Česká zemědělská univerzita v Praze

Technická fakulta

Katedra využití strojů

Bakalářská práce

Bezpečnostní analýza stávajících mesh sítí

Ondřej Pokorný

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ondřej Pokorný

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Bezpečnostní analýza stávajících mesh sítí

Název anglicky

Security analysis of existing mesh networks

Cíle práce

Primárním cílem práce je analyzovat a prakticky ověřit moderní trendy při realizaci mesh sítí nové generace. Zjištěné výsledky budou analyzovány jak z fyzikálního, tak i technologického hlediska a bude stanoven základní předpoklad použití těchto sítí. Druhotným cílem je posoudit bezpečnostní rizika a způsoby zabezpečení stávajících mesh sítí (především WiFi) a navrhnout odpovídající doporučení.

Metodika

Na základě literární rešerše student analyzuje fyzikální a technické možnosti aktuálních mesh sítí dle jednotlivých frekvencí a provede bezpečnostní rozbor použité technologie především z pohledu útoku ”man in the middle”. O těchto testech se na základě výsledku provede detailní srovnání bezpečnostních rizik mesh sítí a sítí s opakovačem.

Doporučený návrh osnovy:

1. Úvod
2. Cíl práce a metodika
3. Analýza teorie mesh sítí
4. Praktické technologie a frekvence využívané v mesh sítích
5. Nasazení mesh sítí v domácích a komerčních prostorách
6. Bezpečnost mesh sítí v jednotlivých technologiích (primárně WiFi)
7. Praktické ověření funkčnosti
8. Finanční zhodnocení
9. Závěr a doporučení

Doporučený rozsah práce

30 až 40 stran textu včetně obrázků, grafů a tabulek

Klíčová slova

mesh, počítačová síť, bezpečnost, IoT

Doporučené zdroje informací

DOSTÁLEK, L. Velký průvodce protokoly TCP/IP. Bezpečnost., Computer Press, 2001, ISBN: 807226513x
firemní literatura
HARVÁNEK, L. KONFIGURACE A ANALÝZA RŮZNÝCH TYPŮ ZAPOJENÍ BEZDRÁTOVÝCH SÍTÍ 802.11 , VUT Brno, BP, 2007
HELD, G. Wireless Mesh Networks, Taylor & Francis Ltd · 2019 , ISDN: 224214381
RANI, A. – KUMAR, N. – SINGH, S. – SINHA, N. – JENA, R. – PATRA, H. Remote sensing data analysis in R. Abigdon: CRC Press, 2021. ISBN 978-0-367-72562-4.
Zandl, P. : WiFi Praktický průvodce, 2003, Computer Press

Předběžný termín obhajoby

2023/2024 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra využití strojů

Elektronicky schváleno dne 10. 3. 2023

doc. Ing. Petr Šařec, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 3. 2023

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 31. 03. 2024

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma: „Bezpečnostní analýza stávajících mesh sítí“ vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů. Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby. Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí. Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.

V Praze dne 31.03.2024 _____

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu práce Ing. Zdeňkovi Votrubovi, Ph.D. za výběr tématu a za možnost pracovat pod jeho vedením. Dále bych rád poděkoval Bc. Michalu Kubínovi a Filipu Švábenickýmu za poskytnutí prostoru a techniky k provedení praktické části.

Bezpečnostní analýza stávajících mesh sítí

Abstrakt

Cílem bakalářské práce je shrnout momentální technologický a bezpečnostní stav meshových sítích. Úvodní literární rešerše se věnuje zkoumání vlastností a struktury meshové sítě, včetně analýzy používaných technologií, jako jsou Wi-Fi, Bluetooth a Zigbee a jejich základní zabezpečení. Dále je provedena analýza praktického využití mesh sítě v různých oblastech jako IoT, Smarthome či Průmysl 4.0. Samotné bezpečnostní hledisko je zkoumáno z několika stran. V práci jsou rozebírány jednotlivé bezpečnostní cíle (důvěrnost, integrita, autentizace, autorizace, dostupnost), jejich nedostatky, či naopak silné stránky. Dále práce identifikuje různé bezpečnostní hrozby, jimž je mesh síť vystavována. Mezi ně patří např. směrovací a DoS (Denial of Service) útoky, jež jsou zde podrobně rozebrány. V poslední části bakalářské práce se nachází praktické testování meshové sítě. Konkrétně se měří odolnost sítě vůči okolním rušivým signálům, jež využívají stejné či podobné frekvenční pásmo. Cílem práce je poskytnout ucelený pohled na bezpečnostní aspekty mesh sítě a přispět k lepší ochraně komunikace a dat v této dynamické a rozmanité síťové topologii.

Klíčová slova: mesh, počítačová síť, bezpečnost, IoT

Security analysis of existing mesh networks

Abstract

The aim of the bachelor thesis is to summarize the current technological and security status of mesh networks. The initial literature search explores the characteristics and structure of a mesh network, including an analysis of the technologies used such as Wi-Fi, Bluetooth and Zigbee and their basic security. Furthermore, an analysis of the practical applications of mesh network in various fields such as IoT, Smarthome and Industry 4.0 is also presented. The security aspect itself is examined from several sides. The different security goals (confidentiality, integrity, authentication, authorization, availability), their weaknesses or on the contrary their strengths are discussed. Furthermore, the thesis identifies various security threats to which the mesh network is exposed. These threats include, for example, routing attacks and Denial of Service (DoS) attacks, which are discussed in detail. In the last part of the bachelor thesis there is a practical testing of a mesh network created by me. Specifically, the network's resistance to nearby interfering signals that use the same or similar frequency band is measured. The aim of the thesis is to provide a comprehensive view of the security aspects of a mesh network and to contribute to a better protection of communication and data in this dynamic and diverse network topology.

Keywords: mesh, computer network, security, IoT

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

IoT	Internet of Things
Wi-Fi	Wireless Fidelity
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ID	Identifikace
DoS	Denial of service
DNS	Domain Name System
MitM	Man in the middle
WLAN	Wireless Local Area Network
DSSS	Direct Sequence Spread Spectrum
CCK	Complimentary Code Keying
OFDM	Orthogonal frequency division multiplexing
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
MIMO	Multiple Input Multiple Output
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

OWE	Wi-Fi Enhanced Open with Opportunistic Wireless Encryption
SAE	Simultaneous Authentication of Equals
RSSI	Received Signal Strength Indication
HCI	Host Controller Interface
EDR	Enhanced Data Rate
PSK	Phase Shift Keying Modulation
GFSK	Gaussian Frequency Shift Keying
ECDH	Elliptic Curve Diffie-Hellman
ACL	Access Control Lists
EAP	Extensible Authentication Protocol
PKI	Public Key Infrastructure
RBAC	Role-based access control
UDP	User Datagram Protocol
ICMP	The Internet Control Message Protocol
QoS	Quality of Service
TCP	Transmission Control Protocol
CDMA	code division multiple access
TDMA	time division multiple access

1. Úvod

Historie mesh sítí sahá do 70. let 20. století, kdy se začaly objevovat první koncepty decentralizovaných a samoorganizujících se sítí. Jedním z klíčových okamžiků této historie byl rok 1971, kdy Norman Abramson a jeho tým na Havajské univerzitě vyvinuli první bezdrátovou mesh síť s názvem ALOHAnet. Tato síť byla určena k propojení počítačů na Havaji a využívala princip náhodného přístupu k médiu, což byla v té době inovativní myšlenka. Další významný krok vpřed nastal v 90. letech 20. století, kdy začaly vznikat první standardy pro bezdrátové sítě, jako je IEEE 802.11 (Wi-Fi). Tím se otevřely nové možnosti využití mesh sítí ve větším měřítku. Nicméně první komerčně dostupné mesh sítě se začaly objevovat až v první dekádě 21. století (1)

To vše je však již minulostí. V dnešní době neustálého rozvoje informačních technologií a digitalizace společnosti se bezpečnost digitálních sítí stává klíčovým aspektem pro zachování integrity, důvěrnosti a dostupnosti dat. S nárůstem počtu připojených zařízení a složitostí síťových infrastruktur vznikají nové bezpečnostní výzvy, které vyžadují systematický přístup k identifikaci potenciálních hrozeb a boji proti nim.

Jedním z nových trendů v síťových technologiích, které získávají na popularitě, jsou sítě typu mesh. Síť mesh je decentralizovaný model propojení zařízení, který umožňuje flexibilní a dynamickou komunikaci mezi uzly bez nutnosti centrálního řízení. Tato síťová topologie nachází uplatnění v široké škále aplikací od průmyslových a senzorových sítí až po systémy inteligentních domácností.

Technologie používané v mesh sítích zahrnují širokou škálu bezdrátových standardů, které umožňují připojení zařízení na různých frekvencích a s různým prostorovým pokrytím. Mezi nejčastěji používané technologie patří Wi-Fi, Bluetooth a Zigbee. Wi-Fi nabízí vysokorychlostní bezdrátové připojení a širokou dostupnost, což z ní dělá ideální volbu pro kancelářské potřeby. Bluetooth poskytuje nízkou spotřebu energie a krátký dosah, takže je vhodný pro připojení mobilních zařízení a senzorů v osobních sítích. Zigbee je optimalizováno pro nízkou spotřebu energie a velký počet uzlů, což je ideální pro průmyslové a senzorické aplikace.

2. Cíl práce

Cílem bakalářské práce je provést komplexní bezpečnostní analýzu mesh sítí s důrazem na identifikaci bezpečnostních rizik a hrozeb spojených s touto topologií. Konkrétně se v práci zaměříme na zkoumání jednotlivých vlastností sítě včetně její struktury, na analýzu používaných technologií, jako jsou Wi-Fi, Bluetooth a Zigbee a jejich základní zabezpečení. Důležitou částí práce bude rozbor jednotlivých bodů a cílů zabezpečené sítě, včetně definování bezpečnostních hrozeb a výzev. V závěru práce bude provedena realizace bezdrátové mesh sítě a následně proběhne měření přenosové rychlosti a síly signálu v závislosti na okolních rušivých? signálech.

3. Metodika práce

Na základě literární rešerše, a to především ze zahraničních zdrojů, byla provedena analýza vlastností a struktury mesh sítí. Následně byly představeny a rozebrány jednotlivé používané technologie, jako jsou Wi-Fi, Bluetooth, ZigBee, včetně jejich základního zabezpečení. Poté byla provedena samotná bezpečnostní analýza. Nejdříve bylo potřeba si definovat jednotlivé cíle a body nezbytné k zajištění bezpečnosti sítě. V dalším kroku jsme pak mohli navázat na analýzu jednotlivých bezpečnostních výzev, jako jsou směrovací a DoS útoky. Závěrečná část práce je věnovaná praktickému měření. V kancelářských prostorách byla realizována testovací bezdrátová mesh síť, na níž se měřila přenosová rychlost a síla signálu. Následně byla realizována pomocná bezdrátová mesh síť, jež vysílala signál na podobné frekvenci a měla za úkol rušit naši testovanou síť.

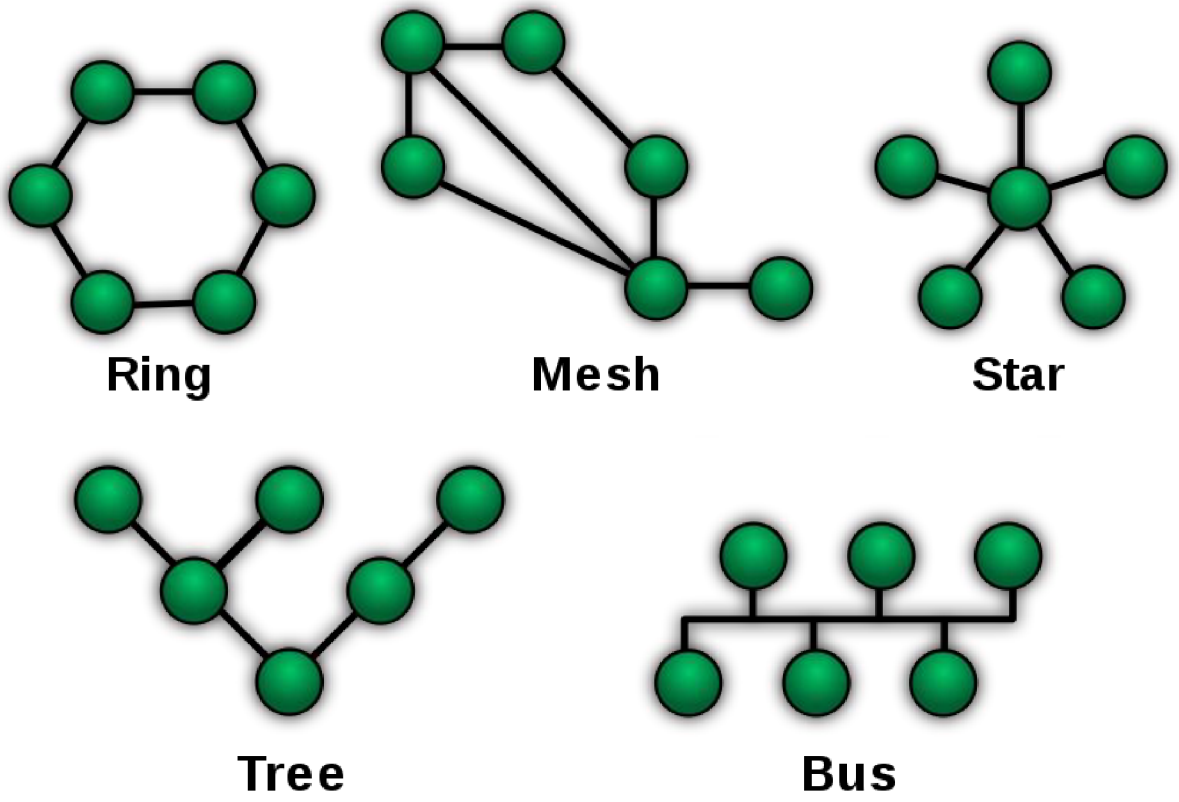
4. Základní charakteristika mesh sítě

Základním principem fungování mesh sítě je propojení uzlů do vzájemně propojené sítě, kde každý uzel může komunikovat přímo s jiným uzlem v jeho dosahu. Tato topologie sítě umožňuje datový tok různými cestami, jelikož každý uzel může fungovat jako prostředník pro přenos informací. Všechny uzly v mesh síti spolupracují na dynamickém směrování dat, tím se optimalizuje přenosová cesta a zvyšuje efektivita využití dostupných zdrojů. Svojí flexibilitou a komplexností se stává klíčovým prvkem v oblastech IoT a senzorových sítí.(2)

4.1 Topologie

Název mesh je odvozen z typu topologie těchto sítí, přičemž topologie sítě udává, jakým způsobem jsou jednotlivé uzly a zařízení propojeny a jak spolu komunikují. Mezi základní topologie řadíme – stromovou (tree), hvězdicovou (star), kruhovou (ring), sběrnicovou (bus) a v neposlední řadě smíšenou (mesh).

Obrázek 1: Schéma síťových topologií.(49)



4.1.1 Mesh topologie

Mezi hlavní charakteristiky mesh sítě patří možnost sebeorganizace a samokonfigurace, což znamená dynamicky reagovat na změny v topologii. Lze tak například přidat a odebrat prvek či uzel bez zásahu do konfigurace sítě. Při poruše nebo přetížení určité cesty je systém schopen automaticky vyhledat cestu novou. Možnost tvorby nových cest umožňuje rovnoměrně rozdělovat zátěž předávaných dat mezi jednotlivé uzly sítě.

Další výhodou mesh sítí je levná a jednoduchá škálovatelnost. Přidávání nových uzlů a zařízení, není na rozdíl od ostatních topologií složité. Stačí, když je nový prvek v dosahu již stávajícího signálu a má vlastnosti směrovače (router) a opakovače (relay). Pokud by většina zařízení tyto vlastnosti neměla, síť by ztratila schopnost dynamicky měnit a vytvářet cesty.(3,4)

5. Používané technologie.

Při návrhu a implementaci bezdrátových mesh sítí se využívá celá řada technologií, které zajišťují základní infrastrukturu pro propojení a komunikaci mezi uzly. Tyto technologie jsou klíčem k vytvoření robustních a spolehlivých sítí, schopných pokrýt různá prostředí a aplikace. Každá technologie má své vlastní výhody a nevýhody pro konkrétní nasazení. Jedním z nejpoužívanějších standardů je Wi-Fi (802.11), která poskytuje robustní bezdrátové připojení a umožňuje vytváření mesh sítí pomocí technologií. Tato technologie je díky své všudypřítomnosti a kompatibilitě s mnoha zařízeními široce dostupná a používaná v domácnostech i na veřejných místech. Další klíčovou technologií jsou Bluetooth sítě, které jsou ideální pro nasazení v IoT a chytrých domácnostech. Bluetooth umožňuje propojení velkého množství zařízení v jedné síti a poskytuje efektivní a spolehlivou komunikaci ve velkých prostorách. Dále se často používají standardy jako Zigbee a Z-Wave, které jsou oblíbené zejména v oblastech, kde je vyžadován velký počet uzlů a nízká spotřeba energie. Mezi tyto oblasti patří především průmyslové a senzorové sítě.

5.1 Wi-Fi (Standardy IEEE 802.11)

Jedná se o sadu standardů pro lokální bezdrátové sítě (WLAN), která je založena na standardech IEEE 802.11. Název je zkratka Wireless Fidelity, který překládáme do češtiny jako bezdrátová věrnost.(5)

Původním cílem Wi-Fi sítě bylo zajistit bezdrátové propojení dvou a více zařízení a následný přenos dat pomocí rádiových vln. Princip fungování spočíval v komunikaci mezi bezdrátovými zařízeními prostřednictvím přístupového bodu, tzv. Access Point. (6)

5.1.1 Jednotlivé verze standartu IEEE 802.11.

Jde o označení standardizačního institutu IEEE (Institute of Electrical and Electronics Engineers) – tento standard definuje bezdrátové sítě v nelicencovaném pásmu 2,4 GHz a 5 GHz. První standard byl vytvořen v roce 1997. Od té doby bylo vytvořeno nespočet dalších verzí, přičemž každá jednotlivá verze má různorodé parametry a je obohacena o novinky.(7,8)

Tabulka 1: Přehled základních standardů IEEE 802.11(8)

Standard	Rok vydání	Frekveční pásmo [GHz]	Maximální přenosová rychlost [Mbit/s]
Původní IEEE 802.11	1997	2,4	2
IEEE 802.11b	1999	2,4	11
IEEE 802.11a	1999	5	54
IEEE 802.11g	2003	2,4	54
IEEE 802.11n	2009	2,4;5	600
IEEE 802.11ax	2019	2,4;5	10 500 (Teoretická)

IEEE 802.11b (Wi-Fi 1)

Byl přijat v roce 1999. Stal se velice populárním a používaným převážně díky své kompatibilitě s původním standardem IEEE 802.11 a jednoduché implementaci. Využívá nelicencované frekvenční pásmo 2,4 GHz, které je sdílené s dalšími zařízeními, včetně Bluetooth technologií a mikrovlnnými troubami. Samotné pásmo 2,4 GHz je rozděleno do 14 kanálů, přičemž každý z nich má šířku pásma 5 MHz, s výjimkou čtrnáctého kanálu, který je vzdálen o 12 MHz od třináctého. V některých státech jsou povoleny pouze kanály od 1 do 11. V praxi se primárně využívají kanály 1, 6 a 11, aby se minimalizovaly interferenční problémy. Stejně jako u původního standardu IEEE 802.11 je zde používána modulace DSSS (Direct Sequence Spread Spectrum), jejíž hlavní výhodou je odolnost vůči rušení a interferenci. Maximální teoretická přenosová rychlost dosahuje 11 Mbps. V praxi se běžně dosahuje rychlosti kolem 4–6 Mbps a dosahu o vzdálenost 100 metrů. Zvýšená rychlost oproti původnímu standardu IEEE 802.11 je také způsobena použitím CCK (Complementary Code Keying).(7)

Tabulka 2: Kanály na frekvenčním pásmu 2,4 GHz (9)

Kanál	Frekvence [GHz]	Kanál	Frekvence [GHz]
1	2,412	8	2,447
2	2,417	9	2,452
3	2,422	10	2,457
4	2,427	11	2,462
5	2,432	12	2,467
6	2,437	13	2,472
7	2,442	14	2,487

IEEE 802.11a (Wi-Fi 2)

Doplněk IEEE 802.11a na rozdíl od IEEE 802.11 využívá frekvenční pásmo 5 GHz. Jedná se o licencované pásmo, které dosahuje výrazně vyšší rychlosti, a to až 54 Mbps. Mírnou nevýhodou je horší propustnost skrz fyzické překážky a dosah. Pro modulaci signálu je zde využívána technologie OFDM (Orthogonal Frequency-Division Multiplexing), jejíž hlavní výhodou není zvýšení přenosové rychlosti, ale rozdělení datového toku na více menších proudů, což umožňuje efektivnější využití frekvenčního pásma. Jelikož se jedná o licencované pásmo, některé kanály jsou sdílené s jinými bezdrátovými službami, jako jsou meteorologické a vojenské systémy.(7)

IEEE 802.11g (Wi-Fi 3)

Navazuje na IEEE 802.11a s rozdílem, že je určen pro frekvenční pásmo 2,4 GHz s šířkou pásma 20 MHz, stejně jako u IEEE 802.11b. Kombinuje tím svoje dva předchůdce a využívá jejich technologie. Je zde použita modulace OFDM a zároveň i DSSS za účelem kompatibility s IEEE 802.11b. Ze začátku využíval zabezpečení WEP (Wired Equivalent Privacy). Později se však doporučil přechod na bezpečnější protokoly, jako je například WPA (Wi-Fi Protected Access). Některá zařízení podporující standard 802.11g umožňují využívat technologii MIMO (Multiple Input Multiple Output), která zvyšuje přenosovou rychlost ve vícecestných prostředích.(7)

5.1.2 Zabezpečení dat na standartu IEEE 802.11

Šifrování dat je jeden z klíčových aspektů pro ochranu dat přenášených vzduchem mezi zařízeními a přístupovými body. V průběhu let bylo vyvinuto několik šifrovacích protokolů z důvodů neustále rostoucích požadavků na bezpečnost.

WEP (Wired Equivalent Privacy)

Jedná se o jeden z prvních šifrovacích protokolů určených k zabezpečení bezdrátových sítí. Hlavním cílem protokolu bylo poskytnout srovnatelné zabezpečení jako mají kabelové sítě. WEP pracuje na linkové vrstvě (Data Link Layer) a používá šifrovací algoritmus RC4 pro šifrování dat, který kombinuje klíč s náhodným inicializačním vektorem. Následnou slabinou je již zmíněný inicializační vektor, který má omezený počet kombinací, jelikož obsahuje pouze 24 bity. Tento protokol byl využíván hlavně ve verzích IEEE 802.11 a IEEE 802.11b, jelikož se tehdy jednalo o jediný způsob zabezpečení." (9,10)

WPA (Wi-Fi Protected Access)

Protokol sloužil jako náhrada za již nedostačující zabezpečení WEP. Objevuje se zde nový šifrovací protokol TKIP (Temporal Key Integrity Protocol), který zahrnuje řadu vylepšení, jako je například dynamická správa klíčů. Je zde používán 128bitový šifrovací klíč s 48bitovým inicializačním vektorem. Postupně byl protokol nahrazen novějšími verzemi, jako jsou WPA2 a WPA3.(9,10)

WPA2 (Wi-Fi Protected Access 2)

Jedná se o novější a výrazně bezpečnější verzi původního WPA protokolu. WPA2 přineslo pokročilejší šifrovací standard AES (Advanced Encryption Standard) s protokolem CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). AES umožňuje využívat klíče o délce 128, 192 a 256 bitů. WPA2 je považován za bezpečný protokol, což vedlo k tomu, že se postupně stal průmyslovým standardem, který je hojně využíván ve Wi-Fi sítích po celém světě(10,11)

WPA3 (Wi-Fi Protected Access 3)

Jedná se o nejnovější bezpečnostní standard pro šifrování bezdrátových sítí Wi-Fi, který byl vyvinut jako nástupce WPA2. Šifrování probíhá pomocí protokolu SAE (Simultaneous Authentication of Equals). Ten využívá tzv. metodu Diffie-Hellman Key Exchange, která

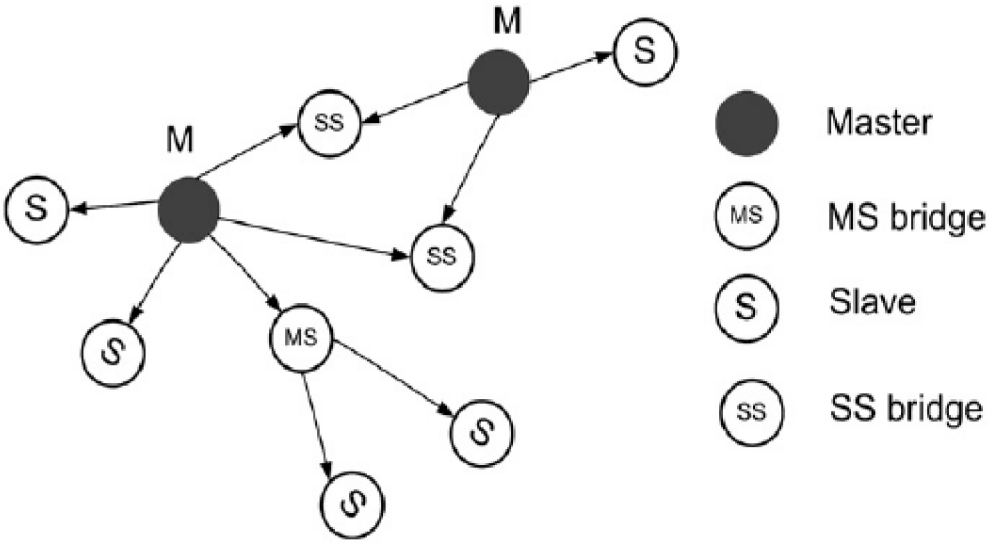
zajišťuje generování společného klíče mezi klientem a přístupovým bodem, aniž by byl vysílán přes síť ve své nezašifrované podobě. Dále standard obsahuje protokol OWE (Wi-Fi Enhanced Open with Opportunistic Wireless Encryption), který poskytuje základní zabezpečení veřejným sítím, které nevyžadují hesla. V neposlední řadě je ještě důležité zmínit protokol Wi-Fi Enhanced Open, který umožňuje bezpečné připojení uživatelů do veřejné sítě pomocí vygenerování jedinečného a dočasného klíče pro každé spojení.
WPA3 je primárně vhodný pro sítě, kde je vyžadována vysoká bezpečnost s vysokým počtem připojených zařízení. Z těchto důvodů se tento standard jeví jako ideální pro IoT a mesh sítě. Nevýhodou je vyšší pořizovací cena, jelikož je potřeba, aby všechny uzly tuto technologii podporovaly.(10,12)

5.2 Bluetooth

Název Bluetooth je odvozen z jména dánského krále Haralda I Modrozuba. Ten dokázal pomocí svých diplomatických schopností přesvědčit válečné kmeny k jednání o míru. Vývojáři se tím snažili dát najevo, že technologie Bluetooth, stejně jako kdysi Harald, má snahu o zjednodušení a provázaní vzájemné komunikace. Technologie byla vytvořena roku 1994 švédskou firmou Ericsson. Původně se jednalo o bezdrátovou náhradu za sériové drátové rozhraní RS-232. Bluetooth bylo standardizováno standardem IEEE 802.15.1. Bluetooth slouží primárně pro domácí a kancelářské aplikace. Samotný standard pak podporuje přenosy typu point-to-point (mezi dvěma body) a point-to-multi-point (mezi bodem a několika body). Systém Bluetooth pracuje v nelicencovaném pásmu 2,4 GHz, stejně jako některé Wi-Fi standardy. Frekvenční pásmo se nachází v rozmezí 2400,0-2483,5 MHz a je rozděleno do 79 kanálů, přičemž každý kanál má rozsah 1 MHz.

Struktura sítě se skládá z buněk nazvaných piconet. Piconet je základní komunikační buňka, která může být tvořena maximálně osmi zařízeními, přičemž jedno z nich funguje jako řídící jednotka (master) a ostatní jsou podřízené jednotky (slave). V každé buňce se vyskytuje pouze jedna řídící jednotka, která může svoji funkci za určitých podmínek předat jinému zařízení. Každé Bluetooth zařízení může fungovat jako řídící a zároveň podřízená jednotka, v tomto případě vzniká tzv. scatternet. Jde o vyšší organizační strukturu, kde je do sebe propojeno několik piconetů.(13,14)

Obrázek 2: Master-slave architektura (47)



Z důvodu potlačení interference s jinými signály je použita metoda tzv. kmitočtových skoků, s rychlostí 1600 skoků za sekundu. Všechna zařízení sdílejí hodiny své nadřazené jednotky. Sdílené hodiny mají dobu taktu 625 mikrosekund (µs), po uplynutí taktu se změní používaný kanál. To má za následek kvalitnější přenos dat a zároveň se zvyšuje bezpečnost přenosu, jelikož pouze odesílací a přijímací zařízení znají posloupnost použitých kanálů pro přenos. V neposlední řadě je signál zesílen pomocí symetrického zesilovače, podle výkonnostní třídy. (13)

Tabulka 3: Typy výkonnostních tříd

Třída	**Maximální povolený výkon**		**Přibližný dosah (bez překážek)**
	mW	**dBm**	
Třída 1	100	20	100 metrů
Třída 2	2,5	4	10 metrů
Třída 3	1	0	1 metr

5.2.1 Jednotlivé verze Bluetooth

Bluetooth 1.0

První verze 1.0 byla spuštěna v červenci 1999. Verze 1.0 měla mnoho nedostatků a problémů, včetně nedostatečné anonymity a bezpečnosti. Mimo jiné obsahovala povinné hardwarové adresy zařízení. Z dnešního pohledu se jedná již o zastaralou technologii.(15)

Bluetooth 1.1

V roce 2002 byl zavedena verze 1.1, která představovala vylepšení předchozí verze, včetně opravy značné části chyb. Byly definovány nové specifikace. Byla zde přidána podpora pro indikátor síly signálu (RSSI) a nešifrované kanály. Vyskytují se zde problémy s přiřazováním rolí master a slave.(16)

Bluetooth 1.2

Přidala se v roce 2003. Je zde zcela přepracovaná specifikace. Výrazně se zvýšila přenosová rychlost na 721 kbit/s. Verze byla vybavena rozhraním HCI (Host Controller Interface), rozšířením synchronního připojení ESCO a technologií Frequency Hopping, čímž se zvýšila bezpečnost a zabránilo se přetížení jednotlivých kanálů.(16)

Bluetooth 2.0

Byla uvedena v roce 2007. Největší změnou tohoto standardu byla podpora technologie EDR (Enhanced Data Rate), která využívá kombinaci modulací GFSK (Gaussian Frequency Shift Keying) a PSK (Phase Shift Keying Modulation), což ve výsledku znamenalo navýšení přenosové rychlosti na 2,2 Mbit/s. Další výhody byly snížení energetické spotřeby a nový způsob párování pomocí PIN kódu.(15)

Bluetooth 3.0

Bluetooth 3.0, označovaný také jako HS (High Speed), byl uveden v roce 2009. Byla zde primárně zvýšena přenosová rychlost, a to až na 24 Mbit/s. Na přenos dat jsou zde využity protokoly Wi-Fi (802.11). To mělo za následek zavedení mnoha nových funkcí, ale i navýšení energetické spotřeby.(15)

Bluetooth 4.0

Hned následující rok se představila verze 4.0. Byla zde poprvé představena úplně nová technologie nazývaná Bluetooth Low Energy, která podporovala všechny předchozí verze, lišila se však v počtu kanálů a jejich šířkách, v přidaných protokolech GATT a GAPP a ve snížené spotřebě energie. Jedná se také o počátek využívání Bluetooth technologie v průmyslu a ve zdravotnictví. V neposlední řadě byla verze obohacena přidáním nového šifrování AES-128.(17)

Bluetooth 5.0

Nový standard byl představen v roce 2016. Je zaměřený na zlepšení konektivity a podporu nově nastupující technologie IoT. Nejnovější verze Bluetooth 5.3 byla vydána v roce 2022 a zavedla podporu topologie mesh. Ačkoliv verze zatím není moc používaná, v budoucnu lze očekávat její hojnější využití.(18)

5.2.2 Zabezpečení dat na technologii Bluetooth

Bezpečnost Bluetooth zajišťují tři základní bezpečnostní složky: autentizace (ověření totožnosti komunikujících stran), autorizace (ověření a povolení přístupu ke službám) a důvěrnost (ochrana před odposloucháváním, data jsou doručována pouze důvěryhodným stranám).(19)

Párování

Aby mohla Bluetooth zařízení spolu komunikovat, je potřeba je nejdříve propojit, tento proces nazýváme párováním. Do obou zařízení zadáváme identický PIN, který obsahuje 8 až 128 bitů.(20)

Autentizace

Veškerý datový tok mezi důvěryhodnými zařízeními je řízen spojovacím klíčem. Spojovací klíč je 128bitové číslo, které se využívá pro prokazování identity. Klíč dělíme podle životnosti; trvalý lze používat opakovaně, zatímco dočasný se po ukončení aktuálního spoje vymaže.(19,20)

Šifrování

Pro každý přenášený paket se generuje šifrovací kód o velikosti 8 až 128 bitů. Na velikosti šifrovacího kódu se obě zařízení dohodnou. Kód se odvozuje z klíče spoje, náhodného čísla, adresy zařízení a hodnoty vnitřních hodin řídící jednotky.(21)

Frekvenční skoky

Metoda tzv. kmitočtových skoků původně nevznikla pro zlepšení bezpečnosti, ale pro potlačení interference s jinými signály. Přesto má pozitivní vliv na celkovou bezpečnost přenášených dat. Zařízení sdílejí hodiny své nadřazené jednotky, přičemž doba taktu je 625 mikrosekundy (µs). Po uplynutí taktu se změní používaný kanál, což má za následek kvalitnější přenos dat a zároveň to zvyšuje bezpečnost přenosu, jelikož pouze odesílací a přijímací zařízení znají posloupnost použitých kanálů pro přenos.(13)

5.2.3 Bluetooth Low Energy (BLE)

Jde o redukovanou a optimalizovanou verzi klasického Bluetooth BR (Basic Rate). Zatímco Bluetooth BR skáče mezi 79 kanály, Bluetooth Low Energy využívá pro komunikaci pouze 37 kanálů, přičemž další 3 kanály slouží čistě pro advertising. To zajišťuje rychlejší navázání spojení a zvyšuje energetickou efektivitu. Dále je šířka kanálu zvětšena na 2 MHz oproti původnímu 1 MHz u BR, což snižuje nároky na filtrování. Dosah signálu je oproti původnímu BT navýšený.

Standard BLE je založen na dvou základních profilech. GATT (Generic Attribute Profile) popisuje princip a způsob přenosu dat. GAP (Generic Access Profile) zase definuje vazby a spojení v topologii. Hierarchie je tu stejná jako u klasického Bluetooth s jediným rozdílem. K řídící jednotce (master) lze připojovat neomezené množství řízených jednotek. Jediné omezení je velikost pamětí řídících a řízených zařízrních.

Aby bylo možné připojit k řídící jednotce více zařízení, je zde využita funkce nazývaná advertising. Ta umožňuje řízeným jednotkám zaslat signál o tom, že mají v paměti data, která chtějí sdílet. Mezitím ostatní zařízení zjišťují pomocí funkce scanning, zda jsou daná data určena pro ně. Celý tento proces udržuje celou síť na minimální spotřebě energie; připojená zařízení se udržují v režimu spánku a jsou probuzena jenom v momentě, kdy je iniciována aktivní komunikace.

K napájení BLE jednotky obvykle postačí knoflíková baterie, která zde vydrží i několik let. Cenou za nízkou spotřebu u Bluetooth Low Energy je citelné omezení přenosu dat. Teoretická maximální přenosová rychlost se vyšplhá až na 1 Mbit/s. V praxi jsou však přenosové rychlosti nižší a pohybují se okolo 100 kbit/s.(22)

5.2.4 Zabezpečení dat na Bluetooth Low Energy

Zabezpečení u Bluetooth Low Energy je do určité míry podobné jako u ostatních verzí. Stejně jako u ostatních verzí Bluetooth, i zde je zabezpečení řešeno párováním, autentizací, šifrováním dat pomocí protokolu AES a frekvenčními skoky. Rapidním rozdílem je rozšíření zabezpečení o koncept LE Secure Connections. Tento koncept byl uveden ve verzi Bluetooth 4.2. Poskytuje bezpečnější způsoby výměny klíčů při párování, za pomocí metody ECDH (Diffie-Hellman).(23)

ECDH (Elliptic Curve Diffie-Hellman)

Jde o kryptografický algoritmus určený pro bezpečnou výměnu klíčů přes nezabezpečený kanál. Nejdříve je potřeba určit bod na eliptické křivce, který bude sloužit jako veřejný generátor. Poloha generátoru je veřejně známa a obě strany ho budou využívat. Následně si každé zařízení vygeneruje svůj vlastní náhodný soukromý klíč. Použitím soukromého klíče a veřejného generátoru se provede operace skalárního násobení na eliptické křivce k vytvoření veřejného klíče, který si zařízení vzájemně vymění. Po přijetí veřejného klíče od druhé strany, ho použije společně s vlastním soukromým klíčem k opětovnému vypočtení skalárního násobení na eliptické křivce. Výsledkem operace je bod na eliptické křivce, který obě strany použijí k odvození sdíleného hesla. I přestože útočník zná parametry eliptické křivky a veřejné klíče, nelze bez znalosti soukromých klíčů efektivně vypočítat sdílený tajný klíč. Díky těmto aspektům je metoda ECDH všeobecně považována za bezpečnou, na rozdíl od ostatních kryptografických algoritmů.(24)

5.3 Zigbee

Zigbee je bezdrátová komunikační technologie, která vznikla v roce 1999 a je využívána v sítích WPAN (Wireless Personal Area Network) a WSN (Wireless Sensor Network). Jedná se o vylepšenou verzi standardu IEEE 802.15.4, který obsahuje pouze dvě vrstvy, konkrétně fyzickou a MAC vrstvu. U Zigbee najdeme čtyři vrstvy: fyzickou, MAC, síťovou a aplikační. Celkově je protokol navržen tak, aby měl nízkou spotřebu energie a minimální

hardwarové požadavky, což má samozřejmě za následek malou přenosovou rychlost (250 kb/s). Dosah signálu se pohybuje v řádu několika stovek metrů. Hlavním důvodem vzniku byla snaha o vytvoření nízkoenergetické bezdrátové technologie, která by umožňovala monitorování, kontrolování a komunikaci mezi zařízeními. V roce 2002 vznikla společnost ZigBee Alliance, která se aktivně podílí na vývoji a spravování protokolu. Dále se na vývoji Zigbee podílí firmy, které se zaměřují na průmyslovou automatizaci, například Siemens, Philips, Samsung. V současné době má ZigBee Alliance přes 200 partnerských společností. (25–27)

Na rozdíl od Bluetooth pracuje Zigbee na více nelicencovaných frekvenčních pásmech. Pásmo 2,4 GHz obsahuje 16 kanálů s maximální přenosovou rychlostí 250 kb/s, pásmo 902-928 MHz poskytuje 10 kanálů s maximální přenosovou rychlostí 40 kb/s a pásmo 868-870 MHz obsahuje 1 kanál s maximální přenosovou rychlostí 2 kb/s. (25–27)

Struktura sítě

Síť Zigbee má dva základní typy zařízení – plně funkční zařízení (FFD – full function device) a zařízení se sníženou funkčností (RFD – reduced function device).

FFD zařízení obsahují veškeré služby standardu, včetně kompletního protokolového rámce, dále mohou komunikovat se všemi zařízeními, které jsou připojené do sítě. FFD může fungovat ve třech formách: ZigBee koordinátor (ZigBee Coordinator), Zigbee Router (ZigBee Router) nebo jako koncové zařízení (ZigBee End Device).

RFD slouží čistě jako koncové zařízení a jeho služby jsou omezeny, včetně přístupu k omezenému počtu protokolů, z důvodu omezení hardwarových a energetických nároků. Navíc RFD umí komunikovat pouze s FFD zařízeními.

Adresace je řízena pomocí tzv. EPID kódů. Jedná se o 64bitový binární kód, jeho zkrácená 16bitová varianta se nazývá PAN ID. Ta umožňuje v jedné síti udržovat až 65535 zařízení a slouží k rozlišení překrývajících se sítí ZigBee. (25–27)

ZigBee Koordinátor (ZigBee Co-ordinator) **-** Každá funkční síť musí obsahovat minimálně jeden koordinátor. Ten zajišťuje kompletní fungování sítě, včetně poskytování všech služeb, připojování a odpojování zařízení ze sítě a přidělování PAN ID. (28)

ZigBee Směrovač (ZigBee Router) – Funguje jako přemostění mezi koncovými zařízeními a koordinátorem. V případě, že koncové zařízení je mimo dosah koordinátoru, lze mezi ně přidat router, který bude přeposílat data a zvyšovat tak dosah sítě. (28)

ZigBee Koncové zařízení (ZigBee End Device) – Hlavním cílem je sbírání dat a následné odesílání do sítě. Díky svým nízkým hardwarovým požadavkům se jedná nejčastěji o sensory, či různá čidla. Jejich napájení probíhá pomocí baterii. (28)

5.3.1 Zabezpečení dat na technologii Zigbee

Bezpečnost na sítích Zigbee zajišťuje tzv. Trust Center. Jedná se o centrální zařízení, které je zodpovědné za kontrolu bezpečnosti, distribuci klíčů a kontrolu přístupu zařízení do sítě. Kromě toho mají sítě Zigbee v sobě zabudované opatření, které zajišťuje ochranu před rušením signálů od ostatních sítí stejného typu.

AES (Advanced Encryption Standard)

Standard je založen na principu symetrického šifrování, což znamená, že pro šifrování i dešifrování dat, se používá stejný klíč. Algoritmus pracuje s daty o velikosti 128 bitu a s délkou klíčů 128, 192 a 256 bitů. Větší délka klíče zajišťuje silnější bezpečnost šifrování, ale vyžaduje větší výpočetní výkon.

Standard AES nahradil dříve využívaný a v dnešní době nespolehlivý standard DES (Data Encryption Standard), jenž byl 64bitový, přičemž 8 bitů bylo kontrolních a 56 efektivních. Tento algoritmus byl lehce prolomitelný.(29,30)

Messege Timeout

Jedná se o funkci, která umožňuje odmítnout zprávy, kterým vypršel čas (timed-out messages). Zařízením můžou ignorovat příchozí data, která jsou nedůvěryhodná a tím zabránit případnému zahlcení. Jejich rozpoznávání funguje na základě sčítání velikosti rámce (A frame counter), který je přidán ke zprávě. Zařízení, které zprávu přijme, porovná hodnotu s hodnotou poslední přijaté zprávy, jestliže se hodnota shoduje, jedná se o opakovanou zprávu.(31)

Access Control Lists

Jde o soubor bezpečnostních mechanismů, které definují přístupová práva jednotlivým zařízením. ACL obsahují seznam identifikátorů, kterými řídí a spravují přístup ke službám sítě: čtení a zápis v síti, příjem dat a odesílání dat. Správně nastavená ACL zamezuje přístup nedůvěryhodných zařízení do sítě.(31)

6. Využití mash sítě

V posledních letech se mesh sítě stávají jednou z klíčových součástí moderních komunikačních infrastruktur. Využívají se zejména tam, kde je potřeba vysoká míra flexibility, jednoduchá škálovatelnost a možnost propojit velké množství zařízení. Uplatnění nachází mesh sítě v oblastech jako je průmysl, zemědělství, IoT, domácí automatizace (smarthome).

6.1 Mesh sítě v IoT

Mesh topologie hraje významnou roli v oblasti internetu věcí (IoT), a to především kvůli velkému počtu zařízení, která se v rámci těchto systémů musí mezi sebou propojit a komunikovat. V IoT se nacházejí různorodá zařízení, počínaje jednoduchými senzory, až po složité výpočetní systémy. Všechna tato zařízení potřebují efektivně sdílet data, a to mesh sítě nabízí. IoT (Internet of Things, česky Internet věcí) lze definovat jako síť fyzických objektů, které jsou spolu propojené pomocí internetu. Jednoznačná definice IoT neexistuje, každá společnost si ji vykládá odlišně. Za objekt můžeme považovat cokoliv, co dokáže, po přidání OS, sbírat a následně odesílat data ostatním zařízením na síti.

Jednou ze silných stránek topologie mesh v IoT je její robustnost a odolnost vůči chybám. Zařízení připojené k IoT, často pracují v dynamickém a nepředvídatelném prostředí, načež je po nich ještě požadován nepřetržitý provoz. Z těchto důvodů je zde klíčová robustnost a schopnost sebeorganizace a samokonfigurace. V případě, že jeden z uzlů selže, či ztratí spojení, mesh síť se autonomně rekonfiguruje a obejde poškozený uzel. Tím se zajistí nepřetržitý provoz sítě bez nutnosti manuálního zásahu. Další důležitá vlastnost v IoT je škálovatelnost. Sítě často obsahují velký počet zařízení, které neustále roste. Mesh topologie umožnuje rozšiřování sítě, bez výraznějšího snížení výkonu a bez zásadnějšího zásahu do infrastruktury. Tato schopnost je velice užitečná především v průmyslovém odvětví a rámci použití tzv. chytrých měst.

Dobrým příkladem mesh sítě v IoT je systém nazývaný chytrá domácnost (smarthome). V chytré domácnosti je připojeno mnoho zařízení jako jsou chytré spotřebiče, senzory, termostaty, osvětlení a bezpečností prvky. V případě, že dojde k výpadku určitého uzlu, změní se trasa toku dat na jiná zařízení. Další využití je v průmyslu, kde je třeba propojit tovární stroje, senzory a další systémy, aby bylo možné monitorovat a optimalizovat výrobu

v reálném čase. Zde se klade důraz na redundanci a různorodost cest, aby se zamezilo výpadku sítě a provoz mohl jet nepřetržitě.

6.2 Smarthome

Smarthome, neboli chytrá domácnost, představuje moderní koncept, jenž spojuje inovativní technologie s každodenním životem. Koncept chytrých domů se začal rapidně rozvíjet koncem 20. století. Původně se vztahoval čistě na moderní typ bydlení s automatizačními spotřebiči, v němž je omezena manuální práce člověka na minimum a jeho majitelům je poskytován co možná největší komfort. V dnešní době neexistuje přesná definice, co je to vlastně smarthome. M noho výrobců a poskytovatelů tzv. chytrých domů vnímá tuto novou technologii odlišně.

Ve zkratce však můžeme smarthome definovat jako obydlí či budovu, vybavenou výpočetní a informační technikou, která dynamicky reaguje na požadavky a potřeby svého uživatele. Celkově můžeme tyto technologie rozdělit do mnoha skupin: zabezpečení, pohodlí, enviromentální, finanční.

6.3 Průmysl 4.0

Průmysl 4.0 je označení pro současný trend automatizace a digitalizace. Výrobci integrují nové technologie, včetně IoT, cloudů a umělé inteligence, do svých výrobních procesů za účelem zefektivnění výroby. Továrny podporující průmysl 4.0 jsou vybaveny vestavěnými softwary, pokročilými senzory a robotikou, která má za úkol shromažďovat a vyhodnocovat data. Tyto technologie vedou k vyšší automatizaci výrobního závodu a zvýšené efektivitě výroby. Nahrazení manuální kontroly umělou inteligencí snižuje počet výrobních chyb, šetří peníze a čas.

7. Bezpečnost mesh sítě

S rostoucím využíváním internetové sítě a její aplikací, roste i bezpečnostní riziko. Není tedy divu, že každým rokem se zvyšují požadavky na zabezpečení soukromých, ale i veřejných sítí. Jak jsme již řekli v předešlé kapitole, mesh sítě se často objevují v průmyslových oblastech, komerčních budovách či v chytrých domech. Často přenášejí velké množství dat, které mohou být citlivá. Ať už se jedná o data zaměstnanců nadnárodní firmy, interní technologické postupy výrobního závodu nebo osobní údaje z vašeho smarthomu. Tyto citlivá data bývají velkým lákadlem pro potenciální útočníky, proto je potřeba dbát na kvalitní a správné zabezpečení každé mesh sítě.

V první řadě je potřeba se ujistit, že je naše mesh síť správně nakonfigurována. Důvod je prostý. Některé vlastnosti sítě, jako je samokonfigurace a samoorganizace, hrají významnou roli v zajištění dostatečné bezpečnosti. Správně fungující síť je schopna se dynamicky přizpůsobovat nevyžádaným změnám, jako jsou jednotlivé poruchy uzlů a tím zajišťovat nepřetržitý datový tok. Konfigurace tím přispívá k bezpečnosti a odolnosti vůči specifickým typům útoků, které se snaží narušit celkovou konektivitu sítě.

Stejné vlastnosti, které přispívají k bezpečnosti, však přinášejí i potenciální bezpečnostní rizika. Obzvláště je tento druh sítě náchylný na útoky typu Wormhole a Man in the middle. Decentralizovaná mesh síť například umožňuje útočníkovi využít tyto vlastnosti k vložení škodlivého uzlu do sítě. V případě, že síť nebude schopna vyhodnotit tento zásah jako bezpečnostní hrozbu, může nastat situace, kde přes škodlivý uzel začnou proudit data z ostatních uzlů, čímž se naskytne možnost útočníkovi všechna data odchytávat a pozměňovat.

7.1 Cíle a vlastnosti zabezpečené sítě

Dobře zabezpečená síť by měla splňovat tyto body: **Důvěrnost, integrita, autentizace, autorizace**, **dostupnost**. Je důležité si uvědomit, že všechny tyto vlastnosti jsou pro bezpečnost sítě nezbytné a je potřeba jim věnovat pozornost.(32)

Důvěrnost a ochrana

Jde o klíčovou ochranu přenášených dat před odposlechem a neoprávněným přístupem, která je zajištěna pomocí šifrovacích algoritmů. Ty převádějí nechráněná data do formy, kterou může dešifrovat pouze zařízení s odpovídajícím dešifrovacím klíčem. To zabrání

potenciálním útočníkům v přečtení obsahu dat v případě, že se jim je podaří odchytit. Jednotlivé šifrovací algoritmy se liší podle použité technologie (Wi-Fi, Bluetooth, ZigBee).(33)

Integrita

Jedná se o vlastnost, která zaručuje, že přenášená data nejsou neoprávněně nebo neúmyslně pozměněna, poškozena, ani s nimi během přenosu není manipulováno. Cílem je zajistit úplnost a správnost informací od jejich vytvoření, až po jejich doručení cílovému zařízení. K zajištění integrity se využívají digitální podpisy a tzv. kryptografické hash funkce, které ze vstupních dat libovolné délky, vytvářejí výstup o pevně dané délce.(33)

Autentizace

Proces, při kterém se ověřuje identita zařízení, uživatelů a uzlů před tím, než jim bude umožněn přístup do sítě. Než dojde k přijetí nebo odeslání dat, je potřeba prověřit, zda se na druhé straně komunikace nachází deklarovaný uživatel a nikoliv někdo, kdo se za uživatele pouze vydává. K těmto procesům se využívají sdílené klíče, digitální certifikáty PKI (Public Key Infrastructure) a v neposlední řadě autentizační protokoly, jako je EAP (Extensible Authentication Protocol).(34)

Autorizace

Na rozdíl od Autentizace neověřuje identitu uživatele, ale rozhoduje o úrovni oprávnění, které jsou uživatelům přidělena. Zamezuje tak přistup ke službám sítě uživatelům, kteří nemají potřebná oprávnění. Např. nastavení firemního notebooku, může měnit jen admin (PC Support). Pracovník používající daný notebook tyto práva nemá. Autorizace bývá často nasazovaná pomocí modelu RBAC (Role-based access control). Uživateli je přidělena role (Administrátor, uživatel, host) se specifickými oprávněními. To zajistí, že každé zařízení má přístup pouze k nezbytně nutným funkcím.(35)

Dostupnost

Schopnost sítě poskytovat uživatelům spolehlivé a nepřetržité služby. Tato vlastnost je z velké části dosažena správnou konfigurací sítě. Základem je samoorganizace, redundance uzlů a více cestné směrovaní. Uzel má kromě své původní cesty na výběr ještě alternativní možnosti směrovaní datového toku. V případě, že dojde k poruše uzlu, přes který byl veden původní datový tok, síť detekuje poruchu a změní trasu datového toku na nový uzel. Tím se

minimalizuje doba výpadku. Tyto vlastnosti přispívají k odolnosti sítě vůči DoS útokům.(33)

7.2 Typy útoků

7.2.1 Směrovací útoky

Jde o druh kybernetických útoků, které se zaměřují konkrétně na směrovací protokoly a procesy v síti. Směrovací protokoly mají zásadní význam pro určování optimálních cest, kterými se datové pakety pohybují v sítích, aby dosáhly svého cíle. Útokem na tyto protokoly mohou útočníci narušit, zachytit, upravit nebo zhoršit síťovou komunikaci. Tyto útoky jsou obzvláště nebezpečné pro ad-hoc a mesh sítě, kde je směrování dat dynamické.

Black-hole

Black-hole je typ síťové bezpečnostní hrozby, při níž útočník zneužívá směrovací protokoly sítě a falešně inzeruje, že má nejkratší cestu k cíli. To způsobí, že všechny datové pakety jsou směrovány směrem k útočníkovi, což mu umožní data zachytit, zmanipulovat nebo zahodit. Tento typ útoku je obzvláště nebezpečný v sítích typu mesh a v ad-hoc, které mohou být kvůli závislosti na dynamických směrovacích protokolech vůči takovému zneužití zranitelné.

Útok funguje tak, že útočník rozšíří ve směrovací síti informace, že má nejkratší nebo nejefektivnější cestu k určitému cíli. Jakmile je zjištěn požadavek na směrování ke koncovému zařízení, útočník odešle směrovací odpověď. Tato odpověď tvrdí, že má nejlepší trasu k cíli, i když tomu tak není. Ostatní uzly v síti, které tomuto tvrzení uvěří, začnou směrovat své datové pakety přes útočníka. To umožňuje útočníkovi odposlouchávat, upravovat nebo jednoduše zahazovat data.(36)

Worm-hole

Útok Worm-hole je typ síťového útoku, který se objevuje především v bezdrátových ad-hoc a mesh sítích. Tento útok spočívá v tom, že útočník zachytí datové pakety v jednom místě, přenese je alternativním komunikačním kanálem a pošle je zpět do sítě v jiném místě. Tento alternativní komunikační kanál je obvykle mnohem rychlejší než standardní síťové spojení a umožňuje útočníkovi předstírat, že dvě vzdálené části sítě jsou si velmi blízké.

Útok lze použít k narušení směrovacích protokolů manipulací s informacemi o tom, jak jsou uzly v síti propojeny. Útočník může přesměrovat síťový provoz přes sebe, což mu umožní odposlouchávat, měnit nebo blokovat data. To může vést k řadě bezpečnostních problémů, včetně úniku citlivých informací, narušení služeb nebo zneužití síťové infrastruktury k šíření škodlivého softwaru.(37)

Grey-hole

Na rozdíl od útoku blackhole, při kterém jsou odchytávány všechny pakety, je útok greyhole zákeřnější a obtížněji odhalitelný, protože útočník odchytává pakety pouze v určitou dobu nebo za určitých podmínek. To vyvolává dojem, že ztráta paketů je způsobena běžnými problémy sítě, nikoli útokem.

Útočník selektivně zahazuje nebo zadržuje určité pakety, zatímco ostatní data jsou předána dál v souladu s routingovými protokoly. To může vést k narušení síťové komunikace a ztrátě důležitých dat. Jelikož útočník neodchytává veškerá přijatá data, může být obtížnější útok detekovat. Útočník může například odchytávat pakety, které jsou důležité pro určité síťové operace nebo aplikace, zatímco méně důležitý provoz nechá projít.(36)

7.2.2 DoS (Denial of Service) útoky

DoS je typ útoku, při kterém se útočník snaží omezit či přerušit provoz sítě pro ostatní uživatele. Tyto útoky často zahlcují síť velkým množstvím dat a různých požadavků. To může spotřebovat šířku pásma a výpočetní zdroje uzlů do té míry, že požadavky ostatních uživatelů nemohou být zpracovány nebo jsou výrazně zpožděny, což narušuje běžný provoz sítě.(38,39)

Volume-based attacks (útoky založené na objemu)

Jde o kategorii DoS (Denial of Service) útoků, jejichž cílem je přetížit šířku pásma cílové sítě nebo serveru. Tyto útoky zahlcují cíl obrovským množstvím dat, čímž ztěžují nebo znemožňují přenos dat ostatních uživatelů. Hlavním cílem je zahltit kapacitu sítě, což vede k narušení služeb pro uživatele.(40)

- ICMP Flood (Ping Flood)

Útok ICMP flood, často nazývaný ping flood, spočívá v tom, že útočník posílá na cíl rychlý sled paketů ICMP Echo Request (ping). Objem požadavků zahltí cíl a znemožní mu je všechny zpracovávat, tím se spotřebovává příchozí i odchozí šířka pásma a může dojít ke zhroucení systému v důsledku vyčerpání zdrojů. (41)

- UDP Flood

Útočník odesílá velké množství paketů protokolu UDP (User Datagram Protocol) na náhodné porty cílového zařízení. Jelikož protokol UDP nevyžaduje k navázání spojení proces handshake, systém se tak automaticky snaží tyto požadavky zpracovávat a odpovídat na ně. To zapříčiní spotřebu šířky pásma a výpočetního výkonu na cílovém zařízení, což vede ke zhoršení nebo odepření služeb ostatním uživatelům.(42)

Protokol attacks (útoky na protokoly)

Zaměřují se na síťovou vrstvu, na které fungují internetové protokoly. Na rozdíl od Volume-based attacks, jejichž cílem je zahltit šířku pásma, se protokolové útoky zaměřují na zneužití slabých míst v samotných síťových protokolech a spotřebovávají prostředky serverů nebo kapacitu síťových zařízení, jako jsou firewally a vyrovnávače zátěže (load balancer). Tyto útoky mohou způsobit významné narušení provozu tím, že spotřebují všechna dostupná připojení, čímž se služby stanou nedostupnými pro běžné uživatele.(40)

- SYN Flood

Útok SYN flood zneužívá proces TCP handshake odesláním velkého množství TCP/SYN paketů, často s nepravou IP adresou, na port cíle. Server reaguje na každý pokus o navázání spojení odesláním odpovědi TCP/SYN-ACK a čeká na závěrečný ACK, který nikdy nedorazí, takže spojení zůstávají napůl otevřená, postupně se takto zahltí všechny dostupné porty.(43)

- Ping of Death (ping smrti)

Útok Ping of Death spočívá v odesílání chybných nebo nadměrně velkých paketů s cílem sabotovat cílový systém. Tyto pakety překračují maximální povolenou velikost. Maximální velikost je definována protokolem IP (65 535 bajtů) a způsobují chyby v cílovém softwaru, což může vést k pádu systému.(44)

Jamming attacks (rušivé útoky)

Jde o formu útoku, při níž útočník záměrně vysílá rušivé signály na stejných nebo blízkých frekvencích, které používá cílová síť. Tímto způsobem dochází k omezení nebo úplnému přerušení bezdrátové komunikace mezi uživateli sítě. Jamming útoky mohou být jak cílené, tak i neúmyslné, mezi neúmyslné rušení řadíme tzv. interferenci (45)

- Interference (neúmyslné rušení)

Interference je jedním z hlavních faktorů ovlivňujících spolehlivost a výkonnost bezdrátových sítí. Tento jev může být způsoben různými faktory a má potenciál vážně narušit nebo dokonce zablokovat komunikaci v bezdrátovém prostředí. Jedním z hlavních zdrojů rušení je přeplněné spektrum. S rostoucím počtem bezdrátových zařízení, jako jsou mobilní telefony, notebooky, chytré televizory a zařízení spadající do IoT, je spektrum stále více přeplněné. To vede k větší pravděpodobnosti kolizí signálů a rušení mezi různými zařízeními, což může vést ke zhoršení výkonu sítě. Dalším faktorem, který může způsobovat rušení, jsou fyzické překážky v prostředí, jako jsou zdi, budovy, stromy nebo jiné objekty. Tyto překážky mohou zeslabit signál nebo způsobit jeho odraz, což může vést k neočekávaným kolizím a rušení komunikace. Někdy může k rušení docházet také v důsledku elektromagnetického rušení z jiných zařízení nebo elektrických systémů, jako jsou vysílače, mikrovlnné trouby, elektrické vedení nebo elektronická zařízení. Tyto zdroje rušení mohou vyzařovat signály v bezdrátovém pásmu a ovlivňovat kvalitu komunikace v síti. Proti rušení lze použít různé strategie a techniky, jako je vícenásobný přístup s kódovým dělením (CDMA) nebo vícenásobný přístup s časovým dělením (TDMA), které umožňují účinné sdílení spektra mezi různými zařízeními. Je také důležité pečlivě naplánovat umístění a konfiguraci bezdrátových zařízení a používat techniky, jako je MIMO (Multiple Input Multiple Output) nebo formování paprsku, aby se minimalizoval dopad rušení a maximalizoval dosah a spolehlivost komunikace.

7.2.3 Man in the middle

Man in the Middle (MitM) je forma kybernetického útoku, kde útočník odposlouchává a někdy i upravuje komunikaci mezi dvěma stranami, které si myslí, že komunikují přímo mezi sebou. Podstata útoku MitM spočívá ve schopnosti útočníka, vmísit se do datového toku mezi dvě legitimní strany. Toho lze dosáhnout různými metodami v závislosti na

schopnostech útočníka a konkrétních zranitelnostech systému. Mezi běžné techniky patří např.:

RP Spoofing: Útočník manipuluje s protokolem ARP (Address Resolution Protocol) v síti takovým způsobem, aby byla MAC adresa útočníka přiřazena k IP adrese oběti, a tím byl veškerý provoz přesměrován na útočníka.

DNS Spoofing: Podvedení serveru DNS, aby název domény přeložil na IP adresu útočníka namísto legitimního serveru a přesměroval uživatele na škodlivé stránky.

Po získání kontroly může útočník odposlouchávat a zachytávat veškerá data předávaná mezi oběťmi, včetně přihlašovacích údajů, osobních informací a citlivých finančních údajů. Pokud jsou data zašifrována, může se je útočník pokusit dešifrovat pomocí různých technik nebo využít zranitelnosti v šifrovacím protokolu.(46)

8. Praktické ověření

Jak už bylo v předešlé kapitole zmíněno, jedním z hlavních bodů dobře zabezpečené sítě je tzv. dostupnost. Jedná se o schopnost sítě poskytovat uživatelům spolehlivé a nepřetržité služby. Námi vytvořená testovací mesh síť bude rušena pomocnou sítí s podobným frekvenčním rozsahem. Pro každé frekvenční pásmo se měří dvě veličiny: přenosová rychlost [mbit/s] a síla signálu [dB]. Následně se vyhodnotí chování sítě a porovnají se jednotlivé frekvence.

Testy vyhodnocují reakci sítě na vnější neúmyslné rušivé signály. Mezi tyto elementy patří především síťové signály o podobných frekvencích, které produkují okolní sítě, dále se může jednat o signály vyprodukované mikrovlnnou troubou či rádiem. Dále sem spadají také úmyslně vysílané signály za účelem omezit, popřípadě poškodit danou síť. Tyto útoky, při nichž útočník záměrně vysílá rušivé signály na stejných nebo blízkých frekvencích, jsou známé pod názvem Jamming attacks (rušivé útoky).

V neposlední řadě dojde k otestování útoku Man in the middle. Jednomu z používaných access pointů se vyresetuje nastavení a odebere se ze sítě. Při znovuzapnutí vyresetovaného access pointu se bude pomocí aplikace Wireshark sledovat, zda nedochází k nechtěnému odesílání paketů na již vyřazené AP

Měření probíhalo v kancelářských budovách na Olšanech, aby bylo simulováno co nejběžnější prostředí pro mesh sítě.

8.1 Frekvenční pásmo 2,4 GHz vs 5 GHz

Při vybírání vhodné frekvence pro bezdrátové mesh sítě je třeba zvážit několik klíčových faktorů. Každé frekvenční pásmo má své výhody a nevýhody, a proto jsou vhodné pro různé případy použití a prostředí.

Frekvenční pásmo 2,4 GHz je již mnoho let základním stavebním kamenem pro bezdrátové technologie, jako jsou Wi-Fi, Bluetooth a Zigbee. Jednou z jeho hlavních výhod je větší dosah ve srovnání s vyššími frekvenčními pásmy, jako je 5 GHz. Díky tomu je ideální pro zajištění pokrytí na velkých plochách nebo přes překážky, jako jsou zdi. Navíc mnoho starších zařízení stále podporuje pouze pásmo 2,4 GHz, takže zůstává relevantní pro zpětnou kompatibilitu. Frekvence 2,4 GHz je však také náchylnější k rušení jinými zařízeními, jako jsou mikrovlnné trouby, bezdrátové telefony či jiné bezdrátové sítě o podobných

frekvencích. To může vést k nižším rychlostem a méně spolehlivému připojení zejména v hustě obydlených oblastech, kde je spektrum přeplněné.

Na druhou stranu 5 GHz frekvenční pásmo nabízí vyšší rychlosti a méně frekvenčního rušení ve srovnání s 2,4 GHz. Díky většímu počtu dostupných kanálů a menšímu přetížení mohou 5 GHz sítě poskytovat vyšší výkon, a to zejména v prostředí s mnoha konkurenčními bezdrátovými signály. Díky tomu je pásmo 5 GHz vhodné pro aplikace, které vyžadují nízkou latenci a vysokou šířku pásma.

Kompenzací za tyto výhody je však kratší dosah. Signály s frekvencí 5 GHz nepronikají fyzickými překážkami (zdi, nábytek) tak dobře jako signály s nižší frekvencí, což omezuje jejich efektivní dosah.(47)

8.2 Návrh a realizace testované sítě

Router

Jako router je použit Netgate 1537 1U. Jedná se o síťový firewall a routovací zařízení vyvinuté společností Netgate. Firewall je poskytován softwarem pfSense. Dále je na routeru nastaven DHCP server a další základní parametry nezbytné pro základní fungování sítě.

Switch

Switch je od společnosti Cisco, konkrétně se jedná o model CBC 350. Je vhodný ke koordinaci síťového provozu. Díky technologii QoS (Quality of Service) nedochází k zahlcení switche, navíc můžeme určovat prioritu koncových zařízení. Nám bude sloužit pouze jako propojení routeru a AP.

Access Point

V síti jsou umístěny tři access pointy. Všechny AP jsou od firmy Ubiquiti. Konkrétně se jedná o model UniFi UAP-AC PRO. Řada modelů UniFi AC je navíc dělaná primárně pro bezdrátové meshové sítě. Modely podporují technologii 802.11ac a vysílají na frekvencích 2,4 GHz a 5 GHz. Z těchto důvodů se jeví jako ideální zařízení pro naši testovací mesh síť.

Nastavení AP probíhalo pomocí UniFi Site Manager, sloužící jako webové rozhraní pro správu a nastavení všech UniFi zařízení.

Obrázek 3: UniFi UAP-AC PRO(50)

8.3 Návrh a realizace rušící sítě

Rušící síť se skládá z routeru, switche a dvou access pointů. Model routeru je zde stejný jako u testované sítě a taktéž funguje jako firewall s DHCP serverem. Switch je od společnosti Cisco, model SG200-08.

Největší rozdíl oproti testované síti je v použití odlišných AP, konkrétně modelů Ubiquiti UniFi AP AC Mesh. I zde se jedná o access point specializovaný na nasazení do mesh sítě. Tento model se vyznačuje tím, že má externí antény, což by mělo mít za následek zvýšení intenzity signálu. Nastavení opět probíhalo pomocí UniFi Site Manager. Počet kanálů a jejich rozsah byl nastaven stejně jako u testované sítě. Simulace datového toku byla zajištěna pomocí aplikace WAN Killer od společnosti Solar Winds.

Obrázek 4: UniFi AP AC Mesh(51)

8.4 Měření přenosové rychlosti

Jak už bylo zmíněno, testování probíhalo v kancelářských prostorách, přičemž testovány byly dvě různé frekvence – 2,4 a 5 GHz. Rychlost byla měřena pomocí aplikace Speedtest by Ookla. Každá frekvence byla měřena celkem třikrát.

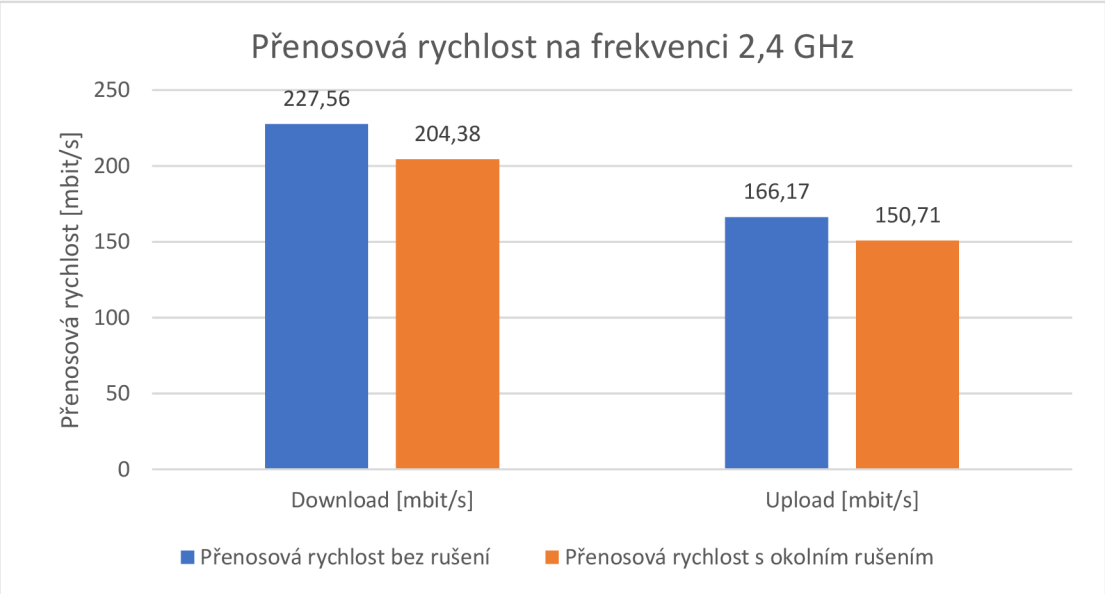
Tabulka 4: Přenosová rychlost bez okolního rušení

Přenosová rychlost bez okolního rušení						
Číslo testu	Test 1		Test 2		Test 3	
Frekvence sítě [GHz]	2,4	5	2,4	5	2,4	5
Download [mbit/s]	228,96	243,63	224,32	241,74	229,41	244,87
Upload [mbit/s]	166,00	183,21	165,96	181,39	166,55	183,04

Tabulka 5: Přenosová rychlost s okolním rušením

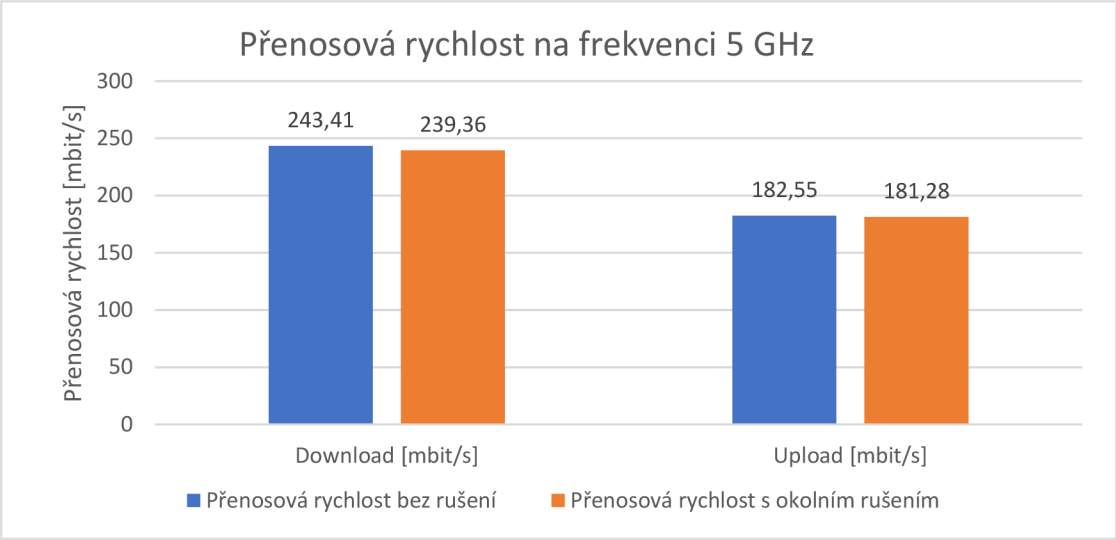
Přenosová rychlost s okolním rušením						
Číslo testu	Test 1		Test 2		Test 3	
Frekvence sítě [GHz]	2,4	5	2,4	5	2,4	5
Download [mbit/s]	207,78	239,28	203,46	240,14	201,89	238,65
Upload [mbit/s]	152,09	181,31	150,39	181,57	149,66	180,97

Obrázek 5: Přenosová rychlost s použitím frekvenčního pásma 2,4 GHz



Jak můžeme z grafu vyčíst, po zapojení rušící sítě klesla rychlost stahování o více než 13 mbit/s, to se v celkovém důsledku nejeví jako výrazný pokles, je však potřeba si uvědomit, že rušení signálu nezpůsobuje útočník, ale pouze sousední síť využívající podobné frekvence.

Obrázek 6: Přenosová rychlost s použitím frekvenčního pásma 5 GHz



U sítě s frekvencí 5 GHz je pokles minimální. Je to dané tím, že frekvence 5 GHz využívá širší pásmo signálu a více kanálů k přenosu dat.

8.5 Měření síly signálu

Dalším cílem našeho měření je sledovat sílu signálu a jeho chování. Signál se měří v decibelech [dB], a to hned z několika důvodů. Prvním důvodem je, že dB nabízí logaritmickou stupnici, která je obzvláště užitečná při práci se širokým rozsahem intenzity signálu. V telekomunikacích se signály mohou značně lišit, a to od extrémně slabých až po velmi silné. Použití logaritmické stupnice nám umožňuje zkomprimovat široký rozsah hodnot do námi přívětivější škály. Dále decibely poskytují spíše relativní než absolutní měření. To znamená, že namísto přímého měření síly signálu se měří poměr mezi dvěma signály. Například v případě měření síly přijímaného signálu vůči referenčnímu signálu nám dB umožňuje vyjádřit, kolikrát silnější, nebo slabší je přijímaný signál ve srovnání s referenčním. Toto relativní měření je výhodné, protože umožňuje snadnější porovnání různých signálů a eliminuje potřebu pevného referenčního bodu (48)

Pro naše měření jsou důležité dvě referenční hodnoty: 0 dB a –100 dB. 0 dB je

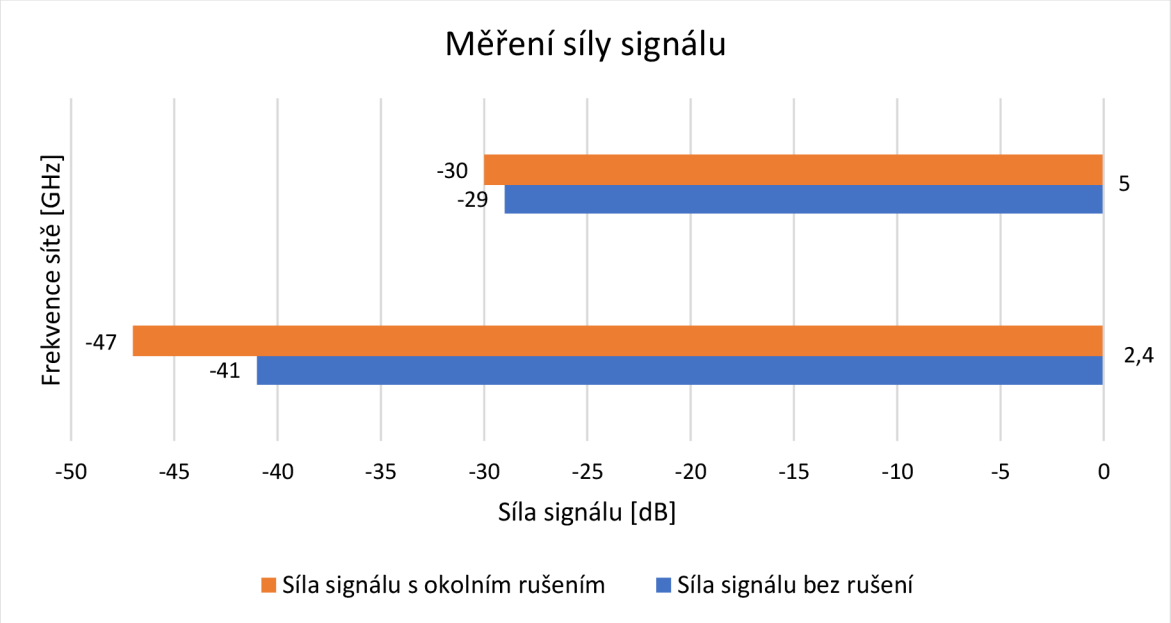
maximální možný signál, který jsou naše access pointy schopné vygenerovat, zároveň je však tento stav také defacto nedosažitelný, jelikož prostředí bez jakéhokoliv rušení není možné v našich podmínkách připravit. −100 dB je přesný opak předešlého signálu, jde o stav, při němž nelze navázat spojení s naším zařízením.

Měření probíhalo ve stejných podmínkách, jako tomu bylo u přenosové rychlosti. I zde se měřily dvě odlišné frekvence: 2,4 a 5 GHz. Měření probíhalo pomocí aplikací NetSpot a Vistumbler.

Tabulka 6: Síla signálu testované sítě

Frekvence sítě [GHz]	2,4	5
Síla signálu bez rušení [dB]	-41	-29
Síla signálu s okolním rušením [dB]	-47	-30

Obrázek 7: Měření síly signálu



Z měření vychází, že signál na frekvenci 5 GHz je výrazně vyšší. Zároveň je také odolnější vůči rušení.

8.6 Porovnání naměřených hodnot

Jak lze z grafu a tabulek vyčíst, testovaná síť, jež používá frekvenční pásmo 5 GHz, odolává rušivým signálům lépe. Je to především dané vlastnostmi použitého frekvenčního pásma. Frekvenční pásmo 5 GHz mělo k dispozici celkově 44 kanálů o šířce 40 MHz, zatímco pásmo 2,4 GHz pracovalo se 6 kanály o šířce 20 MHz.

.

Tabulka 7: Procentuální pokles přenosové rychlosti

Frekveční pásmo [GHz]	2,4	5
Download [mbit/s]	10,19 %	1,66 %
Upload [mbit/s]	9,30 %	0,70 %

Pokud pomineme úvodní interferenci, jež je působena náhlou změnou vytíženosti kanálů, jeví se nám jako stabilnější frekvenční pásmo 5 GHz. Procentuální pokles přenosové rychlosti zde dosáhl u downloadu 1,66 % a 0,7 % u uploadu. Tento pokles lze považovat za zanedbatelný.

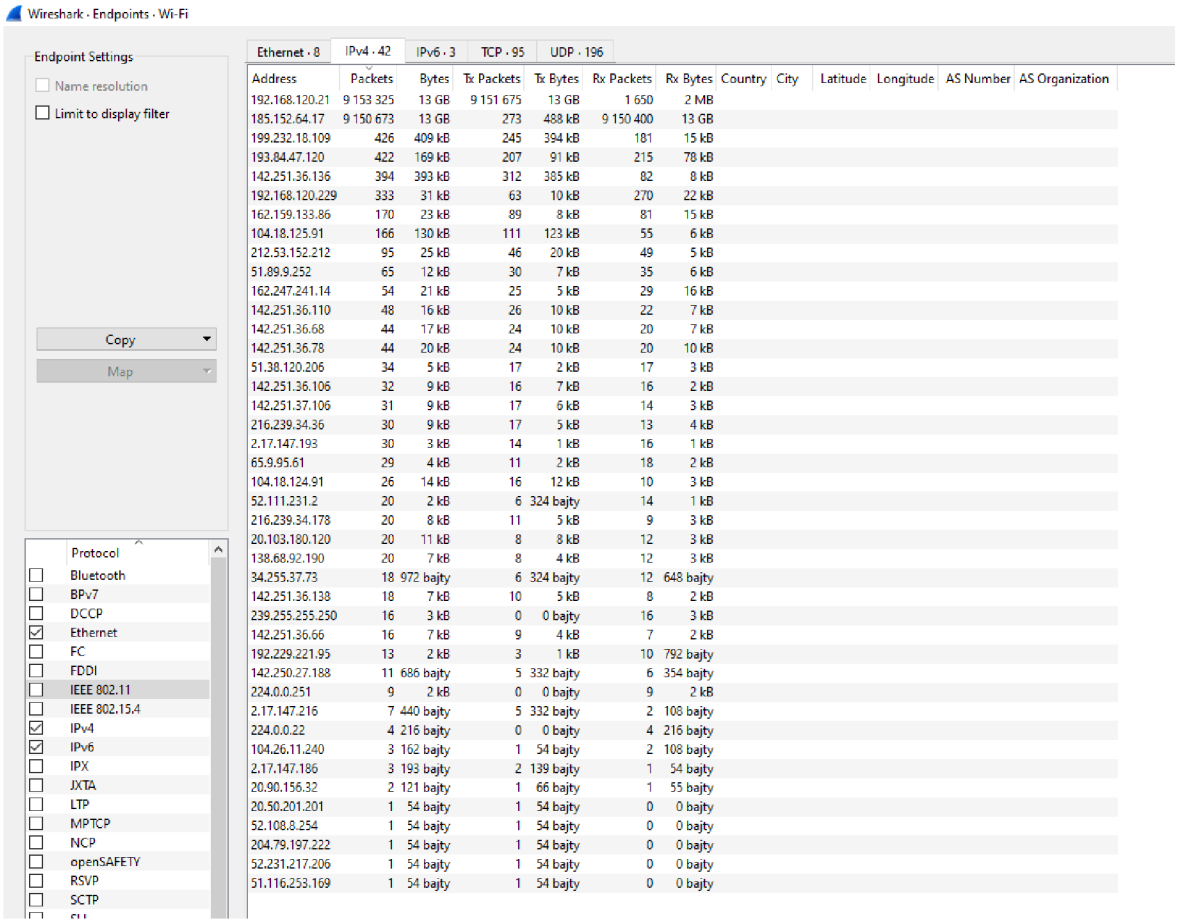
U frekvenčního pásma 2,4 GHz byl výsledek znatelně horší, u downloadu jsme zaznamenali pokles o 10,19 % a u uploadu 9,30 %. Síla signálu frekvenčního pásma 5 GHz klesla pouze o jeden decibel, zatímco u frekvence 2.4 GHz byl pokles 6 decibelů.

8.7 Testování útoku Man in the middle

Poslední část testů spočívala ve vyresetování jednoho z používaných access pointů a následném trackování přenášených packetů.

Jeden z AP byl vyresetován a odebrán ze sítě. Následně byl znovu zapnut a bez konfigurace se nechal na prázdno běžet. V případě, že by testovaná síť byla špatně nakonfigurována, hrozilo by, že vyresetované AP se připojí do sítě i bez vědomí administrátora. V okamžiku, kdy by se to opravdu stalo, se stává ze zařízení bezpečnostní hrozba. Potenciální útočník by mohl jednoduše využít připojené zařízení k odposlouchávání či upravování datového toku.

Obrázek 8: Software WireShark



Samotný test proběhl hladce. Po znovuspuštění odebraného AP probíhaly pokusy o znovupřipojení zařízení. Síť však při každém pokusu vyžadovala schválení od administrátora sítě. Schválení se mohlo potvrdit buď pomocí příkazů v příkazovém řádku, nebo na již zmíněném webovém rozhraní UniFi Site Manager.

Během celé doby trvání testu nebyly zaznamenány žádné pakety směřující do vyresetovaného access pointu.

9. Závěr a doporučení

Je důležité si uvědomit, že žádná síť není stoprocentně bezpečná, a proto je nezbytné minimalizovat rizika a maximalizovat její odolnost vůči potenciálním útokům. Toho lze dosáhnout kombinací technických opatření, vzděláváním uživatelů a pravidelným hodnocením zabezpečení. V případě, že mesh síť využívá technologii Wi-Fi, je doporučeno využít šifrovací protokol WPA3 i za cenu vyšších nákladů. Bezpečnostní protokol WPA2, jenž byl na Wi-Fi sítích dlouho považován za spolehlivý standard, se nyní stává postupně zranitelným. Nedostatek některých bezpečnostních prvků, jako jsou slabiny v šifrování, činí standard WPA2 náchylným k potenciálním útokům. WPA3 naopak přináší řadu pokročilých bezpečnostních mechanismů, které jsou klíčové pro odolnost sítě proti moderním hrozbám. Přechod na WPA3 je proto nejen doporučený, ale pro specifické sítě vyžadující vyšší zabezpečení i nezbytný.

Z analýzy bezpečnostních hrozeb vyplývá, že největší hrozbou pro mesh sítě zůstávají klasické směrovací útoky jako Wormhole, Blackhole, Greyhole. Dále velkou část hrozeb pokrývají DoS (Denial of Service) útoky. Za zmínku stojí také útok Man in the Middle, který je v tomto typu sítě obzvláště nebezpečný.

Z praktického měření lze vyčíst, jakým dynamickým způsobem se síťové odvětví vyvíjí. Zatímco před 15 lety by nám okolní signály mohly pomocí interference defacto znemožnit připojení na síť, dnes je technologie na takové úrovni, že za pomoci správně zvoleného frekvenčního pásma a správného nastavení sítě lze dosáhnout snížení okolního rušení na minimální hodnotu. Z testů vyplývá, že interference na frekvenčním pásmu 5 GHz byla skoro nulová, zatímco na frekvenčním pásmu 2,4 GHz došlo k mírnému poklesu přenosové rychlosti a síly signálu.

Byť se data jednoznačně přiklání k použití 5GHz frekvenčnímu pásmu, rozhodně se nejedná o všeobecné doporučení. Důvod, proč z měření vyšlo 5 GHz pásmo lépe, je ten, že testování probíhalo v jedné místnosti, signál tak nemusel překonávat fyzické překážky, jako jsou zdi. Všeobecně se doporučuje používat frekvenční pásmo 5 GHz zejména v prostředí s mnoha konkurenčními bezdrátovými signály, 2,4 GHz lze aplikovat do míst, kde je zvýšený výskyt fyzických překážek a kde je vyžadován vysoký dosah signálu.

Testování útoku man in the middle proběhlo úspěšně. Žádné pakety nebyly na vyresetovaný access point odeslány. Ten se sice pokoušel připojit zpět do sítě, ale neúspěšně.

10. Seznam použitých zdrojů

1. Kuo FF. Computer Networks—The ALOHA System. J Res Natl Bur Stand (1934) [Internet]. listopad 1981 [citován 24. březen 2024];86(6). Dostupné z: /pmc/articles/PMC6753009/
2. Časopis Automa Bezdrátové sítě typu mesh [Internet]. [citován 31. březen 2024]. Dostupné z: https://automa.cz/cz/casopis-clanky/bezdratove-site-typu-mesh-2005_12_30826_1141/
3. Fonseca CN, Técnico IS. Multipath Routing for Wireless Mesh Networks.
4. Ju HJ, Rubin I. Mesh Topology Construction for Interconnected Wireless LANs. 2005 [citován 17. březen 2024]; Dostupné z: https://websrv.cecs.uci.edu/~papers/secon05/DATA/07-03.PDF
5. IEEE SA - The Evolution of Wi-Fi Technology and Standards [Internet]. [citován 17. březen 2024]. Dostupné z: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/
6. The Evolution of Wi-Fi networks: from IEEE 802.11 to Wi-Fi 6E [Internet]. [citován 17. březen 2024]. Dostupné z: https://www.wevolver.com/article/the-evolution-of-wi-fi-networks-from-ieee-80211-to-wi-fi-6e
7. Banerji S, Chowdhury RS. On IEEE 802.11: Wireless LAN Technology. Original Publication: International Journal of Mobile Network Communications & Telematics (IJMNCT) [Internet]. 2013 [citován 17. březen 2024];3(4). Dostupné z: http://arxiv.org/abs/1307.2661
8. Ergen M. IEEE 802.11 Tutorial. 2002 [citován 17. březen 2024]; Dostupné z: http://ayman.elsayed.free.fr/msc_student/wlan-tutorial.pdf
9. Lashkari AH, Danesh MMS, Samadi B. A survey on wireless security protocols (WEP,WPA and WPA2/802.11i). Proceedings - 2009 2nd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2009. 2009;48–52.
10. Indira Reddy B, Srikanth V. Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2019 IJSRCSEIT | [Internet]. 2019 [citován 17. březen 2024];5(10):2456–3307. Dostupné z: https://doi.org/10.32628/CSEIT1953127
11. AKM Nazmus Sakib B, Ahmed S, Rahman S, Mahmud I, Habibullah Belali M, Nazmus Sakib α A, et al. WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis & Improvement WPA 2 Wi-Fi Protected Access 2 Security Enhancement Analysis Improvement WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis & Improvement. Type: Double Blind Peer Reviewed International Research Journal Publisher: Global Journals Inc [Internet]. [citován 17. březen 2024];12. Dostupné z: https://d1wqtxts1xzle7.cloudfront.net/25969914/2093118344f4387fa3c1cb3.52441134-libre.pdf?1390870022=&response-content-disposition=inline%3B+filename%3DWPA_2_Wi_Fi_Protected_Access_2_Security.pdf&Expires=1710709932&Signature=HL6H~3iHzlCi7TMaEdUlM0WUD3~-SkVG09ovpeXT8267YRhkNpYf36gYfzr9GkRrRzUCqr5swXUHk1srX7uj7dxSbjZpe-TfeFQuOe9d99~MM3Y3ah1m2sASzhnp2i7VMnD8dv24Aw7zbDUW9CFJDxoik8ZDuAft936t1DUJ~HjiPWMG~VvP8i5hu2vbOIgymioa6lXC82kMThXgSEkLiLSLLxoRGM461ZtJCqgq8kQ8oQ~xNAnUf09~X60Oc8jCOBRz-Y9qqP-REK~4hx9

12. Kohlios CP, Hayajneh T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. Electronics 2018, Vol 7, Page 284 [Internet]. 30. říjen 2018 [citován 17. březen 2024];7(11):284. Dostupné z: https://www.mdpi.com/2079-9292/7/11/284/htm
13. Zeadally S, Siddiqui F, Baig Z. 25 Years of Bluetooth Technology. Future Internet 2019, Vol 11, Page 194 [Internet]. 9. září 2019 [citován 10. březen 2024];11(9):194. Dostupné z: https://www.mdpi.com/1999-5903/11/9/194/htm
14. Wang H. Overview of Bluetooth Technology. 2001 [citován 17. březen 2024]; Dostupné z: https://d1wqtxts1xzle7.cloudfront.net/47176358/Bluetooth_Overview-libre.pdf?1468301943=&response-content-disposition=inline%3B+filename%3DOverview_of_Bluetooth_Technology.pdf&Expires=1710716332&Signature=W-fzFASob2aeBBbjAQYr1YSS8Apb4kCpRmOvyvg4fws4seSgNQ1s7vdOUaTw5tFylZKLmEMIf5Su5acWBPr46Z1VnQpruqqE7jELQvaTqvQQwrTp0ItRY0HAX5WXZDhvxHfkbizkQMEj-jOHp3W4-N4LFPko07tdrtFHayRwwAS3Xe2J56KGwCkWnEdlSDAayv5GuRcEMP2zmD7KdMzTp0848Rk-UtoSZvuxF-O33fSKQTsac-EjcRtl~N7t5GGi2UXDHrZB9ngeBNcpMRgXuHGDDOQdzeVK41z-VU~J
15. Jaké jsou rozdíly ve verzích Bluetooth 1.0 až 5.0? [Internet]. [citován 17. březen 2024]. Dostupné z: https://xm.cz/blog/jake-jsou-rozdily-ve-verzich-bluetooth-1-0-az-5-0/
16. Křenek R. Bluetooth Hi-Fi audio systém. MASARYKOVA UNIVERZITA FAKULTA INFORMATIKY [Internet]. 2015 [citován 20. březen 2024]; Dostupné z: https://is.muni.cz/th/d0tjq/Bluetooth_Hi-Fi_audio_system.pdf
17. How GAP and GATT Work - Punch Through [Internet]. [citován 30. březen 2024]. Dostupné z: https://punchthrough.com/how-gap-and-gatt-work/
18. Bluetooth 5: everything you need to know | What Hi-Fi? [Internet]. [citován 20. březen 2024]. Dostupné z: https://www.whathifi.com/advice/bluetooth-5-everything-you-need-to-know
19. Lonzetta AM, Cope P, Campbell J, Mohd BJ, Hayajneh T. Security Vulnerabilities in Bluetooth Technology as Used in IoT. Journal of Sensor and Actuator Networks 2018, Vol 7, Page 28 [Internet]. 19. červenec 2018 [citován 17. březen 2024];7(3). Dostupné z: https://www.mdpi.com/2224-2708/7/3/28/htm
20. Scarfone K, Padgette J. Special Publication 800-121 Guide to Bluetooth Security Recommendations of the National Institute of Standards and Technology.
21. Be-Nazir N, Minar I, Tarique M. BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY. International Journal of Distributed and Parallel Systems (IJDPS. 2012;3(1).
22. Afaneh M. INTRO TO BLUETOOTH LOW ENERGY. 2018;
23. Padgette J, Bahr J, Batra M, Holtmann M, Smithbey R, Chen L, et al. NIST Special Publication 800-121 Revision 2 Guide to Bluetooth Security. [citován 17. březen 2024]; Dostupné z: https://doi.org/10.6028/NIST.SP.800-121r2-upd1
24. Haakegaard R, Lang J. The Elliptic Curve Diffie-Hellman (ECDH). 2015 [citován 17. březen 2024]; Dostupné z: http://koclab.cs.ucsb.edu/teaching/ecc/project/2015Projects/Haakegaard+Lang.pdf
25. Malhotra J. Simulation Analysis of Tree and Mesh Topologies in Zigbee Network. International Journal of Grid Distribution Computing [Internet]. 2015 [citován 17. březen 2024];8(1):81–92. Dostupné z: http://dx.doi.org/10.14257/ijgdc.2015.8.1.08

26. Ranjeet Kumar P, Narayana Rao P. Wireless Networking Through ZigBee Technology. International Journal of Advanced Research in Computer Science and Software Engineering [Internet]. 2012 [citován 17. březen 2024];2(7). Dostupné z: www.ijarcsse.com
27. Introduction to Zigbee Technology. [citován 17. březen 2024]; Dostupné z: https://eclass.uoa.gr/modules/document/file.php/DI367/%CE%A5%CE%BB%CE%B9%CE%BA%CF%8C/introduction-to-zigbee-technology.pdf
28. Schumacher S, Pfeiffer R, Zillner T. Magdeburger Journal zur Sicherheitsforschung The good, the bad and the ugly. [citován 17. březen 2024]; Dostupné z: http://www.sicherheitsforschung-magdeburg.
29. Muhammad Abdullah A, Muhamad Abdullah A. Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. 2017 [citován 17. březen 2024]; Dostupné z: https://www.researchgate.net/publication/317615794
30. Advanced Encryption Standard. [citován 17. březen 2024]; Dostupné z: https://leocontent.umgc.edu/content/dam/course-content/tgs/cst/cst-620/document/AdvancedEncryptionStandard.pdf
31. Kyselý T. Univerzální bezdrátový komunikační spoj pomocí ZigBee modulů [Internet]. Vysoké učení technické v Brně. Fakulta elektrotechniky a komunikačních technologií; 2018 [citován 17. březen 2024]. Dostupné z: http://hdl.handle.net/11012/33087
32. Zhang W, Wang Z, Das SK, Hassan M. Security Issues in Wireless Mesh Networks. [citován 18. březen 2024]; Dostupné z: https://www.cse.unsw.edu.au/~mahbub/PDF_Publications/mesh_2008.pdf
33. What is the CIA Triad? | Definition from TechTarget [Internet]. [citován 25. březen 2024]. Dostupné z: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA
34. Zulkarnain S, Idrus S, Cherrier E, Rosenberger C, Schwartzmann JJ. A Review on Authentication Methods. Aust J Basic Appl Sci [Internet]. 31. březen 2013 [citován 25. březen 2024];7(5):95–107. Dostupné z: https://hal.science/hal-00912435
35. Understanding Authentication, Authorization, and Encryption : TechWeb : Boston University [Internet]. [citován 25. březen 2024]. Dostupné z: https://www.bu.edu/tech/about/security-resources/bestpractice/auth/
36. Kaur R, Singh P. REVIEW OF BLACK HOLE AND GREY HOLE ATTACK. The International Journal of Multimedia & Its Applications (IJMA). 2014;6(6).
37. Hu YC, Perrig A, Johnson DB. Wormhole Attacks in Wireless Networks. IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS [Internet]. 2006 [citován 18. březen 2024];24(2). Dostupné z: https://www.cs.rice.edu/~dbj/pubs/jsac-wormhole.pdf
38. What is a denial-of-service (DoS) attack? | Cloudflare [Internet]. [citován 18. březen 2024]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/
39. What is a denial of service attack (DoS) ? - Palo Alto Networks [Internet]. [citován 18. březen 2024]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos
40. Three Types of DDoS Attacks| ThousandEyes [Internet]. [citován 18. březen 2024]. Dostupné z: https://www.thousandeyes.com/blog/three-types-ddos-attacks
41. What is a Ping Flood | ICMP Flood DDoS Attack | Imperva [Internet]. [citován 18. březen 2024]. Dostupné z: https://www.imperva.com/learn/ddos/ping-icmp-flood/

42. UDP flood DDoS attack | Cloudflare [Internet]. [citován 18. březen 2024]. Dostupné z: https://www.cloudflare.com/learning/ddos/udp-flood-ddos-attack/
43. SYN flood DDoS attack | Cloudflare [Internet]. [citován 18. březen 2024]. Dostupné z: https://www.cloudflare.com/learning/ddos/syn-flood-ddos-attack/
44. What is Ping of Death (PoD) | Prevention & Mitigation Methods | Imperva [Internet]. [citován 18. březen 2024]. Dostupné z: https://www.imperva.com/learn/ddos/ping-of-death/
45. Li C, Wang Z, Yang C. Secure routing for wireless mesh networks. International Journal of Network Security [Internet]. 1. září 2011 [citován 18. březen 2024];13(2). Dostupné z: https://www.researchgate.net/publication/48202679_Secure_Routing_in_Wireless_Mesh_Networks
46. What is MITM (Man in the Middle) Attack | Imperva [Internet]. [citován 18. březen 2024]. Dostupné z: https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/
47. 2.4 GHz vs. 5 GHz vs. 6 GHz: What's the Difference? - Intel [Internet]. [citován 31. březen 2024]. Dostupné z: https://www.intel.com/content/www/us/en/products/docs/wireless/2-4-vs-5ghz.html
48. Why is almost everything negative in Wireless? - Cisco Community [Internet]. [citován 20. březen 2024]. Dostupné z: https://community.cisco.com/t5/small-business-support-knowledge-base/why-is-almost-everything-negative-in-wireless/ta-p/3159743
49. Network topology - Simple English Wikipedia, the free encyclopedia [Internet]. [citován 18. březen 2024]. Dostupné z: https://simple.wikipedia.org/wiki/Network_topology
50. Ubiquiti UniFi UAP-AC-PRO - WiFi Access Point | Alza.cz [Internet]. [citován 31. březen 2024]. Dostupné z: https://www.alza.cz/ubiquiti-unifi-uap-ac-pro-levne-d4202360.htm
51. Ubiquiti UniFi AP AC Mesh - WiFi Access Point | Alza.cz [Internet]. [citován 31. březen 2024]. Dostupné z: https://www.alza.cz/ubiquiti-unifi-ap-ac-mesh-d4848610.htm