz-7.5GHz	0.3/0.6 MHz; 2 MHz	22MHz
Modulation type	GFSK	BPSK, QPSK	BPSK (+ ASK), O-QPSK	BPSK, QPSK COFDM, CCK, M-QAM
Spreading	FHSS	DS-UWB, MB-OFDM	DSSS	DSSS, CCK, OFDM
Coexistence mechanism	Adaptive freq. hopping	Adaptive freq. hopping	Dynamic freq. selection	Dynamic freq. selection transmit power control (802.11h)
Basic cell	Piconet	Piconet	Star	BSS
Extension of the basic cell	Scatternet	Peer-peer	Cluster tree-mesh	ESS
Max number of cell nodes	8	8	> 65000	2007
Data protection	16-bit CRC	32-bit CRC	16-bit CRC	32-bit CRC

Obrázek 2 - Porovnání bezdrátových přenosových protokolů

3.4.1 Wi-Fi

Wi-Fi používá sadu síťových standardů **IEEE 802.11**, rozšiřuje síťové normy 802 na bezdrátový nosič dat tím, že upřesňuje provoz bezdrátové sítě (WLAN) v rádiových pásmech ISM.

První verze Wi-Fi byla zveřejněna v roce 1997. V normě 802.11 se definuje síťová vrstva řízení přístupu k médiu (MAC) a fyzická vrstva.

Standardy IEEE 802.11 b/g využívají frekvenční pásmo 2,4 GHz (viz Obrázek 2), zatímco verze 802.11a využívá pásmo 5 GHz, a 802.11n využívá mechanismus MIMO (Multiple Input - Multiple Output) na využití obou zmíněných pásem.

Standard 802.11 pro bezdrátové sítě LAN má 2 režimy, režim ad-hoc (peer-to-peer), nebo v režimu infrastruktury (peer-to-AP). (Rahman, 2015)

3.4.2 Zigbee

Zigbee je komunikační bezdrátová technologie s malým dosahem, která je známá především nízkou spotřebou energie, nízkou přenosovou rychlostí a nízkými náklady.
Protokol linkové a fyzické vrstvy funguje na standardu **IEEE 802.15.4** a ZigBee Alliance je zodpovědná za vývoj síťové a aplikační vrstvy.
Tato technologie je nejvíce vhodná pro bezdrátovou komunikaci na malé vzdálenosti mezi elektronickými přístroji.
Maximální přenosová rychlost této technologie je pouze 250 kb/s, což je nižší než u Bluetooth, ale stále je velmi vhodná pro aplikace s nízkým datovým provozem a velkým počtem zařízení.
Zigbee využívá fyzickou vrstvu IEEE 802.15.4, díky které je umožněna současná komunikace více zařízení.
Celkově je Zigbee velmi inovativním a účinným řešením pro bezdrátovou komunikaci na malou vzdálenost s nízkou spotřebou energie pro větší počet zařízení.
(Rahman, 2015)

3.4.3 Bluetooth

Bluetooth je bezdrátová technologie fungující na standardu **IEEE 802.15.1**. (Danbatta, a další, 2019).
Funguje na principu rádiového frekvenčního spektra o dosahu 2,4 GHz, které není licencované a je určeno pro zařízení k náhradě kabelů, jako jsou klávesnice, myši, chytré hodinky, tiskárny atd.
Bluetooth je také možný využít na komunikaci mezi přenosnými počítači, nebo jako most mezi různými sítěmi, také může sloužit jako uzel ad-hoc sítě.
Velmi často se využívá v bezdrátových osobních sítích, což jsou sítě, které poskytují komunikaci mezi zákaznickými zařízeními.
Předtím než vyšla verze Bluetooth 4.1 byly hlavními aplikacemi Bluetooth připojené páry zákaznických zařízení, která se spolu spojovala prostřednictvím nízko výkonného rádia, jako

mohl být například dálkový ovladač a televizor, chytré hodinky a chytrý telefon, nebo sluchátka a hudební přehrávač. (Sofi, 2016)

3.4.4 UWB

UWB je obecné označení pro rádiovou komunikaci, která využívá šířku pásma, která se blíží nebo je větší než 500 MHz. V poslední době se průzkum UWB zaměřuje na impulsní rádiové UWB (IR-UWB). Tato technika využívá radiofrekvenční impulsy s velmi krátkou dobou trvání (nano nebo pikosekundy), což má za následek velkou šířku pásma.
IR-UWB má tři hlavní výhody.
První výhodou je, že UWB podporuje velkou kapacitu kanálu díky velké šířce pásma, což umožňuje nízký přenosový výkon, který je potřeba, aby se zabránilo úzkopásmovému rušení s jinými bezdrátovými technologiemi.
Druhou výhodou je, že krátká doba trvání pulzů má za vliv, že dopad toho, že má více cest je méně významný, protože příchod pulzů lze oddělit a filtrovat v přijímači.
Třetí výhodou je, že vysoké časové rozlišení umožňuje velmi přesné časování.
(Coppens, a další, 2022)

3.4.5 Bluetooth LE

„*Bluetooth Low Energy (BLE, Bluetooth 4, Bluetooth Smart) je inovativní technologie vyvinutá skupinou Bluetooth Special Interest Group (SIG), jejímž cílem je stát se nejlepší alternativou k velkému množství standardních bezdrátových technologií, které již existují a jsou rozšířené na trhu* Bluetooth *Low Energy je nízkoenergetická verze Bluetooth specifikovaná ve verzi 4.0*.“ (Tosi a další, str. 1, 2017)
Zařízení BLE není kompatibilní s běžným zařízením Bluetooth, protože se jedná o jinou technologii. Zařízení Blutooth s duálním režimem však podporují jak BLE, tak klasické Bluetooth. (Armentano, 2017)

3.4.6 Připojení

Když si zařízení BLE přeje navázat spojení, nejprve neustále vysílá reklamní pakety, aby dalo najevo svou snahu. Časový interval mezi reklamními pakety se pohybuje od 20 ms do

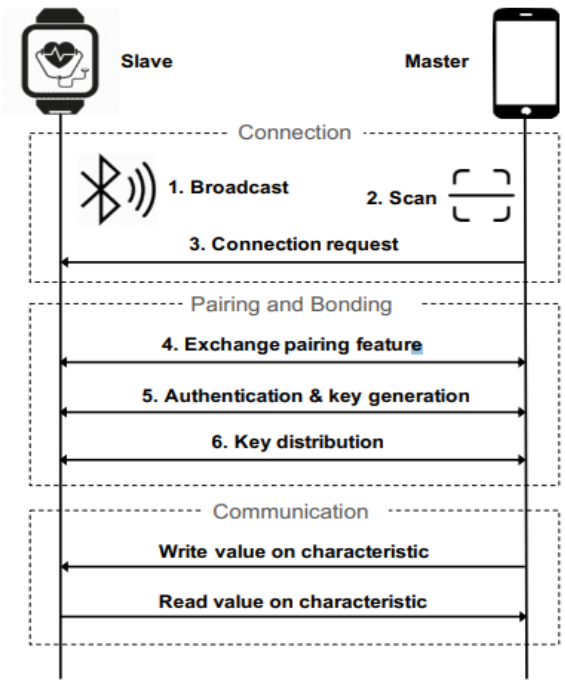
10,24 sekundy s volitelným náhodným zpožděním v rozmezí 0 ms až 10 ms přidaným za účelem zamezení kolizí. (Zuo, a další, 2019)

3.4.7 Párování a spojování

Hned po navázání spojení zahájí master a slave párování (viz obrázek 3), cílem je vytvořit zabezpečený kanál na kterém mohou mezi sebou komunikovat sjednáním šifrovacího klíče. Většinou si prvně vymění své párovací funkce (např: vstupní a výstupní funkce jako může být klávesnice a displej), poté se rozhodnou, který párovací protokol by měl být přijat. (Zuo, a další, 2019)

3.4.8 Komunikace

Po spárování a spojení si mohou slave a master vyměňovat data. Struktura dat se striktně řídí profilem (GATT), který má obvykle hierarchickou strukturu.
(Zuo a další, 2019)
GATT je zásobník profilů, který je navržen tak, aby podporoval komunikaci mezi zařízeními (D2D) s nadřazeným zařízením, a vytvářel tak hvězdicovou topologii.
(Hirsch a další, 2023)



Obrázek 3 - Bluetooth LE – Workflow

3.5 Aplikace v IoT

Koncept IoT (internet věcí) je čím dál tím více populární u využití moderních technologií, a to nejen ve fyzické podobě, ale také ve virtuálním světě.
Má za jeden z hlavních cílů zlepšení lidského života, často se objevuje v inteligentních domech, budovách a automobilech.
V IoT aplikacích inteligentních domácností se využívá například monitorovací systém založený na IoT, který využívá senzory a komunikační část, jako je Bluetooth a Wi-Fi. Bluetooth má omezený dosah, aby překonal tyto omezení, tak se využívá technologie IoT.
Také je zmíněn podnik pro chytré město používající aplikace založené na IoT, využívá pohybové senzory pro sběr a analýzu dat, celkově se IoT aplikace týkají vytváření propojené sítě, která podporuje automatizaci a vylepšuje efektivitu ve všech oblastech fungování. (Rahman, 2015)

3.5.1 Monitorování Energetické Efektivity Výrobního Procesu

V dnešní době se efektivní využití energie stává jednou z nahlížených priorit ve výrobním procesu kvůli růstu obav ze změny klimatu a usměrňujícím požadavkům.
Ze všech sektorů koncových uživatelů, na něž se zaměřuje zvyšování energetické působivosti, je výrobní proces považován za jeden z nejvíce ambiciózních, protože je největším spotřebitelem ze všech odvětví koncových uživatelů.
(Tan a další, 2017)
Podle Singapurských energetických statistik byla v roce 2015 spotřeba energie ve průmyslovém sektoru až 42,6% celkové spotřeby energie, poté následovaná komerčním sektorem s 36,5 % a sektorem domácností s 14,9 %. (Tan a další, 2017)

3.5.2 Bezpečnost Průmyslových Zařízení a Sítí

Chytré továrny se v poslední době staly trendy téma, průmyslová síťová zařízení a zařízení na bezpečnost se používají k spolehlivé a přímé správě objemného množství dat generovaných ve výrobě, velké množství dat, které je generováno v průmyslových závodech, jako jsou právě chytré továrny jsou nezbytné, aby nedošlo ke ztrátě dat a narušení bezpečnosti.
Prostředí a velikost inteligentních továren se ale liší.

Bezpečnostní a síťová zařízení v IT prostředí nezohledňují vlastnosti průmyslových řídicích systémů.

Pro účinnou správu a provoz průmyslových řídicích systémů je současný stav průmyslového síťového vybavení a bezpečnostního vybavení velmi vhodný.

Zkoumá se aktuální stav průmyslových síťových zařízení a bezpečnostních zařízení a porovnávají se mezi sebou a analyzují podobná zařízení v IT prostředí.

Existují příklady technologické analýzy a výzkumu průmyslových síťových zařízení a bezpečnostních zařízení.

Příklady výzkumu a vývoje pro analýzu technologií bezpečnostních a průmyslových síťových zařízení neexistují.

Kvůli tomu je potřeba analyzovat a porovnat technologie průmyslových síťových zařízení a bezpečnostních zařízení s podobnými zařízeními v IT.

Porovnáním a analýzou technologií průmyslových síťových zařízení a bezpečnostních zařízení s podobnými zařízeními v prostředí IT je možné vybrat zařízení pro zařízení národní infrastruktury a

Výběr zařízení a síťové architektury pro zabezpečení průmyslových zařízení

a síťové architektury pro zabezpečení zařízení národní infrastruktury a průmyslových zařízení. (Shin a další, 2020)

3.6 NB-IoT

Internet věcí (IoT) umožňuje připojit více různých zařízení k internetu a vyměňovat data s nimi, ovládat a monitorovat je. Mobilní technologie jsou důležité, aby se IoT rozvíjelo, neboť se hodí pro zařízení, které mají různé vlastnosti v nákladech, složitosti a výkonu. Úzkopásmový internet věcí (NB-IoT) byl vytvořen asociací 3GPP a nabízí výrazně větší a lepší pokrytí a nízké náklady pro zařízení s nízkou propustností a spotřebou energie. Možnosti použití NB-IoT zahrnují měření spotřeby, monitorování životního prostředí a ochranu majetku. NB-IoT kanály mají omezení na 180 kHz šířky pásma a používají pouze jeden blok fyzických prostředků LTE. NB-IoT může buď fungovat samostatně či integrován do sítě LTE. NB-IoT používá podobnou technologii jako využívá LTE pro downlink a základní systém s jedním nosičem (SC-FDMA) pro uplink. NB-IoT je součástí specifikace

3GPP verze 14 a produkt Qualcomm FSM je vyvíjen společností Qualcomm Technologies. (Chakrapani a další, 2019)

3.7 Smart Meter

Smart Meter neboli chytrý elektroměr slouží ke sledování spotřeby elektřiny, posluhuje také k přenosu dat poskytovatelům služeb pomocí různých typů komunikačních linek, kde se tyto informace využívají pro vyúčtování zákazníkům, analýzy spotřeby energie, vyrovnání zátěže a optimalizaci cen. (Salam, 2020)

3.8 Bezpečnost v IoT

Bezpečnostní hrozby spojené s IoT jsou složité a rozsáhlé.
Dle společnosti Gartner by měla být více než čtvrtina všech kybernetických útoků na firmy spojena s internetem věcí.
V současnosti na trhu upřednostňuje více cena a komfort před zabezpečením které má mnohdy za následek právě úspěšný kybernetický útok.
Existuje nedostatečná ochrana starších firmwarů a uživatelé se nedostatečně vzdělávají a informují o bezpečnosti. (Nebbione a Calzarossa, 2020)
Například už bylo vytvořeno mnoho protokolů pro různé typy aplikací, každý výrobce chce maximální možný podíl na trhu pro své navrhované objekty a protokoly.
Tlak trhu proto tlačí výrobce a prodejce k co nejrychlejší produkci svých položek.
Brzká výroba a uvedení na trh odsouvá bezpečnost do budoucna, to má někdy za následek fatální scénáře kvůli absenci bezpečnosti.
Někdy jsou tyto objekty nasazovány v reálném světě a kritické infrastruktuře (zdravotnictví a průmysl), z toho důvodu může být hrozba zvýšená, zařízení nejsou izolována, ale jsou připojena k místní síti nebo dokonce k internetu.
Bez řádného členění může kompromitace jednoho zařízení vést ke kompromitaci celé sítě. (Tournier a další, 2020)

„Zranitelnosti zařízení IoT jsou čím dál tím častější a útoky se stávají čím dál tím rafinovanějšími a silnějšími. Studie ukazují, že většina zařízení trpí určitou formou zranitelností. Například v roce 2016 botnet Mirai využil tisíce unesených zařízení IoT jako

vektory útoku k masivnímu DDoS útoku. V létě 2019 bylo objeveno 11 nulldenních zranitelností, které postihly populární operační systém VxWorks.“
(Nebbione a Calzarossa, str. 2, 2020)

Dalším důležitým aspektem, který by se měl vzít v potaz je informovanost a vzdělanost uživatelů v ohledu bezpečnosti v IoT, mnoho uživatelů si neuvědomuje rizika spojená s výchozími přihlašovacími údaji a nechává je nezměněné.
Existují zákony, jako je například IoT Consumer TIPS Act, který podporuje vzdělávací zdroje pro uživatele. (Nebbione a Calzarossa, 2020).

3.9 Vývoj trendů v IoT

„*V příštím století se planeta Země oblékne do elektronické kůže. Bude používat internet jako lešení, které bude podporovat a přenášet její vjemy. Tato kůže se již sešívá. Skládá se z milionů zabudovaných elektronických měřicích zařízení: termostatů, tlakoměrů, detektorů znečištění, kamer, mikrofonů, glukózových senzorů, EKG, elektroencefalografů. Ty budou zkoumat a monitorovat města a ohrožené druhy, atmosféru, naše lodě, dálnice a flotily nákladních aut, naše rozhovory, naše těla – dokonce i naše sny."*
(Irmak a Bozdal, str. 1, 2018)
Internet věcí je v dnešní době už velkým trendem, který má svá rizika i přínosy. Když se začal rozvíjet a zavádět, objevilo se spoustu překážek. Je zcela jasné, že stejné ale i další překážky se objeví u internetu věcí, jakmile se začne ještě více rozvíjet. Vytvoří IoT pro lidstvo temnou dobu, v ohledu soukromí, sledování či porušování práv spotřebitelů? Jak bude lidstvo komunikovat s IoT prostředím v osobním, ekonomickém a společenském životě? V současné době lze výzvy a pochybnosti týkající se technologie internetu věcí shrnout takto. (Irmak a Bozdal, 2018).

3.9.1 Bezpečnost a ochrana soukromí

Ačkoli bezpečnost a ochrana soukromí jsou obecnými výzvami informačních technologií, nové aplikace a atributy internetu věcí vytvářejí nové rozmanité problémy v oblasti bezpečnosti a ochrany soukromí. První prioritou by měla být identifikace těchto problémů. Společnosti a vývojáři informačních technologií by si měli být vědomi skutečnosti, že každý

uživatel internetu věcí na světě chce důvěřovat technologiím z hlediska bezpečnosti a ochrany soukromí. Každá technologie s neúčinným zabezpečením je terčem kybernetických útoků a krádeží. Největším kouzlem informačních technologií se po mnoha událostech narušujících soukromí stávají očekávání uživatelů a jejich důvěra v pohodlí. (Irmak a Bozdal, 2018)

3.9.2 Interoperabilita a standardy

Interoperabilita je definována jako schopnost produktu, služby, systému nebo různých sil vzájemně komunikovat, vyměňovat si informace a fungovat. Interoperabilita, konfigurace, označení a standardizace internetu věcí nejsou dosud propracovány. Proto je interoperabilita a standardy IoT velkou oblastí pro výzkumníky, kteří se zabývají výzvami IoT. (Irmak a Bozdal, 2018)

3.9.3 Otázky Ekonomiky a pokroku

Podle McKinsey Global Institute má internet věcí v roce 2025 celkový potenciální ekonomický dopad 3,9 až 11,1 bilionu dolarů ročně [38]. Jak bude dosaženo rovnoměrného rozdělení pro všechny části světa, protože se předpokládá, že internet věcí by měl být nástrojem pro globální posílení postavení bez ohledu na umístění spotřebitele, region, zemi nebo úroveň ekonomického rozvoje? (Irmak a Bozdal, 2018).

3.9.4 Škálovatelnost

Schopnost vývoje a rozšiřování aplikací, standardů a služeb internetu věcí je v současné době nepředvídatelná. Mělo by být provedeno více než odhadovaných výzkumů týkajících se výkonu a nákladů v reakci na změny v propustnosti nebo poptávce. (Irmak a Bozdal, 2018).

3.9.5 Objem dat a jejich interpretace:

Vzhledem ke všem zařízením internetu věcí, jako jsou senzory, akční členy, sítě, vytvářená data atd., je snadné předvídat problémy související s těmito otázkami. Společný vývoj a vzájemné studium internetu věcí a velkých dat bude jádrem problémů s objemy dat a jejich interpretací. (Irmak a Bozdal, 2018)

3.9.6 Potřeba energie

Fenomén internetu věcí nabízí neomezené zapojení zařízení, která odpovídajícím způsobem potřebují neomezené napájení. Zařízení internetu věcí se budou používat v prostředí, kde neexistuje možnost nabíjení. Jejich energie pro vykonávání navržených funkcí je omezená. Existují některá řešení, jak tento energetický problém překonat. Prvním řešením je zvýšení kapacity baterie, ale většina zařízení IoT je navržena v malých rozměrech a měla by být lehká, proto není další prostor pro větší baterii. Zásadní otázka zní: budou zařízení schopna vyrobit potřebnou energii? (Irmak a Bozdal, 2018)

3.10 Metoda AHP

„AHP metodu vytvořil Saaty (1980) pro řešení rozhodovacích problémů ve složitých a multikriteriálních situacích.“ (Darko a další, str. 4, 2019).
AHP nám pomáhá při rozhodování, které je charakterizováno mnoha vzájemně propojenými a také velmi často konkurujícími si faktory, a určuje priority při rozhodování mezi danými faktory, pokud jsou stanoveny v cíli rozhodování. Velmi důležitým aspektem jsou rozhodovací faktory s ohledem na jejich důležitost, aby bylo možné mezi nimi provádět kompromisy. (Darko a další, 2019)

AHP metoda se skládá ze tří kroků:

3.10.1 Vytvoření hierarchie

První úroveň hierarchie obsahuje kritický cíl, zatímco další nižší úrovně představují postupné rozdělení rozdělovacích kritérií, sub kritérií a alternativ pro dosažení našeho kritického cíle. (Darko a další, 2019).

3.10.2 Párová porovnání

Rozhodovatelé (často experti v dané oblasti) provedou párové srovnání prvků na každé úrovni hierarchie mezi sebou, přičemž je předpokládáno, že jsou prvky na sobě nezávislé.
V tomto ohledu a se zřetelem na cíl rozhodování se porovnává poměrná důležitost každých dvou kritérií na 2. úrovní hierarchie. Také se srovnávají 2 dílčí kritéria v rámci stejného kritéria na 2. úrovni, a tak dále. (Darko a další, 2019).

3.10.3 Kontrola konzistence

Expertní posudky jsou nezbytné pro stanovení relativní důležitosti každého jednotlivého kritéria a každé alternativy k dosažení cíle rozhodování. Kvůli tomu, že AHP umožňuje subjektivní úsudky rozhodovatelů, není konzistence a správnost úsudků zaručena.
Proto je tento krok nezbytný pro zajištění optimálního výsledku.
Pro kontrolu konzistence párových porovnání je třeba zvážit výpočet poměru konzistence.
V této fázi je nutno přezkoumat své původní úsudky, pokud by vypočtený poměr konzistence překročil mezní hodnotu 0,1. Poté co byla provedena všechna nutná párová porovnání a revize a také, že poměr konzistence je menší než 0,1, lze poté posudky slučovat a stanovit priority rozhodovacích kritérií spolu s dílčími kritérii. (Darko a další, 2019).

4 Vlastní práce

V praktické části bakalářské práce se zaměříme na provedení systematického hodnocení a srovnání vybraných bezdrátových protokolů pro internet věcí (IoT). Naším hlavním cílem bude analyzovat a porovnat výkonnost tří klíčových protokolů – Wi-Fi, Zigbee a Bluetooth – v kontextu dvou specifických průmyslových IoT aplikací. Tato analýza bude zahrnovat identifikaci klíčových charakteristik a požadavků každé aplikace na přenos dat, následovanou implementací nebo simulací přenosů dat s využitím vybraných protokolů.

Budeme zkoumat, jak každý z těchto protokolů splňuje specifické požadavky aplikací týkající se latence, spolehlivosti, spotřeby energie a dalších kritických faktorů. Implementace nebo simulace proběhnou v reálném nebo simulovaném prostředí odpovídajícím průmyslovým podmínkám. Cílem bude získat data o výkonnosti každého protokolu v různých scénářích a podmínkách.

Po provedení testů a sběru dat následuje důkladné zhodnocení výsledků a srovnání protokolů vzhledem k stanoveným požadavkům aplikací. Diskutujeme o klíčových aspektech úspěchů a výzev, které se objevily během hodnocení. Závěry práce budou vytvořeny na základě těchto výsledků a poskytnou komplexní pohled na efektivnost a vhodnost každého protokolu pro konkrétní průmyslové aplikace v prostředí internetu věcí.

4.1 Výběr a charakterizace IoT aplikací

Praktická část bakalářské práce bude pečlivě strukturována s důrazem na výběr a charakterizaci klíčových aplikací pro internet věcí (IoT) v průmyslovém prostředí. Tento krok hraje klíčovou roli v celkovém hodnocení bezdrátových protokolů, neboť specifika každé aplikace ovlivňují požadavky na přenos dat a následně volbu optimálních bezdrátových protokolů.

Výběr Aplikací:
Identifikace vhodných aplikací začala detailní analýzou průmyslových odvětví, s důrazem na oblasti s potenciálem pro využití IoT. Zároveň byly brány v úvahu aktuální trendy a

výzvy, kterým čelí průmyslový sektor. Výsledkem byly dvě klíčové aplikace, přičemž každá byla vybrána s ohledem na svůj strategický význam pro průmyslové prostředí.

Charakterizace Aplikací:
Podrobná charakterizace každé aplikace následně poskytla pevný rámec pro hodnocení bezdrátových protokolů. Specifické funkce a požadavky byly definovány s cílem získat co nejvíce relevantních informací pro následnou analýzu. Tato fáze zahrnovala určení klíčových aspektů, jako jsou typy dat, četnost přenosů, doba odezvy a bezpečnostní požadavky.

Vztah k Aplikacím a Protokolům:
Celkový cíl této části práce spočívá v nalezení optimálních bezdrátových protokolů pro každou specifickou aplikaci. To zahrnuje detailní zhodnocení kompatibility protokolů s jedinečnými požadavky každé aplikace, a to včetně analýzy, jak se protokoly vyrovnávají s parametry jako latence, spolehlivost a energetická efektivnost v kontextu průmyslových operací.

4.1.1 Identifikace aplikací

Prvním krokem v rámci praktické části bylo provedení pečlivé identifikace klíčových IoT aplikací, které byly strategicky vybrány s ohledem na svůj význam v průmyslovém sektoru. Tato etapa byla zahájena komplexní analýzou průmyslových odvětví, kde byly identifikovány oblasti s potenciálem pro implementaci IoT aplikací a přínosy pro průmyslové procesy.

Monitorování Energetické Efektivity Výrobního Procesu bylo pečlivě vybráno jako jedna z klíčových aplikací. Tato volba vycházela ze stoupajícího důrazu na efektivní využívání energie v průmyslových provozech. Cílem této aplikace je sledování, sběr a analýza dat o spotřebě energie v reálném čase, s důrazem na identifikaci oblastí pro energetické úspory a optimalizaci výkonu zařízení. Jak bylo popsáno v kapitole 3.5.1

Podobnou aplikací se zabývá projekt firmy Schneider Electric nazvaný "EcoStruxure Power Monitoring Expert", který poskytuje komplexní sledování a analýzu spotřeby energie v průmyslových a komerčních objektech.

Bezpečnost Průmyslových Zařízení a Sítí byla vybrána jako druha klíčová aplikace. Tato aplikace byla zvolena vzhledem k rostoucí komplexitě průmyslových sítí a potřebě posílení bezpečnosti průmyslových zařízení před kybernetickými hrozbami. Zaměřuje se na detekci anomálií, sledování přístupů a zabezpečení komunikace mezi průmyslovými zařízeními. Jak bylo popsáno v kapitole 3.5.2

Podobnou aplikací je projekt společnosti Siemens s názvem "Siemens Industrial Security", který se zaměřuje na zajištění kybernetické bezpečnosti průmyslových zařízení a sítí.

Tento krok identifikace aplikací poskytl pevný základ pro následnou charakterizaci a srovnání bezdrátových protokolů, jelikož každá z těchto aplikací nese specifické požadavky na přenos dat, které budou klíčovým faktorem v hodnocení vhodnosti jednotlivých protokolů v průmyslovém prostředí IoT.

4.1.2 Charakterizace Aplikací

Po identifikaci klíčových IoT aplikací byla provedena detailní charakterizace, která poskytla hlubší vhled do specifických požadavků a vlastností každé aplikace. Tato fáze je klíčovým krokem při určování, jaké bezdrátové protokoly budou nejvhodnější pro konkrétní průmyslové scénáře.

Monitorování Energetické Efektivity Výrobního Procesu:
Tato aplikace byla pečlivě rozpracována s důrazem na klíčové funkce a požadavky. Specifikované vlastnosti zahrnovaly:

Sběr Dat o Spotřebě Energie: Aplikace vyžaduje efektivní sběr dat týkajících se spotřeby energie průmyslových zařízení.

Identifikace Energetických Úspor: Zaměřuje se na schopnost identifikovat oblasti, kde lze implementovat opatření ke snížení energetické náročnosti.

Sledování Výkonu Zařízení: Důraz je kladen na sledování výkonu zařízení v reálném čase s cílem optimalizovat jejich efektivitu.

Bezpečnost Průmyslových Zařízení a Sítí:
Charakterizace této aplikace zahrnovala důkladný popis klíčových vlastností:

Detekce Anomálií: Aplikace se zaměřuje na schopnost detekce neobvyklých či podezřelých aktivit v průmyslových sítích.

Sledování Přístupů: Identifikuje a sleduje přístupy k průmyslovým zařízením, s cílem minimalizovat riziko neoprávněného přístupu.

Zabezpečení Komunikace: Klade důraz na zabezpečení komunikace mezi průmyslovými zařízeními, včetně šifrování a ochrany před kybernetickými hrozbami.

Tato podrobná charakterizace každé aplikace poskytuje základ pro následnou fázi hodnocení bezdrátových protokolů vzhledem k specifickým potřebám každé aplikace.

4.2 Definování požadavků na přenos dat

Druhá etapa praktické části bakalářské práce je věnována pečlivému definování specifických požadavků na přenos dat pro vybrané IoT aplikace. Tato fáze je klíčovým krokem v procesu optimalizace výběru bezdrátových protokolů, které musí efektivně splňovat unikátní požadavky každé aplikace v průmyslovém prostředí.

Definování Požadavků pro **Monitorování Energetické Efektivity Výrobního Procesu**:

V této fázi byly specifikovány následující klíčové požadavky s ohledem na charakter aplikace:

Minimální Latence: Pro účinné monitorování a reakci na aktuální energetické vzory vyžaduje aplikace minimální latenci při přenosu dat. To je zásadní pro okamžitou analýzu a optimalizaci spotřeby energie v reálném čase.

Vysoká Spolehlivost Přenosu Dat: Vzhledem k důležitosti sbíraných dat pro analýzy vyžaduje aplikace vysokou úroveň spolehlivosti při přenosu dat. Nespolehlivost by mohla způsobit ztrátu důležitých informací o energetické efektivitě výrobního procesu.

Optimalizovaná Šířka Pásma: S ohledem na objem dat spojených s energetickou spotřebou zařízení vyžaduje aplikace bezdrátový protokol, který efektivně využívá šířku pásma a minimalizuje zpoždění při přenosu dat.

Dlouhá Životnost Baterie: V případě bezdrátových senzorů vyžaduje aplikace bezdrátový protokol s nízkou spotřebou energie, což přispívá k prodloužení životnosti baterií a minimalizaci potřeby časté výměny.

Definování Požadavků pro **Bezpečnost Průmyslových Zařízení a Sítí:**

Při charakterizaci této aplikace byly stanoveny klíčové požadavky s ohledem na specifické bezpečnostní potřeby průmyslových operací:

Nízká Latence Při Detekci Anomálií: Pro aktivní identifikaci a odhalení bezpečnostních hrozeb vyžaduje aplikace nízkou latenci při detekci anomálií v průmyslových sítích. Rychlá reakce na neobvyklé události je zásadní pro minimalizaci rizika.

Spolehlivá Komunikace: S ohledem na citlivost na bezpečnostní hrozby vyžaduje aplikace bezdrátový protokol, který zajišťuje spolehlivou komunikaci bez rizika ztráty dat. Každá zpráva musí být doručena bezpečně a bez možnosti manipulace.

Šifrovaná Komunikace: Bezpečnostní opatření zahrnují šifrovanou komunikaci mezi průmyslovými zařízeními. Zabezpečení přenášených dat je klíčovým prvkem pro minimalizaci rizika kybernetických útoků a udržení integrity průmyslových sítí.

Nízká Spotřeba Energie v Čekacím Režimu: S ohledem na životnost bezdrátových prvků vyžaduje aplikace bezdrátový protokol s nízkou spotřebou energie v režimu čekání. To přispívá k prodloužení životnosti baterií a minimalizaci nákladů na údržbu.

Tato podrobná definice požadavků na přenos dat pro každou aplikaci poskytuje pevný základ pro následnou analýzu a srovnání vybraných bezdrátových protokolů v rámci průmyslového prostředí IoT.

4.3 Výběr IoT bezdrátových protokolů

V rámci této etapy praktické části bakalářské práce byl podniknut pečlivý a systemický přístup k výběru tří klíčových bezdrátových protokolů: Wi-Fi, Zigbee a Bluetooth. Tento proces vycházel z detailní analýzy každého z těchto protokolů s cílem identifikovat jejich unikátní vlastnosti a schopnosti, které by mohly být klíčové pro průmyslové aplikace v rámci internetu věcí (IoT).

Zahájila se pečlivá analýza každého bezdrátového protokolu, zaměřující se na jeho specifické charakteristiky a přednosti. Důraz byl kladen na schopnost každého protokolu efektivně a spolehlivě přenášet data v průmyslovém prostředí, s ohledem na požadavky IoT zařízení. Během této analýzy byly zkoumány aspekty jako přenosová rychlost, spolehlivost připojení, energetická účinnost a další klíčové faktory ovlivňující výkonnost bezdrátových protokolů.

Výsledkem této pečlivé analýzy byl vybraný soubor protokolů, který byl považován za nejvhodnější pro následné srovnání a aplikaci v průmyslových scénářích IoT. Tento důkladný výběr poskytuje pevný základ pro další etapy výzkumu, kde bude probíhat detailní

hodnocení výkonnosti a vhodnosti každého z těchto protokolů v konkrétních průmyslových aplikacích.

4.3.1 Výběr a popis jednotlivých protokolů

Byl proveden pečlivý výběr tří klíčových bezdrátových protokolů: Wi-Fi, Zigbee a Bluetooth. Tato volba byla provedena s ohledem na jejich jedinečné vlastnosti a schopnosti, které mohou být klíčové pro průmyslové aplikace v kontextu internetu věcí. Abychom lépe porozuměli těmto protokolům, je nutné se podívat na obecný kontext bezdrátových technologií a jejich využití v moderních komunikačních systémech.

Bezdrátové technologie hrají klíčovou roli v propojování zařízení a umožňují efektivní výměnu dat. V teoretické části práce jsme se podrobně zabývali konceptem internetu věcí (IoT) a jeho rostoucím významem v současném technologickém prostředí. Koncept IoT představuje integraci informačních technologií a hardwaru, která umožňuje ukládání, zpracování a průběžné využívání dat.

Wi-Fi, Zigbee a Bluetooth jsou klíčovými hráči v oblasti bezdrátových komunikačních technologií. Každý z těchto protokolů má své vlastní specifické využití a výhody. V rámci praktické části se zaměřujeme na jejich detailní popis, analyzujeme technické vlastnosti a srovnáváme je v kontextu vybraných průmyslových aplikací.

Wi-Fi:
Wi-Fi bylo zahrnuto jako standardní bezdrátový protokol kvůli vynikající vysoké přenosové rychlostí a stabilního připojení. Tato vlastnost je zásadní v průmyslových prostředích, kde je nezbytný rychlý a spolehlivý přenos dat. Wi-Fi se tak stává ideální volbou pro aplikace vyžadující vysokou propustnost, jako je monitorování a kontrola procesů v průmyslových zařízeních, kde je klíčová rychlá odezva na data.

Zigbee:
Zigbee byl vybrán kvůli své specializaci na nízkou spotřebu energie a optimalizaci pro průmyslová prostředí s velkým počtem zařízení. Tato charakteristika Zigbee hraje klíčovou

roli v situacích, kde je nutné efektivně spravovat energii a koordinovat komunikaci v sítích s nízkou spotřebou energie. Zigbee tak poskytuje optimální řešení pro rozsáhlé průmyslové nasazení, zejména v oblastech, kde je kritická efektivní energetická správa.

Bluetooth:
Bluetooth, a zejména jeho verze s technologií Low Energy (BLE), byl zahrnut díky své nízké spotřebě energie a schopnosti poskytovat nízkou latenci. Tyto vlastnosti jsou klíčové pro krátkodobá spojení a periodické přenosy dat, což se osvědčuje v průmyslových aplikacích s omezenými energetickými zdroji. Bluetooth může být efektivní volbou pro bezdrátovou komunikaci v oblasti bezpečnosti průmyslových zařízení a sítí, kde je klíčovým faktorem minimalizace energetické náročnosti.

Tento precizní výběr bezdrátových protokolů poskytuje solidní základ pro následné srovnání jejich výkonnosti a vhodnosti v konkrétních průmyslových aplikacích v rámci internetu věcí. Každý protokol byl vybrán s ohledem na jedinečné požadavky a charakteristiky průmyslových scénářů, což nám umožní získat hlubší vhled do jejich potenciálu a omezení.

4.4 Specifikace kritérií pro vícekriteriální analýzu

V rámci specifikace kritérií pro vícekriteriální analýzu bezdrátových protokolů pro IoT aplikace bychom se zaměřili na klíčová kritéria s důrazem na nejdůležitější aspekt – zabezpečení:

Zabezpečení:
Úroveň zabezpečení protokolu při přenosu dat. V průmyslových aplikacích, kde je důvěrnost a integrita dat klíčová, je zabezpečení primárním kritériem pro výběr bezdrátového protokolu.

Latence:
Časový interval mezi odesláním a doručením dat. Zvláště důležité pro aplikace vyžadující rychlou odezvu, přičemž nízká latence může být klíčovým faktorem.

Spolehlivost:
Schopnost protokolu přenášet data bez chyb a ztrát. V průmyslových prostředích, kde jsou nesprávná data nežádoucí, je spolehlivost zásadním faktorem.

Energetická Efektivnost:
Spotřeba energie při přenosu dat. Vzhledem k častému nasazení zařízení IoT na bateriový pohon je energetická efektivnost klíčovým hlediskem.

Dosah:
Maximální vzdálenost, na kterou je možné úspěšně přenášet data. Toto kritérium je klíčové pro průmyslová prostředí, kde může být potřeba pokrýt velké fyzické plochy s rozsáhlými zařízeními. Efektivní dosah protokolu může mít významný vliv na celkovou funkčnost a úspěšnost nasazení IoT v průmyslu.

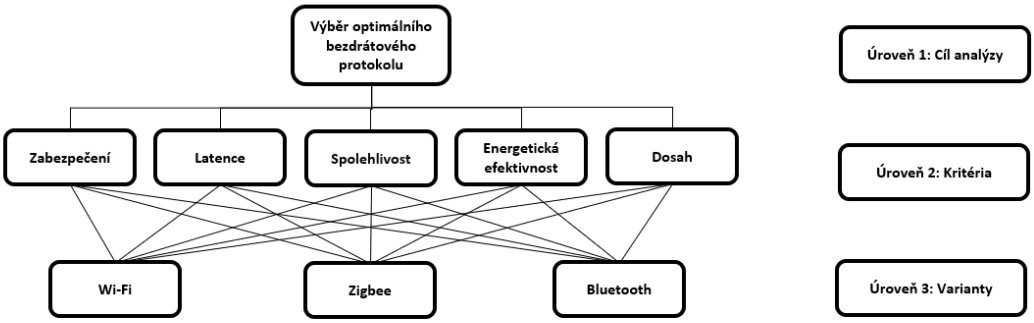
Tato kritéria byla vybrána s ohledem na důležité aspekty průmyslových aplikací a IoT prostředí, přičemž zabezpečení bylo zvýrazněno jako nejvýznamnější faktor.

4.5 Stanovení hlavního cíle

Hlavním cílem této vícekriteriální analýzy je identifikovat a doporučit optimální bezdrátový protokol pro průmyslové aplikace v rámci internetu věcí (IoT). Analýza se zaměřuje na klíčová kritéria, na zabezpečení, latenci, spolehlivost, energetickou efektivnost a dosah. Cílem je poskytnout informace a doporučení pro výběr protokolu, který nejlépe vyhovuje specifickým potřebám průmyslových scénářů využívajících technologie IoT. Budeme používat metodu Analytického Hierarchického Procesu (AHP).

4.6 Vytvoření hierarchie pro výběr optimálního bezdrátového IoT protokolu

V této části jsme aplikovali metodu Analytického Hierarchického Procesu (AHP) pro kriteriální ohodnocení a porovnání 3 bezdrátových IoT protokolů, kterými jsou: Wi-Fi, Zigbee a Bluetooth (viz obrázek 4). Naším cílem bylo vyhledat optimální bezdrátový protokol který nejlépe splňuje všechna kritéria.



Obrázek 4- Analytický hierarchický proces – IoT Protokoly

4.7 Stanovení vah kritérií

„Stanovení vah kritérií bývá výchozím krokem analýzy modelu vícekriteriální analýzy variant. Téměř výhradně je informace získaná některým z dále uvedených postupů použita ke stanovení preferenčních vztahů mezi variantami v závislosti na cílech celé analýzy. Tyto metody lze použít i pro kvantifikaci slovního vyjádření hodnocení variant.“ (viz tabulka 1). (T. Šubrt, a další, str. 171, 2011)

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

Tabulka 1 - Saatyho škála hodnocení kritérií

4.8 Sestavení matice porovnání

Na základě Saatyho škály jsme sestavili matici porovnání (viz. Tabulka 1) pro každou dvojici kritérií. Tyto matice reflektovaly relativní váhy a preference mezi kritérii.

4.9 Výpočet vlastních vektorů

Pro každou matici byly provedeny výpočty vlastních vektorů (viz. Tabulka 2), což jsou vektory odpovídající vlastním číslům dané matice. Tyto vektory reprezentují relativní důležitost jednotlivých kritérií. Byla použita funkce GEOMEAN pro zjištění Geometrického průměru a vypočtení vah (preferencí).

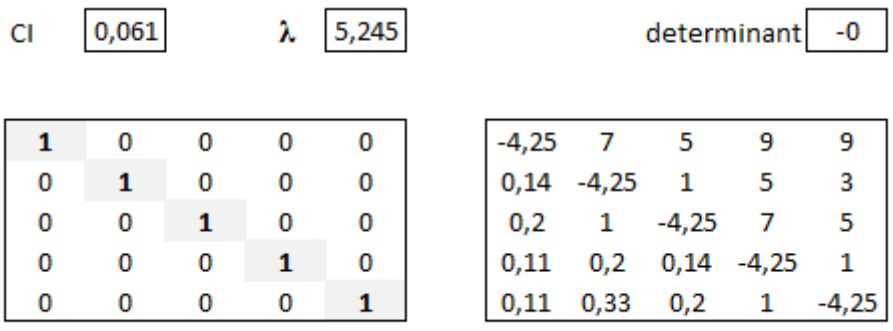
	Zabezpečení	Latence	Spolehlivost	Energetická efektivnost	Dosah	Geometrický průměr	Váha (preference)
Zabezpečení	1	7	5	9	9	4,903	0,596
Latence	0.14	1	1	5	3	1,1600	0,141
Spolehlivost	0.20	1	1	7	5	1,4758	0,179
Energetická efektivnost	0.11	0.20	0.14	1	1	0,3146	0,038
Dosah	0.11	0.33	0.20	1	1	0,3734	0,045
Součet	x	x	x	x	x	8,2273	1

Tabulka 2 – Výpočty vlastních vektorů

4.10 Kontrola konzistence

Byla provedena kontrola konsistence vah, například pomocí indexu konzistence, k ověření logické konzistence stanovených váh (viz obrázek 5). Pro správnou kontrolu byla zvolena **Citlivostní analýza** v aplikaci Microsoft Excel.

Citlivostní analýza: Výsledek, který byl zjištěn naznačuje, že subjektivní hodnocení kritérií je považováno za spolehlivé.



Obrázek 5- Citlivostní analýza

4.11 Stanovení kompromisní varianty

Bezpečnost	Wi-Fi	Zigbee	Bluetooth	Geo. průměr	Dílčí váhy	Vážené dílčí váhy	λ	Determinant
Wi-Fi	1	5	5	2,924	0,714	0,426	3	-0,000405916
Zigbee	0,2	1	1	0,585	0,143	0,085	3	-0,000405916
Bluetooth	0,2	1	1	0,585	0,143	0,085	3	-0,000405916

Tabulka 3 - Výpočet vážených dílčích váh u Bezpečnosti

Spolehlivost	Wi-Fi	Zigbee	Bluetooth	Geo. průměr	Dílčí váhy	Vážené dílčí váhy	λ	Determinant
Wi-Fi	1	5	3	2,466	0,649	0,116	3	-0,000404002
Zigbee	0,2	1	0,5	0,464	0,122	0,022	3	-0,000404002
Bluetooth	0,33	2	1	0,871	0,229	0,041	3	-0,000404002

Tabulka 4 - Výpočet vážených dílčích váh u Spolehlivosti

Latence	Wi-Fi	Zigbee	Bluetooth	Geo. průměr	Dílčí váhy	Vážené dílčí váhy	λ	Determinant
Wi-Fi	1	7	5	3,271	0,731	0,103	3,05	-0,000499843
Zigbee	0,14	1	0,33	0,359	0,080	0,011	3,05	-0,000499843
Bluetooth	0,2	3	1	0,843	0,189	0,027	3,05	-0,000499843

Tabulka 5 - Výpočet vážených dílčích váh u Latence

Energetická efektivnost	Wi-Fi	Zigbee	Bluetooth	Geo. průměr	Dílčí váhy	Vážené dílčí váhy	λ	Determinant
Wi-Fi	1	0,11	0,25	0,302	0,069	0,003	3	-0,000858503
Zigbee	9	1	3	3	0,682	0,026	3	-0,000858503
Bluetooth	4	0,33	1	1,097	0,249	0,01	3	-0,000858503

Tabulka 6 - Výpočet vážených dílčích váh u Energetické efektivity

Dosah	Wi-Fi	Zigbee	Bluetooth	Geo. průměr	Dílčí váhy	Vážené dílčí váhy	λ	Determinant
Wi-Fi	1	7	7	3,659	0,779	0,035	2,99	-0,00044235
Zigbee	0,14	1	1	0,519	0,111	0,005	2,99	-0,00044235
Bluetooth	0,14	1	1	0,519	0,111	0,005	2,99	-0,00044235

Tabulka 7 - Výpočet vážených dílčích váh u Dosahu

Z předešlých tabulek vyšly vážené dílčí váhy pro každou alternativu (viz Tabulky 3-7), které jsou rozhodující pro kritický výběr nejvhodnější alternativy.

5 Výsledky a diskuse

V rámci aplikace metody Analytického Hierarchického Procesu (AHP) bylo systematicky hodnoceno a porovnáno tři klíčové bezdrátové komunikační technologie: Wi-Fi, Zigbee a Bluetooth. Cílem bylo identifikovat optimální protokol pro konkrétní průmyslová nasazení v rámci internetu věcí (IoT). Hodnocení zohlednilo několik kritérií, jako jsou bezpečnost, latence, spolehlivost, energetická efektivita a dosah.

Protokoly	Syntéza preferencí	Pořadí
Wi-Fi	0,683	1.
Zigbee	0,149	3.
Bluetooth	0,167	2.

Tabulka 8 - Výsledky hodnocení kritérií

5.1 Analýza výsledku

Výsledná analýza ukazuje, že nejsilnější alternativou (bezdrátovým protokolem) je Wi-Fi, následovaná Bluetooth a poté ZigBee (viz Tabulka 8), ze všech hodnocených kritérií je právě tento protokol nejvýhodnější variantou pro použití, vše ale záleží na konkrétních průmyslových scénářích.

5.2 Hodnocení kritérií

- **Bezpečnost:** V rámci AHP analýzy byla Wi-Fi ohodnocena jako nejbezpečnější volba s vynikajícími bezpečnostními prvky, což je klíčové pro průmyslová nasazení.
- **Latence:** Bluetooth dosáhlo nejlepších výsledků v oblasti latence, což může být kritické pro aplikace vyžadující rychlé přenosy dat.
- **Spolehlivost:** Wi-Fi vynikla v oblasti spolehlivosti, což je zásadní pro průmyslové prostředí s vysokým počtem zařízení.
- **Energetická Efektivita:** Zigbee bylo opět hodnoceno nejlépe v nízké spotřebě energie, což je klíčový faktor pro zařízení s omezenými zdroji.
- **Dosah:** Wi-Fi bylo ohodnoceno s největším dosahem, což může být klíčové v rozsáhlých průmyslových prostředích.

5.3 Omezení a možná vylepšení metodologie

Omezení:

- Omezený rozsah výzkumu: I přestože jsme provedli důkladné hodnocení tří klíčových vybraných bezdrátových protokolů (Wi-Fi, Zigbee, Bluetooth) v rámci AHP metody, lze nalézt omezení v rozsahu výzkumu. Vzhledem k tomu, že další protokoly nebyly zahrnuty do analýzy, mohli ovlivnit celkovou komplexnost výběru optimálního protokolu pro průmyslové nasazení.
- Omezení hodnotících kritérií: I přestože byla vybrána klíčová kritéria, jako bezpečnost, latence, spolehlivost, energetická efektivita a dosah, jsou další faktory, které mohou ovlivnit výběr optimálního protokolu, proto některé specifické požadavky průmyslových prostředí mohly být přehlédnuty.

Možné vylepšení metodologie:

- Rozšíření rozsahu výzkumu: Pro dosažení komplexnějšího porovnání, by mohlo být prospěšné rozšířit rozsah našeho výzkumu přidáním dalších bezdrátových protokolů, což by zapříčinilo širší perspektivu na problematiku a pomoci identifikovat alternativní řešení.
- Zahrnutí dalších kritérií: V budoucím výzkumu by mohlo být užitečné vybrat další specifické faktory, to by mohlo vést k ještě přesnějším a komplexnějším výsledkům.

5.4 Výzvy a budoucí směry

Zaměření na optimalizaci bezdrátových protokolů v průmyslovém prostředí vychází ze stále rostoucí potřeby přizpůsobit tyto technologie konkrétním potřebám průmyslových odvětví. Různorodé výzvy, jako je potřeba stability, spolehlivosti, nízké latence a energetické efektivity, vyžadují inovativní přístupy a úpravy existujících protokolů. Bezpečnostní aspekty IoT jsou stále naléhavější vzhledem k rostoucímu povědomí o možných bezpečnostních rizicích v průmyslových systémech využívajících bezdrátové komunikace.

Integrace umělé inteligence (AI) do bezdrátových protokolů reflektuje snahu poskytnout průmyslovým systémům vyšší úroveň autonomie a schopnost adaptace. Tyto inovace by mohly přinést efektivnější a chytřejší řešení pro specifické potřeby průmyslových aplikací IoT. V neposlední řadě, důraz na integraci s průmyslovými standardy a protokoly je odvozen ze snahy zajistit efektivní propojení bezdrátových technologií s existujícími průmyslovými normami, což přispěje k zajištění kompatibility a interoperability v průmyslových prostředích.

Optimalizace Protokolů pro Průmyslová Nasazení:

- V kontextu průmyslových aplikací IoT bude jednou z výzev úprava a optimalizace bezdrátových protokolů tak, aby co nejlépe vyhovovaly specifickým potřebám průmyslu. Zohledněním požadavků na stabilitu, spolehlivost a nízkou latenci bude třeba dosáhnout optimálních výsledků v průmyslovém prostředí.

Zabezpečení IoT v Průmyslových Systémech:

- Bezpečnostní aspekt IoT v průmyslových prostředích bude klíčovým tématem, budoucí směry by se měly zaměřit na inovace v oblasti bezpečnostních opatření, šifrování dat a identifikace potenciálních bezpečnostních rizik spojených s průmyslovým nasazením.

Integrace s Průmyslovými Standardy a Protokoly:

- Aby bylo dosaženo efektivní integrace IoT do průmyslových systémů, je nezbytné brát v úvahu existující průmyslové standardy a protokoly. Budoucí směry by mohly klást důraz na propojení bezdrátových protokolů s průmyslovými normami a zajištění kompatibility.

Efektivní Energetické Řešení:

- S ohledem na průmyslová odvětví, kde mohou být některá zařízení obtížně dosažitelná nebo v náročných podmínkách, bude klíčové hledat inovativní způsoby optimalizace energetické efektivnosti bezdrátových protokolů.

Rozvoj Umělé Intelligence pro IoT:

- Integrace prvků umělé inteligence (AI) do bezdrátových protokolů může poskytnout možnosti pro lepší autonomii a schopnost adaptace systémů IoT v průmyslu.

6 Závěr

V této bakalářské práci byla provedena důkladná analýza a srovnání tří klíčových bezdrátových protokolů pro internet věcí: Wi-Fi, Zigbee a Bluetooth.
Teoretická část práce se zaměřila na podrobnou charakterizaci těchto protokolů, přičemž rešerše umožnila získání hlubší znalosti o jejich vlastnostech, výhodách a omezeních.

Praktická část se zaměřila na výběr a analýzu dvou konkrétních průmyslových aplikací: Monitorování Energetické Efektivity Výrobního Procesu a Bezpečnost Průmyslových Zařízení a Sítí. Tyto aplikace byly dále podrobně charakterizovány, a následně byly definovány specifické požadavky na přenos dat, které tvořily základ pro hodnocení vybraných bezdrátových protokolů.

Vybrané protokoly, Wi-Fi, Zigbee a Bluetooth, byly následně podrobeny systematickému hodnocení v rámci vícekriteriální analýzy, využívající metodu Analytického Hierarchického Procesu (AHP). Tato analýza byla provedena s ohledem na klíčová kritéria, jako je bezpečnost, latence, spolehlivost, energetická efektivnost a dosah, přičemž byly stanoveny váhy jednotlivých kritérií pomocí Saatyho metody.

Výsledky této analýzy ukázaly, že v kontextu stanovených kritérií a požadavků průmyslových aplikací se nejlépe osvědčila varianta Wi-Fi, která byla identifikována jako optimální kompromisní volba. Nicméně i ostatní varianty, jakými jsou Zigbee a Bluetooth, jsou v průmyslovém prostředí uznávané a využívané. I když dosahují průměrných hodnot v některých kritériích, stále poskytují spolehlivé možnosti pro bezdrátovou komunikaci v průmyslu. Každá z těchto technologií může být uplatněna v závislosti na specifických potřebách a podmínkách průmyslových aplikací v rámci internetu věcí.

7 Seznam použitých zdrojů

HANES, David, Gonzalo SALGUEIRO, Patrick GROSSETETE, Rob BARTON a Jerome HENRY. IoT fundamentals: networking technologies, protocols, and use cases for the Internet of things. Indianapolis, IN: Cisco press, [2017]. ISBN 978-1587144561.

SALAM, Abdul. Internet of things for sustainable community development: wireless communications, sensing, and systems. IN: Cham Springer [2020]. ISBN 978-3030352905

ARMENTANO, Ricardo, a kol. The Internet of Things: Foundation for Smart Cities, eHealth, and Ubiquitous Computing. [online], [2017]. [cit. 2024-03-13].
Dostupné z: <https://www.scribd.com/document/491577064/The-Internet-of-Things-Foundation-for-Smart-Cities-eHealth-and-Ubiquitous-Computing-PDFDrive-pdf>

ELHADI, S. a kol. Comparative Study of IoT Protocols. [online]. 2018. [cit. 2024-03-13].
Dostupné z: <https://ssrn.com/abstract=3186315>

TOURNIER, J. a kol. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. [online]. 2021. [cit. 2024-03-13].
Dostupné z: <https://doi.org/10.1016/j.iot.2020.100264>

NAVEEN, S. Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges [online]. 2016. [cit. 2024-03-13].
Dostupné z:
<https://www.researchgate.net/publication/330501274_Study_of_IoT_Understanding_IoT_Architecture_Applications_Issues_and_Challenges>

RAHMAN, A. Comparison of Internet of Things (IoT) Data Link Protocols. [online]. 2015. [cit. 2024-03-13].
Dostupné z: <https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_dlc.pdf>

SOFI, M. Bluetooth Protocol in Internet of Things (IoT), Security Challenges and a Comparison with Wi-Fi Protocol: A Review. [online]. 2016. [cit. 2024-03-13]. Dostupné z: <https://www.researchgate.net/publication/311086845_Bluetooth_Protocol_in_Internet_of Things_IoT_Security_Challenges_and_a_Comparison_with_Wi-Fi_Protocol_A_Review>

SHIN, D. Characteristic Analysis of Industrial Network and Security Equipment [online]. 2020. [cit. 2024-03-13].
Dostupné z: <https://koreascience.kr/article/JAKO202019550426874.page>
CHAKRAPANI, A. NB-IoT Uplink Receiver Design and Performance Study [online]. 2019. [cit. 2024-03-13].
Dostupné z: <https://ieeexplore.ieee.org/abstract/document/8922625>

NEBBIONE, G. Security of IoT Application Layer Protocols: Challenges and Findings [online]. 2020. 2 s. [cit. 2024-03-13].
Dostupné z: <https://www.mdpi.com/1999-5903/12/3/55>

SALMAN, T. Networking protocols and standards for internet of things. [online]. 2020. [cit. 2024-03-13].
Dostupné z: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119173601.ch13>

SALEEM, J. a kol. IoT standardisation: challenges, perspectives, and solution [online]. 2018. [cit. 2024-03-13].
Dostupné z: <https://dl.acm.org/doi/abs/10.1145/3231053.3231103>

MRABET, H. a kol. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis [online]. 2020. [cit. 2024-03-13].
Dostupné z: <https://www.mdpi.com/1424-8220/20/13/3625>

DANBATTA, S. VAROL, A. Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation [online]. 2019. [cit. 2024-03-13].
Dostupné z: <https://ieeexplore.ieee.org/abstract/document/8757472>

COPPENS, D. a kol. An Overview of UWB Standards and Organizations (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions [online]. 2022. [cit. 2024-03-13].
Dostupné z: <https://ieeexplore.ieee.org/abstract/document/9810941>

TOSI, J. a kol. Performance Evaluation of Bluetooth Low Energy: A Systematic Review [online]. 2017. 1 s. [cit. 2024-03-13].
Dostupné z: <https://www.mdpi.com/1424-8220/17/12/2898>

ZUO, C. a kol. Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps [online]. 2019. [cit. 2024-03-13].
Dostupné z: <https://dl.acm.org/doi/abs/10.1145/3319535.3354240>

HIRSCH, C. a kol. DynGATT: A dynamic GATT-based data synchronization protocol for BLE networks [online]. 2023. [cit. 2024-03-13].
Dostupné z: <https://www.sciencedirect.com/science/article/pii/S1389128623000051>

TAN, Y. a kol. DynGATT: Internet-of-Things Enabled Real-time Monitoring of Energy Efficiency on Manufacturing Shop Floors [online]. 2017. [cit. 2024-03-13].
Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2212827116314111>

IRMAK, E. BOZDAL, M. Internet of Things (IoT): The Most Up-To-Date Challenges, Architectures, Emerging Trends and Potential Opportunities [online]. 2018. [cit. 2024-03-13]. Dostupné z: <https://www.researchgate.net/profile/Mehmet-Bozdal/publication/325222068_Internet_of_Things_IoT_The_Most_Up-To-Date_Challenges_Architectures_Emerging_Trends_and_Potential_Opportunities/links/5b09e112a6fdcc8c25325369/Internet-of-Things-IoT-The-Most-Up-To-Date-Challenges-Architectures-Emerging-Trends-and-Potential-Opportunities.pdf>

DARKO, A. a kol. Review of application of analytic hierarchy process (AHP) in construction [online]. 2018. [cit. 2024-03-13].
Dostupné z: <https://www.tandfonline.com/doi/abs/10.1080/15623599.2018.1452098>

ŠUBRT, Tomáš et al. Ekonomicko-matematické metody. Plzeň : Aleš Čeněk, 2011, 171 s. ISBN 978-80-7380-345-2.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

IoT – Internet of Things, Internet věcí

RFID – Radio Frequency Identification, Identifikace na rádiové frekvenci

GATT – Generic Attribute Profile, profil generických atributů

IEEE – Institute of Electrical and Electronics Engineers, Institut elektrotechnických a elektronických inženýrů

LAN – Local Area Network, lokální síť

MIMO – Multiple Input, Multiple Output

UWB – Ultra Wideband

BLE – Bluetooth Low Energy

DDOS – Distributed Denial of service, distribuovaný DoS