VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Denys Partnov

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

SONDA PRO PASIVNÍ ODPOSLECH STANDARDU IEEE 802.11

PASSIVE CAPTURING PROBE FOR IEEE 802.11 STANDARD

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Denys Partnov**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Jan Pospíšil**
SUPERVISOR

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Denys Partnov ***ID:*** 206683

Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Sonda pro pasivní odposlech standardu IEEE 802.11

POKYNY PRO VYPRACOVÁNÍ:

Student se zaměří na standard IEEE 802.11 pro rodinu bezdrátových protokolů. Bude provedena potřebná analýza jednotlivých vrstev komunikace tak, aby bylo možné tyto informace následně využít pro praktickou část. Následně se student zaměří na možnosti a metody pasivního odposlechu, kde budou analyzovány převážně dostupné hardwarové možnosti. Na základě podloženého výběru pak bude provedena implementace a rozsáhlé testování pro nejčastěji využívané protokoly rodiny IEEE 802.11. Praktická část tak bude obsahovat samotnou implementaci, testování a výslednou optimalizaci pasivní sondy pro odposlech a to na frekvencích 2,4 i 5 GHz. Z naměřených dat budou vytvořeny statistiky a bude prokázáno úspěšné zachytávání pomocí srovnání jednotlivých provozů (zachyceného a regulérního).

DOPORUČENÁ LITERATURA:

[1] GONG, Michelle, Brian HART a Shiwen MAO. Advanced Wireless LAN Technologies: IEEE 802.11AC and Beyond. GetMobile: Mobile Computing and Communications [online]. ACM, 2015, 18(4), 48-52 [cit. 2019-09-15]. DOI: 10.1145/2721914.2721933. ISSN 15591662.

[2] RIGELSFORD, Jon. 802.11 Wireless Networks: The Definitive Guide. Sensor Review [online]. Emerald Group Publishing Limited, 2003, 23(2) [cit. 2019-09-15]. DOI: 10.1108/sr.2003.08723bae.003. ISSN 0260-2288.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: Ing. Jan Pospíšil

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Bakalářská práce se zabývá obecným popisem protokolu 802.11, kde jsou vysvětleny a popsány jednotlivé vrstvy, na kterých protokol pracuje. Pozornost byla zaměřena i na možnosti zabezpečení bezdrátového provozu. Praktická část se pak zabývá tvorbou kompletního nástroje pro pasivní odposlech provozu v sítích IEEE 802.11. Kde jde zejména o zpracování statistik provozu. Výsledný program, napsaný v jazyce Python, umožňuje uživateli zobrazovat aktuání informace typu: počet přenesených rámců, kanál, pásmo, síla přijímaného signálu a jiné. Následně je možné výsledky zobrazovat v podobě grafů. V rámci testovacího měření byla ověřena správná funkčnost programu.

KLÍČOVÁ SLOVA

Sonda, Pasivní odposlech, IEEE 802.11

ABSTRACT

The bachelor's thesis deals with a general description of the 802.11 protocol, where the individual layers on which the protocol works are explained and described. Attention was also focused on the possibilities of securing wireless traffic. The practical part then deals with the creation of a complete tool for passive interception of traffic in IEEE 802.11 networks. Where it is mainly about processing traffic statistics. The resulting program, written in Python, allows the user to display current information such as: number of transmitted frames, channel, band, received signal strength, and more. Subsequently, the results can be displayed in the form of graphs. As part of the test measurement, the correct functionality of the program was verified.

KEYWORDS

Passive capturing, IEEE 802.11

PARTNOV, Denys. *Sonda pro pasivní odposlech standardu IEEE 802.11*. Brno, 2021, 104 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Jan Pospíšil

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Sonda pro pasivní odposlech standardu IEEE 802.11“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu diplomové práce panu Ing. Janu Pospíšilovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Bakalářská práce se věnuje standardu IEEE 802.11 pro rodinu bezdrátových protokolů i analýze jednotlivých vrstev komunikace tohoto protokolu. V rámci této práce jsou popsané sítě založené na standardu IEEE 802.11 a taky prozkoumané jednotlivé vrstvy komunikace a možností pasivního odposlechů provozu v síti. Jsou popsané výhody a nevýhody nejčastěji využívaných bezpečnostních protokolů, jejich implementace z pohledu bezpečnosti, a možné zranitelnosti. Na základě zjištěné informace, v praktické části této práce byl implementován a následně optimalizován kompletní nástroj, v programovacím jazyce Python, pro pasivní odposlech provozu v bezdrátových sítích a jeho zachycení. V rámci rozsáhlého testování pro nejčastěji využívané protokoly rodiny IEEE 802.11 byla prakticky ověřena funkcionalita nástroje a ukázáno, jakou informaci se dá zjistit během pasivního odposlechu. Dále v rámci praktické části bylo provedeno několik testovacích odposlechů provozu podle testovacích plánů. Testovací plány v sobě zahrnují ověření efektivity pasivního odposlechu provozu v závislosti na použitém protokolu 802.11, určení závislosti ztrátovosti dat při odposlechu provozu vzhledem k použité frekvenci a vytíženosti sítě a taky určení, které informace se dají zjistit pomocí pasivního odposlechu sítě.

1 Standard IEEE 802.11

Tato kapitola popisuje obecný přehled protokolu 802.11, jeho architekturu a strukturu sítí založených na tomto protokolu.

1.1 Přehled sítí 802.11

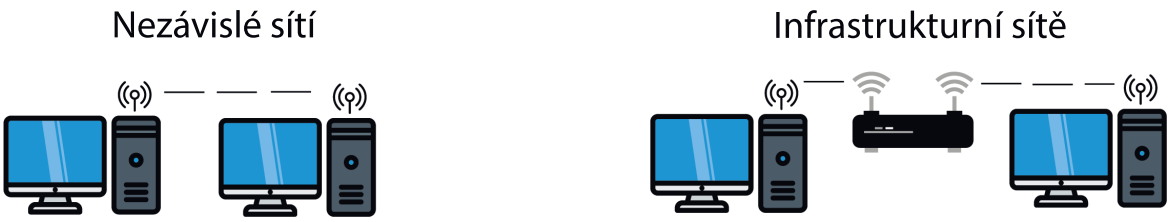
Protokol 802.11 spadá do řady IEEE 802, což je řadou specifikací pro LAN sítě. IEEE 802.11 je soustředěn na dvě poslední vrstvy OSI modelu, to jsou fyzická (PHY) a linková (MAC).

Fyzická vrstva definuje fyzikální vlastnosti všech zařízení jako jsou například napěťové úrovně a vlastnosti kabelů. Linková vrstva uspořádá data z fyzické vrstvy do logických celků, rámců. Mezi jiné úkoly linkové vrstvy patří také seřazení přenášených rámců, nastavení parametrů přenosu. V podstatě tato vrstva poskytuje funkce k přenosu dat a detekuje, případně opravuje chyby vzniklé na fyzické vrstvě.

Standard 802.11 ve své struktuře má podobné aspekty jako IEEE 802.3 (Ethernet), a to z toho důvodu, že byl vyvíjen s cílem zpětné kompatibility. V podstatě je 802.11 adaptace klasického Ethernetu pro bezdrátové prostředí. Například pro MAC adresy bezdrátových karet síťového rozhraní jsou přiřazeny 48 bitové adresy, které pro praktické účely vypadají stejně jako adresy kart síťového rozhraní Ethernet. Ve skutečnosti se přiřazení MAC adresy provádí ze stejného fondu adres, takže karty 802.11 mají jedinečné adresy i při nasazení do sítě s kabelovými stanicemi Ethernet.[2]

1.1.1 Typy sítí

Základem jakékoliv sítě 802.11 je *Basic service set* (BSS), což je obyčejná skupina stanic, které komunikují mezi sebou. Místo, kde stanice komunikují, se nazývá *základní oblast služeb*, velikost plochy tohoto místa určují vlastnosti bezdrátového média. Rozlišujeme několik typů BSS.[2]



Obr. 1.1: Typy sítí 802.11

Nezávislé sítě

Nezávislé sítě nebo *Independent BSS* (IBSS) jsou sítě, kde stanice komunikují přímo mezi sebou bez přístupového bodu. Nejmenší IBSS síť může být vytvořena pomocí dvou stanic. Zpravidla se tento typ sítí používá na krátkou dobu, například pro schůzku na konferenci. Po zahájení schůzky účastníci vytvoří IBSS síť ke sdílení dat mezi sebou. Když setkání končí, IBSS je rozpuštěna. Vzhledem k jejich krátkému trvání a malé velikosti jsou IBSS někdy označovány jako Ad-hoc BSS nebo Ad-hoc sítě.[2]

Infrastrukturní sítě

Infrastrukturní sítě nebo *Infrastructure BSS*, jsou takové sítě, které mají přístupový bod. Pomocí přístupového bodu probíhá všechna komunikace uvnitř sítí, včetně komunikace mezi stanicemi. V infrastrukturní síti musí být stanice spojeny s přístupovým bodem, aby bylo možné získat síťové služby. Připojení stanice k přístupovému bodu probíhá v rámci speciálního procesu. Sdružení (*association*) je proces, kterým se mobilní stanice připojí k 802.11 síti, tento proces není symetrický. Mobilní stanice vždy zahájí proces připojení a přístupové body se mohou rozhodnout, zda udělit nebo zamítnout přístup na základě obsahu žádosti.[2]

Rozšířené oblasti služeb

Extended service areas (ESS) nebo rozšířené oblasti služeb jsou sítě založené na principu spojení několika infrastrukturních sítí do jedné velké sítě. Funguje to tak, že každá z menších sítí je nakonfigurována stejně a všechny jsou připojené do jedné páteřní sítě pomocí hub nebo switch. Rozšířené oblasti služeb jsou abstrakce na nejvyšší úrovni podporované sítěmi 802.11. Přístupové body v ESS fungují ve shodě, aby vnější svět mohl používat jedinou MAC adresu pro komunikaci se stanicí někde v ESS. Na obrázku 1.1.1 je směrovač, který používá jednou MAC adresu k doručování rámců do mobilní stanice. Přístupový bod, se kterým je mobilní stanice přidružena, dodá rámec.[2]

Typy bezdrátových sítí podle rozsahu

V závislosti na rozsahu poskytovaného přenosu informací v bezdrátové síti jsou rozděleny do následujících kategorií:

WPAN

Bezdrátové osobní sítě (WPAN) jsou sítě, jejichž standard vyvinula pracovní skupina IEEE 802.15. WPAN se používá pro komunikaci různých zařízení, včetně počítačů, domácích a kancelářských zařízení, komunikačních zařízení atd. Fyzické a kanálové úrovně jsou regulovány normou IEEE 802.15.4. Rozsah WPAN se pohybuje od

několika desítek centimetrů do několika metrů. WPAN se používá jak k propojení jednotlivých zařízení navzájem, tak k jejich připojení k sítím vyšší úrovně, například globálnímu internetu.

WLAN

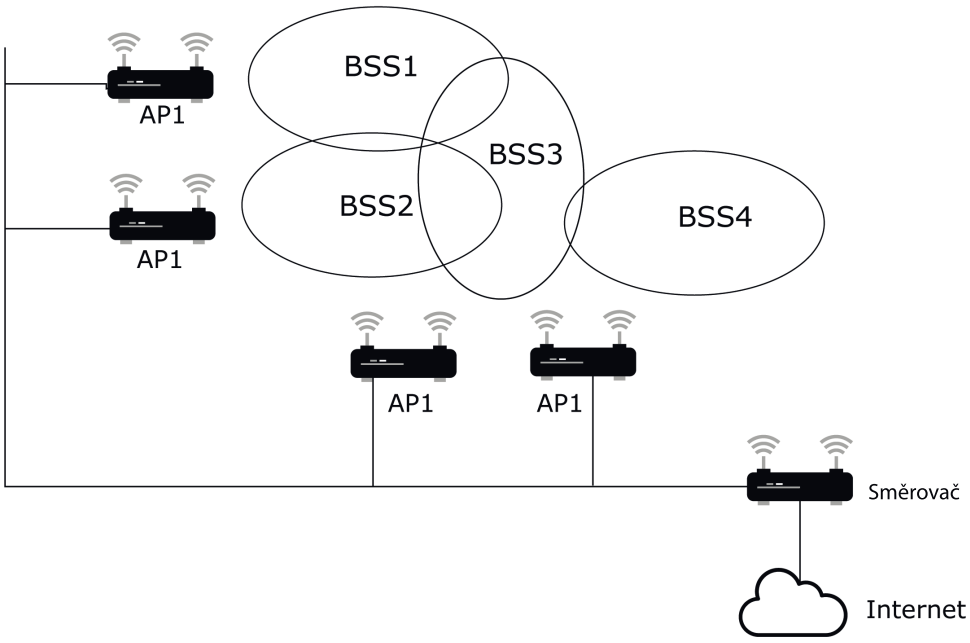
Bezdrátové místní sítě. Poskytují přenos informací na vzdálenost od několika desítek do několika set metrů. Tato kategorie zahrnuje sítě Wi-Fi.

WMAN

Bezdrátové sítě pro celé město. Poskytujte širokopásmový přístup k síti prostřednictvím rádiového kanálu. WMAN síť popisuje standart IEEE 802.16 publikovaný v dubnu 2002. 802.16 je takzvaná technologie „poslední míle“ využívající frekvenční rozsah od 10 do 66 GHz. Protože se jedná o rozsah centimetrů a milimetrů, je předpokladem přímá viditelnost mezi anténami transceiverových zařízení. Standard podporuje technologie topologie point-to-multipoint, duplexní kmitočtové dělení (FDD) a duplexní časové dělení (TDD) s podporou kvality služeb (QoS). Je možný přenos zvuku a videa.

WWAN

Bezdrátové širokopásmové sítě. Nejběžnějším typem těchto sítí jsou sítě GPRS, které fungují v řádu desítek kilometrů.



Obr. 1.2: Rozšířené oblasti služeb

1.1.2 Jednotlivé standardy 802.11

Tato podkapitola popisuje jednotlivé standardy protokolu 802.11 a jejich rozdíly. Existuje několik typů sítí WLAN, které se liší organizací signálu, rychlostí přenosu dat, poloměrem pokrytí sítě a charakteristikami rádiových vysílačů a přijímačů. Nejpoužívanější bezdrátové sítě jsou 802.11b, 802.11g, 802.11n, 802.11ac a další. Specifikace 802.11a a 802.11b byly poprvé schváleny v roce 1999, ale nejrozšířenější jsou zařízení založená na standardu 802.11b.

802.11-1997

Původní verze bezdrátového síťového standardu IEEE 802.11 byla vydána v roce 1997 a revidovaná v roce 1999. Většina protokolů popsaných v této verzi se nyní používá jen zřídka. Standard definoval dvě základní části protokolů, které jsou platné i v dnešních, modernějších protokolech, a to jsou MAC vrstva a PHY vrstva. PHY vrstva měla dvě možnosti fungování: pomocí rádiových vln a infračerveného záření. Tento protokol stanovil dvě bitové rychlosti: 1 Mbps nebo 2 Mbps a taky rádiový přenos na frekvenci 2,4 GHz. Dále stanovil alternativní technologie modulací na fyzické vrstvě: DSSS a FHSS.[5]

802.11a

Standard 802.11a byl přijat v roce 1999, své využití však našel až od roku 2001. Tato norma se používá hlavně v USA a Japonsku, v Evropě široké využití nemá. Standard 802.11a používá schéma modulace signálu s názvem *Orthogonal Frequency Division Multiplexing* (OFDM). Hlavní datový proud je rozdělen do několika paralelních dílčích toků s relativně nízkou bitovou rychlostí a poté je k jejich modulaci použit vhodný počet nosných. Standard definuje tři povinné rychlosti přenosu dat (6, 12 a 24 Mbps) a dalších pět (9, 18, 24, 48 a 54 Mbps). Je také možné použít dva kanály současně, což zdvojnásobuje rychlost přenosu dat.[5]

802.11b

Standard 802.11b je založen na modulaci DSSS (*Direct Sequence Spread Spectrum*). Celý operační rozsah je rozdělen na 14 kanálů, oddělených 25 MHz, aby se vyloučilo vzájemné rušení. Data se přenášejí přes jeden z těchto kanálů bez přepínání na jiné. Je možné současné použití pouze 3 kanálů. Přenosová rychlost se může automaticky měnit v závislosti na úrovni rušení a vzdálenosti mezi vysílačem a přijímačem.

Standard IEEE 802.11b realizuje maximální teoretickou přenosovou rychlost 11 Mbps, což je srovnatelné s 10 BaseT Ethernet kabeláží. Tato rychlost je možná při přenosu dat jedním zařízením WLAN. Pokud v prostředí současně pracuje větší počet účastnických stanic, pak je šířka pásma rozdělena mezi všechny a rychlost přenosu dat na uživatele klesá. Tento standard je dnes nejpopulárnější a ve skutečnosti

nese známku Wi-Fi. Stejně jako u původního standardu IEEE 802.11 se v této verzi používá pro přenos pásmo 2,4 GHz.[5]

802.11g

Standard 802.11g byl schválen v červnu 2003. Jedná se o další vylepšení specifikace IEEE 802.11b a implementuje datový přenos ve stejném frekvenčním rozsahu. Hlavní výhodou tohoto standardu je zvýšená propustnost - rychlost přenosu dat v rádiovém kanálu dosahuje 54 Mbps ve srovnání s 11 Mbps pro 802.11b. Stejně jako IEEE 802.11b funguje nová specifikace v pásmu 2,4 GHz, ale ke zvýšení rychlosti používá stejné modulační schéma jako 802.11a, ortogonální multiplexování s frekvenčním dělením (OFDM). Standard 802.11g je kompatibilní s 802.11b. Adaptéry 802.11b tedy mohou fungovat v sítích 802.11g (ale ne rychlejší než 11 Mbps) a adaptéry 802.11g mohou snížit rychlost přenosu dat na 11 Mbps, aby fungovaly ve starších sítích 802.11b.[5]

802.11n

Standard 802.11n také označován jako Wi-Fi 4, byl ratifikován 11. září 2009. Při použití v režimu 802.11n s jinými zařízeními 802.11n téměř čtyřnásobně zvyšuje rychlost přenosu dat ve srovnání se zařízeními 802.11g (která mají maximální rychlost 54 Mbps). Maximální teoretická rychlost přenosu dat je 600 Mbps při použití přenosu dat přes čtyři antény najednou. Rychlost přenosu jedné antény je tedy až 150 Mbps. Standard IEEE 802.11n je založen na technologii OFDM-MIMO. Většina funkcí je vypůjčena ze standardu 802.11a, avšak standard IEEE 802.11n má schopnost používat jak kmitočtový rozsah přijatý pro standard IEEE 802.11a, tak kmitočtový rozsah přijatý pro standardy IEEE 802.11b/g. Zařízení podporující standard IEEE 802.11n tedy mohou pracovat ve frekvenčním rozsahu 5 nebo 2,4 GHz, přičemž konkrétní implementace závisí na zemi.

Zvýšení přenosové rychlosti ve standardu IEEE 802.11n je dosaženo díky zdvojnásobení šířky kanálu z 20 na 40 MHz a také díky implementaci technologie MIMO. S pomocí MIMO se provádí prostorové multiplexování: současný přenos několika informačních toků na jednom kanálu, použití vícecestného způsobu doručení signálu, což minimalizuje účinek rušení a ztráty dat, ale vyžaduje několik antén. Tato schopnost současně vysílat a přijímat data zvyšuje propustnost zařízení 802.11n.[5]

802.11ac

Standard 802.11ac je dalším vývojem technologií zavedených do standardu 802.11n. Ve specifikacích jsou zařízení standardu 802.11ac klasifikována jako VHT (*Very High Throughput*) - s velmi vysokou propustností. Sítě 802.11ac fungují výhradně v pásmu

5 GHz. Šířka pásma rádiového kanálu může být 20, 40, 80 a 160 MHz. Je také možné kombinovat dva rádiové kanály 80 + 80 MHz.

Změny oproti 802.11n zahrnují širší kanály, více prostorových toků, modulace vyššího řádu (až 256-QAM vs. 64-QAM) a přidání víceuživatelského MIMO (MU-MIMO), což přináší datovou rychlost až 433,3 Mbps na prostorový proud, celkem 1300 Mbps, v 80 MHz kanálech pásma 5 GHz.[5]

802.11ad

IEEE 802.11ad je standard, který definuje novou fyzickou vrstvu pro sítě 802.11, které pracují v 60 milimetrovém vlnovém spektru 60 GHz. Toto frekvenční pásmo má výrazně odlišné charakteristiky šíření než pásma 2,4 GHz a 5 GHz, kde fungují sítě Wi-Fi. Zařízení implementující standard 802.11ad jsou uváděny na trh pod značkou WiGig. IEEE 802.11ad je protokol používaný pro velmi vysoké přenosové rychlosti (až 7 Gbps) a pro komunikaci na krátkou vzdálenost (1–10 metrů).[5]

802.11ax

IEEE 802.11ax (Wi-Fi 6) je nástupcem protokolu 802.11ac a zvýší účinnost sítí WLAN. Cílem tohoto projektu, který je v současné době ve vývoji, je 4 krát větší propustnost 802.11ac v uživatelské vrstvě. V předchozím protokolu 802.11 (konkrétně 802.11ac) byl zaveden MIMO pro více uživatelů, což je technika prostorového multiplexování. MU-MIMO umožňuje přístupovému bodu vytvářet paprsky směrem ke každému klientovi a současně přenášet informace. Tím se sníží interference mezi klienty a zvýší se celková propustnost, protože více klientů může přijímat data současně. U protokolů 802.11ax je podobné multiplexování zavedeno ve frekvenční oblasti, jmenovitě OFDMA. S touto technikou je více klientů přiřazeno k různým zdrojovým jednotkám v dostupném spektru. Tímto způsobem lze 80 MHz kanál rozdělit do více zdrojů, takže více klientů současně přijímá různý typ dat ve stejném spektru.[5]

1.2 Fyzická vrstva 802.11

Tato kapitola se věnuje fyzické vrstvě, bývá značena zkratkou PHY. Na fyzické úrovni jsou definovány dvě širokopásmové vysokofrekvenční metody přenosu a jedna je v infračerveném rozsahu. Technologie širokopásmového signálu používané v radiofrekvenčních metodách zvyšují spolehlivost, propustnost a umožňují mnoha nepřipojeným zařízením sdílet stejné frekvenční pásmo s minimálním vzájemným rušením.

802.11 používá přímé sekvenční rozprostřené spektrum (DSSS) a frekvenční skokové rozprostřené spektrum (FHSS). Tyto metody jsou zásadně odlišné a navzájem nekompatibilní. Obě používají techniky rozprostřeného spektra a využívají rádiové

vysílání v nelicencovaných pásmech spektra při frekvenci přibližně 2,4 GHz. Frekvenční pásma bez licence se v posledním desetiletí zvýšila z důvodu technologického pokroku, který umožnil vývoj kompaktních a levných rádiových vysílačů a přijímačů. Pomocí těchto vysílačů a přijímačů pro komunikaci dat jiného druhu lze implementovat mnoho aplikací (existujících nebo nových).

Tradičně bylo rádiové spektrum považováno za vzácný přírodní zdroj, jehož používání musí regulovat vnitrostátní správy. Tyto správy rozhodují o uživatelích, kterým byla udělena licence k využívání spektra, a za toto použití ukládají nějaký druh platby. Toto schéma funguje dobře pro tradiční uživatele (veřejné operátory, provozovatele vysílání a vládní agentury), ale nelze jej účinně použít, pokud by počet potenciálních uživatelů konkrétní aplikace mohl být řádu milionů. To neplatí pouze pro WLAN, ale také pro jiné aplikace, jako je všudypřítomný otvírač garážových vrat.[5]

1.2.1 Obecný přehled fyzické vrstvy 802.11

Fyzická vrstva definuje elektrické a fyzické specifikace zařízení. Definuje zejména vztah mezi zařízením a přenosovým médiem. Hlavní funkce a služby poskytované fyzickou vrstvou jsou následující:

a) Navázání a ukončení připojení ke komunikačnímu médiu.

b) Účast na procesu komunikace, kde jsou efektivně sdílené prostředí mezi více uživateli. Například řešení sporů a řízení toku dat.

c) Modulace nebo převod mezi reprezentací digitálních dat v uživatelském zařízení a odpovídajícím signálům přenášené přes komunikační kanál. Jedná se o signály pracující přes fyzickou kabeláž (například měď a optické vlákno) nebo prostřednictvím rádiového spojení.

Fyzická vrstva se skládá ze dvou podúrovní:

1. PLCP (*Physical Layer Convergence Protocol*) - provádí postup pro mapování MAC PDU (prvek datového protokolu) do rámce FHSS nebo DSSS.

2. PMD (*Physical Medium Dependent*) - "mediální závislá podvrstva". Tato úroveň se bude lišit pro různé přenosové rychlosti a různé standardy ze série 802.11. Podvrstva PMD poskytuje data a služby pro podvrstvu PLCP a funkce rádiového přenosu a příjmu, které vedou k toku dat, časovým informacím a parametrům příjmu.[5]

1.2.2 Fyzická vrstva standardů sítě Wi-Fi

V teto kapitole jsou popsané fyzické vrstvy skupinových standardů 802.11, které se liší technologiemi a dosažitelnými rychlostmi.

Základní standard 802.11

Základní (původní) standard 802.11 reguluje provoz zařízení na střední frekvenci 2,4 GHz s maximální rychlostí až 2 Mbps. Na fyzické vrstvě základního protokolu 802.11 jsou implementovány 2 metody přenosu dat, které umožňují přenášet rámec podvrstvy MAC z jedné stanice na druhou:

a) metoda přeskakování frekvence FHSS (*Frequency Hopping Spread Spectrum*),

b) volitelná metoda rozprostřeného spektra DSSS (*Direct Sequence Spread Spectrum*).

Metoda FHSS je podobná přeskakování frekvencí v sítích GSM a EDGE a metoda DSSS je do značné míry podobná metodě v systému dělení kódů CDMA. Zařízení FHSS rozdělují frekvenční pásmo určené pro jejich provoz od 2,402 do 2,480 GHz na 79 nepřekrývajících se kanálů. Každý ze 79 kanálů je široký 1 MHz. Odesílatel a příjemce se dohodnou na schématu přeskakování kanálů a data se posílají postupně na různé kanály pomocí vybraného schématu. Skákací frekvence musí být mezi šesti kanály alespoň 2,5 krát za sekundu. Technologie FHSS a DSSS poskytuje maximální rychlost přenosu dat pouze 2 Mbps, zatímco nyní existují rychlejší sítě založené na standardech 802.11b, 802.11a, 802.11g, 802.11n.[5]

Standard 802.11b

Na fyzické vrstvě 802.11b je implementována metoda vysokorychlostního přenosu širokopásmového kanálu pomocí metody HR-DSSS (*High Rate Direct Sequence Spread Spectrum*). Signál je kódován pomocí diferenciální dvoupolohové nebo čtyřpolohové fázové modulace (DBPSK nebo DQPSK). S nosnou modulační frekvencí 11 MHz je celková rychlost 1 nebo 2 Mbps, v závislosti na typu modulace. Standard 802.11b poskytuje přenosové rychlosti 11 a 5,5 Mbps. K tomu se používá doplňkové kódování klíčů (modulace CCK), které umožňuje kódovat 8 bitů na symbol, což odpovídá přenosové rychlosti 11 Mbps. Při přenosové rychlosti 5,5 Mbps jsou 4 bity kódovány do jednoho symbolu. Protokol také poskytuje opravu chyb FEC. V rozšířené verzi standardu 802.11b+ může být rychlost přenosu dat až 22 Mbps. Standard 802.11b používá monitorování kvality kanálu k automatické změně datové rychlosti v závislosti na úrovni signálu/interference. Teoretická rychlost proto jednoznačně neodpovídá skutečné rychlosti přenosu dat. V posledních letech se zvýšil počet bezdrátových zařízení po celém světě, jejichž používání někdy způsobilo problém rušení a přetížení v pásmu 2,4 GHz. Sítě 802.11b fungují v tomto nelicencovaném pásmu. Pro uvolnění pásma 2,4 GHz byl vyvinut standard 802.11a pro frekvence 5 GHz. V tomto rozsahu je úroveň hlukové konstelace nižší. Ve standardu 802.11b je jako další modulační metoda použito paketové binární konvoluční kódování PBCCC. Tento mechanismus umožňuje dosáhnout šířky pásma 5,5, 11 a 22 Mbps.[5]

Standard 802.11a

Standard 802.11a používá dvě střední frekvence v oblasti 5 GHz a má maximální přenosovou rychlost až 54 Mbps. Tato specifikace je založena na zásadně odlišném mechanismu vícenásobného přístupu, než jsou standardy bezdrátových sítí a Wi-Fi popsané dříve. Ve standardu 802.11a je jako hlavní technika rozprostřeného spektra použit ortogonální frekvenčně dělený multiplex (OFDM). Technologie OFDM zavedla koncept ochranného intervalu GI (Guard Interval), během kterého bude probíhat cyklické opakování OFDM. Předpona je přidána k vysílanému symbolu na vysílači a odstraněna, když je symbol přijat na přijímači. Tento ochranný interval snižuje rychlost přenosu dat.

Nevýhody technologie 802.11a zahrnují vyšší spotřebu energie pro frekvence 5 GHz a menší rozsah (zařízení pro frekvenci 2,4 GHz může pracovat na vzdálenost až 300 metrů a pro frekvenci 5 GHz - přibližně 100 m).[5]

Standard 802.11g

802.11g je vylepšená verze 802.11b. Je navržen pro provoz na frekvencích 2,4 GHz s maximální rychlostí 54 Mbps. Je to podobné jako 802.11a ve frekvenci a 802.11a v maximální rychlosti. Umožňuje DSSS a OFDM rozprostřené spektrum.[5]

Standard 802.11n

Standard 802.11n je navržen tak, aby zlepšil rychlosti přenosu dat a rozšířil rozsah přenosu dat. Stejně jako standard 802.11a je založen na technologii OFDM. Zvýšení rychlosti přenosu informací v tomto standardu je dosaženo pomocí následujících opatření.

1. Zdvojnásobení šířky pásma kanálu z 20 na 40 MHz, zatímco režim 20 MHz je povinný a je pro něj nastaven základní režim přenosové rychlosti.

2. Aplikace technologie vícekanálových anténních systémů MIMO (*Multiple Input Multiple Output*), tj. více vstupů a více výstupů. Je založena na použití více vysílacích a přijímacích antén. Přenášený datový proud je rozdělen na nezávislé bitové sekvence, které jsou odesílány současně pomocí různých antén. Díky více anténám umožňuje systém MIMO prostorové multiplexování proudů, což vede k vyšším datovým rychlostem. Systém MIMO také umožňuje současný přenos jednoho a téhož datového proudu přes několik antén. Kvůli víceúrovňovému šíření přijímač přijímá více signálů. Pomocí technologie MIMO jsou tyto signály zpracovávány a původní signál je z nich rekonstruován, což pomáhá zlepšit poměr signálu k šumu. Například zařízení 802.11n s více vysílacími a přijímacími anténami může zvýšit rychlost přenosu dat a zároveň zlepšit poměr signálu k rušení.[5]

1.2.3 Techniky rozprostřeného spektra (SS)

Šíření spektra je metoda zvyšování efektivity přenosu informací pomocí modulovaných signálů kanálem se silným lineárním zkreslením (únikem), což vede ke zvýšení signální základny. Metody rozprostřeného spektra dostávají svůj název podle skutečnosti, že šířka pásma použitá pro přenos signálu je mnohem širší, než je minimum potřebné pro přenos dat. Komunikační systém se nazývá systémem s rozprostřeným spektrem pokud splní podmínky:

1. Použitá šířka pásma je mnohem širší, než je minimum potřebné pro přenos dat.

2. Šíření spektra se provádí pomocí takzvaného šíření (nebo kódu) signálu, který nezávisí na přenášených informacích.

3. Rekonstrukce původních dat přijímačem („zbavení spektra“) se provádí porovnáním přijatého signálu a synchronizované kopie šířícího se signálu.

Je třeba poznamenat, že šíření signálu nastává také u některých standardních modulačních schémat, jako je frekvenční modulace a pulzní kódová modulace. Tato schémata se však nevztahují na metody rozprostřeného spektra, protože nesplňují všechny výše uvedené podmínky.

Pro dosažení větší šířky pásma se používají systémy s rozprostřeným spektrem kódů ve vysílači, nezávislé na datech, před modulací, které musí znát přijímač. Přijímač, který nezná kód, by nebyl schopen kódovaná data dekódovat. Ve srovnání s úzkopásmovým přenosem je obtížnější detekovat, zachytit nebo dekódovat přenosy s rozprostřeným spektrem. Hlavní aplikace těchto systémů byly tedy zpočátku vojenské. Stejné vlastnosti však mají výhody v komerčních systémech, protože jsou méně citlivé na rušení od jiných uživatelů a méně pravděpodobně interferují s ostatními. To platí zejména tehdy, když rušící / rušený uživatel používá úzkopásmový přenos. Oba druhy systémů mohou koexistovat ve stejném frekvenčním pásmu s malým vzájemným rušením. V hlučném prostředí nejsou rozdíly mezi úzkopásmovým a rozprostřeným spektrem systémů.

Systémy s rozprostřeným spektrem jsou obecně složitější, a proto byly přijaty do komerčních systémů, pouze pokud technologický pokrok umožnil integraci výkonných procesorů digitálních signálů, které lze vyrobit ve velkém množství za velmi nízké náklady. Nejčastěji používané techniky rozprostřeného spektra jsou FH a DS. Protože oba byly zahrnuty do standardu IEEE 802.11.[5]

1.2.4 Typy rozprostřeného spektra

Techniky šíření spektra byly původně navrženy pro zpravodajské a vojenské účely. Hlavní myšlenkou metody je distribuovat informační signál v širokém rádiovém pásmu, což ve výsledku významně zkomplikuje potlačení nebo odposlech signálu.

Princip fungování metod spočívá v „rozmazání“ rádiového signálu v širokém frekvenčním pásmu pomocí speciálních distribučních algoritmů. Generování širokopásmových signálů (také signálů podobných šumu) se provádí pomocí generátoru pseudonáhodných čísel (PNG), který definuje distribuční algoritmus. Každý přijímač musí znát kódovací sekvenci pro dekódování zprávy. Zařízení s různými PN spolu ve skutečnosti nekomunikují. Vzhledem k tomu, že síla signálu je rozložena na velkou šířku pásma, jeho spektrální charakteristiky se podobají šumu v rádiovém kanálu. Bezdrátové přenosové systémy používají dvě metody rozprostřeného spektra: FHSS a DSSS.

V metodě FHSS jsou přijímač a vysílač synchronně naladěny na různé nosné frekvence každých několik milisekund v souladu s algoritmem pseudonáhodné sekvence. Zprávu může přijmout pouze příjemce, který používá stejnou sekvenci. To předpokládá, že ostatní systémy pracující ve stejném kmitočtovém rozsahu používají odlišnou sekvenci, a proto se navzájem prakticky neinterferují. V případech, kdy se dva vysílače pokusí použít stejnou frekvenci současně, existuje protokol rozlišení kolize, ve kterém se vysílač pokusí znovu odeslat data na následující frekvenci v pořadí.

Metodu DSSS lze reprezentovat následovně. Celé použité široké frekvenční pásmo je rozděleno do několika subkanálů - podle standardu 802.11 je subkanálů 11. Každý přenášený bit informací se podle předem stanoveného algoritmu změní na sekvenci 11 bitů a těchto 11 bitů je přenášeno současně a paralelně pomocí všech 11 subkanálů. Po přijetí je přijatá bitová sekvence dekódována pomocí stejného algoritmu jako při jejím kódování. Další dvojice přijímač-vysílač může používat jiný algoritmus kódování a dekódování a takových algoritmů může být spousta.

Každá ze dvou širokopásmových přenosových metod má své výhody i nevýhody. Metoda DSSS umožňuje dosáhnout vyšší propustnosti ve srovnání s FHSS, poskytuje vyšší odolnost vůči úzkopásmovému rušení a delší komunikační rozsah. Technologie DSSS však vyžaduje sofistikovanější a nákladnější vybavení než FHSS. Proto produkty pro FHSS vyrábí podstatně větší počet společností. Další výhodou zařízení FHSS (na rozdíl od DSSS) je schopnost zůstat v provozu v podmínkách širokopásmového rušení. Je pravda, že samy často interferují s konvenčními úzkopásmovými zařízeními, jde však o inteferenci s nízkou spektrální hustotou.[5]

1.3 Linková vrstva 802.11

Tato kapitola popisuje linkovou vrstvu (MAC) standartu IEEE 802.11 WLAN, shrnuje některé obecné úvahy o návrhu MAC vrstvy a popisuje funkce, které se obvykle vyskytují v protokolu WLAN.

1.3.1 Obecný přehled linkové vrstvy

Vrstva datového spojení 802.11 se skládá ze dvou podvrstev: *Logical Link Control* (LLC) a *Media Access Control* (MAC). 802.11 používá stejné LLC a 48 bitové adresování jako jiné sítě 802, což usnadňuje kombinování bezdrátových a kabelových sítí, ale vrstva MAC je velmi odlišná.

Vrstva MAC 802.11 je velmi podobná vrstvě implementované v 802.3, kde podporuje více uživatelů na sdíleném nosiči. Sítě 802.3 Ethernet používají protokol *Carrier Sence Multiple Access with Collision Detection* (CSMA/CD), který určuje, jak ethernetové stanice přistupují ke kabelové lince a jak detekují a řeší kolize, ke kterým dochází, když se několik zařízení pokusí navázat komunikaci přes síť. K detekci kolize musí být stanice schopna přijímat i vysílat současně. Standard 802.11 umožňuje použití poloduplexních vysílačů, takže v bezdrátových sítích 802.11 nemůže stanice detekovat kolize během přenosu. Aby se tento rozdíl vyrovnal, používá standard 802.11 upravený protokol známý jako *Carrier Sense Multiple Access with Collision Prevention* (CSMA/CA) nebo *Distributed Coordination Function* (DCF). CSMA/CA se snaží zabránit kolizím pomocí explicitního potvrzení paketu (ACK), což znamená, že přijímací stanice odešle paket ACK, aby potvrdila, že paket byl přijat neporušený.

CSMA/CA funguje následovně. Stanice, která si přeje vysílat, testuje kanál, a pokud není detekována žádná aktivita, stanice čeká na náhodnou dobu a poté vysílá, pokud je přenosové médium stále volné. Pokud paket dorazí neporušený, přijímací stanice odešle paket ACK, po jehož přijetí odesílatel ukončí přenosový proces. Pokud vysílací stanice nepřijala paket ACK, v důsledku skutečnosti, že nebyl přijat datový paket nebo došlo k poškození ACK, je vytvořen předpoklad, že došlo ke kolizi, a datový paket je vysílán znovu v náhodném intervalu .

Algoritmus odbavení kanálu (CCA) se používá k určení, zda je kanál volný. Jeho podstatou je měřit energii signálu na anténě a určovat sílu přijímaného signálu (RSSI). Pokud je síla přijímaného signálu pod určitou hodnotou, pak je kanál prohlášen za volný a úroveň MAC obdrží stav CTS. Pokud je výkon vyšší než určitá hodnota, je přenos dat zpožděn podle pravidel protokolu.

Linková vrstva poskytuje nejen funkční, ale i procedurální prostředky pro přenos dat přes fyzickou vrstvu nebo síťové spojení s nezbytnou synchronizací, kontrolou chyb a řízení toku rozdělením dat do rámců a jejich postupným přenosem, aby byla data spolehlivá pro přijímající uzel a také zbavila horní vrstvy odpovědnosti za přidávání dat na síťovou linku a také příjem dat. [3]

LLC podvrstva

Horní vrstva vrstvy datového spojení (*Logical Link Control*) poskytuje službu sí-

ťové vrstvě, umisťuje informace o protokolu síťové vrstvy do rámečku a interaguje se spodní vrstvou (MAC). LLC je zodpovědná za multiplexování a demultiplexování protokolů síťové vrstvy. Na konci odeslání získá vrstva LLC informace o protokolu síťové vrstvy, jako je IP, IPX, ARP atd., vyplní ji v záhlaví rámce (multiplexování) a předá ji vrstvě MAC. Na přijímacím konci je vrstva LLC zodpovědná za převzetí rámce z fyzické vrstvy, identifikaci síťového protokolu a předání datagramu správnému protokolu síťové vrstvy na síťové vrstvě výše (de-multiplexování). LLC také poskytuje volitelné služby, jako je řízení toku, potvrzení a detekce chyb.[3]

MAC podvrstva

Tato nižší podvrstva interaguje s fyzickou vrstvou a definuje, kdo bude mít přístup k médiu. Poskytuje také rozdělení dat do rámců, které jsou přenášeny přes fyzickou vrstvu, tyto rámce obsahují informace o požadavcích na fyzickou vlastnost média a také typ protokolu vrstvy datové linky, který se používá pro přenos.[3]

1.3.2 Operace na linkové vrstvě

Níže jsou uvedeny operace, které jsou podporovány linkovou vrstvou.

Sestavení rámců

Data ve vrstvě datového spojení ze síťové vrstvy jsou rozdělena na menší kousky dat zvaných rámce, které zapouzdřují data síťové vrstvy takovým způsobem, že je to fyzické vrstvě srozumitelné. Rámce jsou přijímány fyzickou vrstvou a odesílány ve formě proudu bitů bez ohledu na strukturu nebo formát dat. Rámec má tři části: záhlaví, data a zápatí. Záhlaví rámce obsahuje řídicí informace určené protokolem vrstvy datového spojení, aby poskytly funkce, které vyžadovalo komunikační prostředí. Typická pole záhlaví rámce zahrnují:

a) Počátek a konec rámce: uvádí počáteční a koncový limit rámce.

b) Adresování: skládá se z fyzických adres zdrojového a cílového hostitele.

c) Typ: uvádí typ PDU, který je obsažen v rámci.

d) Kontrola kvality - řídí tok dat.

Na konec dat v rámci se přidá zápatí, které obsahuje pole pro detekci chyb a poslední pole pro označení konce rámce. To pomáhá při určování, zda byly v přijatém rámci zjištěny nějaké chyby, které jsou popsány v další části. To pomáhá zajistit spolehlivé údaje pro horní vrstvy.[4]

Fyzické adresování

Záhlaví rámce vrstvy datového spojení má pole pro adresování, které se používá pro přenos dat přes síťové spojení. Toto pole se skládá z fyzických adres, což je zdrojová

adresa rámce a cílová adresa rámce vysílajícího přes síťové spojení. Tyto adresy jsou specifické pro místní síť a lze je použít pouze pro přenos ve stejné síti.[4]

Detekce a oprava chyb

Detekce a oprava chyb jsou důležité operace podporované vrstvou datového spojení. Když jsou data přenášena přes síťové spojení, existuje vysoká pravděpodobnost, že signály na síťovém spojení budou rušeny zkreslením, útlumem a elektromagnetickým šumem. Tyto poruchy mohou nakonec podstatně změnit bitové hodnoty představované signály způsobujícími bitové chyby, přijímající uzel může chybně interpretovat, že bit v rámci je jeden, když se vysílá jako nula, a naopak. Protože by se nemuselo vyplatit odeslat datagram náchylný k chybám do síťových vrstev, vrstva datového spojení poskytuje mechanismus pro detekci těchto bitových chyb. Rámec se skládá ze zápatí přidaného na konec dat, které se skládá z pole obecně označovaného jako kontrola sekvence rámců (FSC), které určuje, zda během přenosu a příjmu rámce došlo k jakýmkoli chybám. Rámec na vysílacím uzlu má bity detekce chyb v poli FSC zápatí a když je rámec vysílán do přijímajícího uzlu, provede se kontrola chyb.

Nejčastější viděné chyby jsou jednobitová chyba, což znamená, že pouze jeden bit dat se změnil z 1 na 0 a 0 na 1 a chyba shluku, což znamená, že jsou změněny dva nebo více bitů dat způsobujících chybu. Techniky detekce a korekce chyb umožňují přijímači detekovat výskyt bitových chyb, ale není to vždy stoprocentně spolehlivě a stále může existovat možnost, že v datech bude přijata nezjištěná bitová chyba a přijímač o ní nebude vědět. Aby se snížila pravděpodobnost takových výskytů, je nutné odpovídajícím způsobem zvolit schéma detekce chyb.[4]

Řízení toku

Uzly na každé straně přenosu po síťovém spojení mají omezenou kapacitu rámce. To by se mohlo stát potenciálním problémem, například pokud přijímající uzel zpracovává přijaté rámce pomalu ve srovnání s rychlostí, kterou jsou do něj rámce odesílány, to by mohlo způsobit vážné přetížení sítě, což někdy způsobí ztrátu dat. Dalo by se očekávat, že odesílatel i přijímač vyřeší tento problém stejnou rychlostí, ale ve skutečností to není možné. Vrstva datového spojení poskytuje řízení toku jako službu, která řeší tento problém. Řízení toku zajišťuje, že vysílací zařízení nepřetíží příjemce a také zvýší účinnost. Existuje několik způsobů řízení toku dat.[4]

I. Stop-and-Wait

V tomto mechanismu odesílatel odesílá data, zastaví a čeká na potvrzení přijetí dat od přijímače. Odesílatel nemůže odeslat další data, dokud nepřijme potvrzení.[4]

II. Posuvné okno

V tomto přístupu bude odesílatel i příjemce používat vyrovnávací paměť stejné velikosti, která zabrání nutnosti čekat na odesílatele a zároveň odesílatel může posílat data bez čekání na potvrzení příjemce. Tento mechanismus poskytuje taky efektivní využití šířky pásma.[4]

III. Jednobitové posuvné okno

V tomto přístupu je velikost vyrovnávací paměti jeden bit, což znamená, že odesílatel a přijímač mohou odesílat pouze 0 a 1. Poskytuje sekvenci, potvrzení a číslo paketu a používá plně duplexní kanál. Funguje dobře, když odesílatel nejprve odesílá data a poté přijímač začne odesílat data po přijetí dat. Pokud však odesílatel i příjemce odesílají data současně, vede to k chybám nebo duplikaci paketů.[4]

IV. Go Back N

V tomto přístupu je odesílateli poskytnuta velikost okna. Odesílatel odesílá rámce bez přijetí jakéhokoli potvrzení příjemce. Přijímač je také vybaven velkou velikostí okna a potvrzení sledování sekvence rámců. Poté, co odesílatel odešle celý rámec, zkontroluje sekvenci přijatého ACK který obdrží od příjemce. Pokud je NACK přijímán v konkrétním rámci, pak jsou všechny rámce vysílány zpět po tomto konkrétním NACK.[4]

V. Selektivní opakování

V tomto přístupu, na rozdíl od předchozího přístupu, kdy musí být všechny rámce po NACK pro rámec znovu vysílány, je pro velikost okna přijímače poskytnut vyrovnávací prostor, který má v paměti rámce. V případě chyby příjemce pošle NACK pro konkrétní rámec, a odesílatel zopakuje vysílání toho konkrétního rámce bez nutnosti opakovat zbytečné vysílání ostatních rámců.[4]

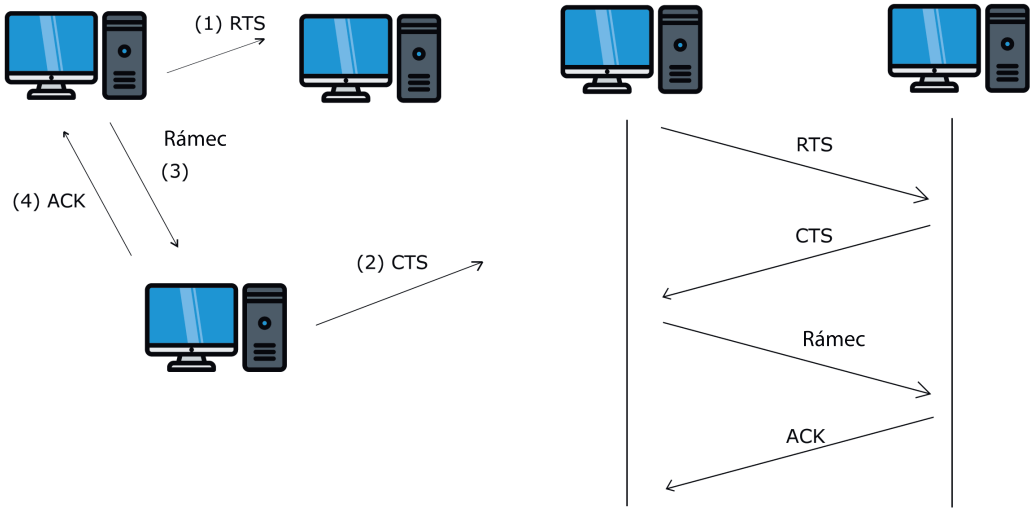
1.3.3 Kvalita rádiového přenosu

Na kabelovém Ethernetu po vyslání rámce se předpokládá to, že jej cíl přijímá správně, naproti tomu u rádiového spojení je jiná situace, hlavně z důvodu rušení nemůžeme předpokládat bezproblémové doručení do cíle, zejména pokud jsou použité nelicencovaná frekvenční pásma. I úzkopásmové přenosy podléhají šumu a rušení, ale zařízení vysílající na veřejných frekvenčních pásmech musí předpokládat, že rušení bude existovat a musí fungovat kolem něj. Návrháři 802.11 zvažovali způsoby, jak obejít záření z mikrovlnné trouby a jiné vysokofrekvenční zdroje. Kromě šumu může dojít k vyblednutí více cest které také vedou k situacím, ve kterých rámce nelze přenášet. Z toho důvodu, na rozdíl od mnoha jiných protokolů, byl na linkové

vrstvě 802.11 byl zaváděn mechanizmus pro kontrolu doručení zprávy. Poté, co stanice vyslala rámec, nějakou dobu čeká na potvrzující odpověď ACK, a až potom začne vysílat další rámec. Pokud některá část přenosu selže, rámec je považován za ztracený.[2]

1.3.4 Problém skrytého uzlu

V bezdrátových sítích může být obtížné odhalit kolize způsobené skrytými uzly protože bezdrátové transceivery jsou obecně poloduplexní. Nepřenášejí a nepřijímají ve stejném čase. Podstata tohoto problému spočívá v tom, že několik stanic připojených do jednoho přístupového bodu z nějakého důvodu nemohou přijímat zprávy mezi sebou a tím pádem si myslí, že na médiu není žádný přenos a začnou tedy vysílat svůj rámec. V tuto chvíli nastává kolize kterou pomáhá vyřešit mechanizmus RTS/CTS.



Obr. 1.3: Mechanizmus RTS/CTS

Aby nedocházelo ke kolizím, protokol 802.11 umožňuje stanicím používat žádost o odeslání *Ready to Send* (RTS) a potvrzení připraveni na přijetí *Clear to Send* (CTS). Obrázek 1.3.4 znázorňuje postup, ve kterém stanice, která chce zahájit přenos, pošle RTS zprávu příjemci, tato zpráva slouží k několika účelům: kromě rezervace rádiového spojení pro vysílání, umlčí všechny stanice, které to slyší. Pokud příjemce nemá aktuálně probíhající přenos, pošle CTS zprávu a tím potvrdí, že může přijímat zprávu. Následně odesílatel pošle rámec a čeká na zprávu potvrzující úspěšný příjem (ACK). Poté když byl ACK přijat, spojení se ukončí.[2]

2 Bezpečnost 802.11

Popularita bezdrátových lokálních sítí již prošla fází prudkého růstu a dosáhla stavu technologie „známá všem“. Domácí hotspoty a mini-routery Wi-Fi jsou levné a široce dostupné, hotspoty jsou dostatečně běžné, notebook bez Wi-Fi je anachronismem. Stejně jako mnoho jiných inovativních technologií přináší použití bezdrátových sítí nejen nové výhody, ale také nová rizika. Popularita Wi-Fi vytvořila novou generaci hackerů, kteří se specializují na vynalézání stále více způsobů hackování bezdrátových sítí a útoků na uživatele a podnikovou infrastrukturu. Od roku 2004 společnost Gartner varuje, že jedním z hlavních problémů bude zabezpečení WLAN - a prognóza je oprávněná. [9]

2.1 Obecný pohled na bezpečnost Wi-Fi

Tradiční kabelové sítě používají k přenosu informací kabel. Kabel je považován za „kontrolované“ prostředí chráněné budovami a místnostmi, ve kterých je umístěn. Externí „cizí“ provoz, který vstupuje do chráněného segmentu sítě, je filtrován firewallem a analyzován systémy IDS / IPS. Aby útočník získal přístup do takového segmentu kabelové sítě, musí překonat buď fyzický bezpečnostní systém budovy, nebo bránu firewall.

Bezdrátové sítě používají rádiové vlny. Bezdrátový prostor je sdílené prostředí s malou nebo žádnou kontrolou. Poskytování ekvivalentu fyzického zabezpečení kabelovým sítím zde jednoduše není možné. Jakmile uživatel připojí přístupový bod ke kabelové síti, jeho signál může projít zdmi, podlahami, okny budovy. Segment připojené sítě se tak stane přístupným z jiného patra nebo dokonce ze sousední budovy, parkoviště nebo na druhém konci ulice - rádiový signál se může šířit stovky metrů mimo budovu. Jedinou fyzickou hranicí bezdrátové sítě je síla signálu.

Na rozdíl od kabelových sítí, kde je bod připojení uživatele k síti dobře definovaný a známý - jedná se o zásuvku ve zdi, v bezdrátových sítích se tedy je možné připojit k síti odkudkoli, pokud je signál dostatečně silný . Vysílání je také sdíleným médiem. Všechna bezdrátová zařízení jsou součástí jednoho obrovského „rozbočovače“ - a jakékoli bezdrátové zařízení může „vidět“ všechny bezdrátové sousedy v síti. V takovém případě je obecně nemožné identifikovat přijímač pracující v pasivním režimu (pouze poslech).[9]

2.1.1 Metody omezení přístupu

Filtrování MAC adres

Tato metoda není součástí standardu IEEE 802.11. Filtrování lze provést třemi

způsoby:

1. Přístupový bod umožňuje přístup stanicím s jakoukoli MAC adresou;

2. Přístupový bod umožňuje přístup pouze stanicím, jejichž adresy MAC jsou v seznamu důvěryhodných;

3. Přístupový bod odepře přístup stanicím, jejichž MAC adresy jsou v „black listu“;

Nejspolehlivější z hlediska zabezpečení je druhá možnost, i když není navržena tak, aby detekovala změnu MAC adresy, což je pro útočníka snadné implementovat.

Skrytý režim SSID

Aby se přístupový bod sám detekoval, pravidelně vysílá majákové rámce. Každý takový rámec obsahuje informace o službě pro připojení a je přítomný zejména SSID (identifikátor bezdrátové sítě). V případě skrytého SSID je toto pole prázdné, to znamená, že není možné najít vaši bezdrátovou síť a nemůžete se k ní připojit bez znalostí hodnoty SSID. Ale všechny stanice v síti připojené k přístupovému bodu znají SSID a při připojování, když odesílají žádost o připojení, označují identifikátory sítě dostupné v jejich profilech připojení. Poslechem provozu může útočník snadno získat hodnotu SSID požadovanou pro připojení k požadovanému přístupovému bodu.[10]

Metody ověřování

Bez ověřování

Pracovní stanice odešle požadavek na ověření, který obsahuje pouze MAC adresu klienta. Přístupový bod odpovídá odmítnutím nebo potvrzením autentizace. Rozhodnutí je učiněno na základě filtrování MAC adres, to znamená, že ve skutečnosti nejde o zabezpečenou ochranu bezdrátové sítě Wi-Fi na základě omezení přístupu. Použité šifry: žádné šifrování, statický WEP, CKIP.[10]

Ověření sdíleného klíče (*Shared Key Authentication*)

Musí být nakonfigurován statický šifrovací klíč pro algoritmus WEP (*Wired Equivalent Privacy*). Klient odešle požadavek na přístupový bod k ověření, pro který obdrží potvrzení, které obsahuje 128 bajtů náhodných informací. Stanice šifruje přijatá data pomocí algoritmů WEP a odešle šifrovací text spolu s požadavkem na přidružení. Přístupový bod dešifruje text a porovná ho s původními daty. Pokud existuje shoda, je odesláno potvrzení přidružení a klient je považován za připojeného k síti. Schéma ověřování pomocí sdíleného klíče je zranitelná vůči útokům typu „Člověk uprostřed“. Šifrovací algoritmus WEP je jednoduchý XOR sekvence klíčů s užitečnými informacemi, takže naslouchání provozu mezi stanicí a přístupovým

bodem můžete obnovit část klíče. Použité šifry: žádné šifrování, dynamický WEP, CKIP.[10]

Ověření podle MAC

Tato metoda není poskytována v IEEE 802.11, ale je podporována většinou výrobců zařízení, jako jsou D-Link a Cisco. MAC adresa klienta je porovnána s tabulkou povolených MAC adres uložených na přístupovém bodu nebo je použit externí ověřovací server. Používá se jako další opatření ochrany. [10]

IEEE začalo vyvíjet nový standard IEEE 802.11i, ale kvůli obtížím se schvalováním organizace WECA (Wi-Fi Alliance) společně s IEEE oznámily standard WPA (*Wi-Fi Protected Access*). WPA používá TKIP (*Temporal Key Integrity Protocol*), který využívá vylepšený způsob správy klíčů a změny klíčového snímku po snímku.[10]

Chráněný přístup Wi-Fi (WPA)

Po prvních úspěšných útocích na WEP bylo rozhodnuto vyvinout nový standard 802.11i. Před vydáním však byl vydán „přechodný“ standard WPA, který zahrnoval nový ověřovací systém založený na standardu 802.1X a novou šifrovací metodu TKIP. Existují dvě možnosti ověřování: pomocí serveru RADIUS (WPA-Enterprise) a pomocí předinstalovaného klíče (WPA-PSK). Použité šifry: TKIP (standardní), AES-CCMP (rozšíření), WEP (pro zpětnou kompatibilitu). [10]

Chráněný přístup WI-FI2 (WPA2, 802.11i)

WPA2 nebo 802.11i je konečná verze standardu bezdrátového zabezpečení. Jako hlavní šifra byla vybrána silná bloková šifra AES. Systém ověřování prošel ve srovnání s WPA minimálními změnami. Stejně jako WPA má WPA2 dvě možnosti pro ověřování WPA2-Enterprise s ověřováním pomocí serveru RADIUS a WPA2-PSK s předinstalovaným klíčem. Použité šifry: AES-CCMP (standard), TKIP (pro zpětnou kompatibilitu). [10]

Centralizovaná správa klíčů Cisco (CCKM)

Možnost ověřování od CISCO. Podporuje roaming mezi přístupovými body. Klient je na serveru RADIUS ověřen jednou, poté může přepínat mezi přístupovými body. Použité šifry: WEP, CKIP, TKIP, AES-CCMP. [10]

2.2 Bezpečnostní protokoly 802.11

2.2.1 WEP

Wired Equivalent Privacy (WEP) je algoritmus pro zabezpečení sítí Wi-Fi. Používá se k zajištění důvěrnosti a ochraně přenášených dat oprávněných uživatelů bezdrátové sítě před odposlechem. Existují dvě varianty WEP – WEP-40 a WEP-104, které se liší pouze délkou klíče. Tato technologie je nyní zastaralá, protože ji lze prolomit během několika minut. Nadále je však široce používána. Pro zabezpečení v sítích Wi-Fi se doporučuje WPA.[13]

WEP Autentizace

Zabezpečení WEP zahrnuje dvě části, autentizaci a šifrování. Ověřování v WEP zahrnuje ověření zařízení při prvním připojení k síti. Proces ověřování v bezdrátových sítích používajících WEP má zabránit připojení zařízení / stanic k síti, pokud neznají klíč WEP. Při ověřování založeném na WEP bezdrátové zařízení odešle požadavek na ověření přístupovému bodu, poté přístupový bod odešle 128 bitovou náhodnou výzvu ve formě prostého textu klientovi. Bezdrátové zařízení používá sdílený tajný klíč k podepsání výzvy a odešle ji přístupovému bodu. Přístupový bod dešifruje podepsanou zprávu pomocí sdíleného tajného klíče a ověří výzvu, kterou již odeslal. Pokud se výzva shoduje, autentizace proběhlá úspěšně.

Bohužel, ve WEP není po autentizaci vyměněn žádný tajný klíč. Stejný tajný klíč nebo sdílený klíč se používá pro autentizaci i šifrování. Neexistuje tedy způsob, jak zjistit, zda následující zprávy pocházejí z důvěryhodného zařízení nebo od podvodníka. Tento druh autentizace je náchylný k „Man in the middle“ útoku. Tato autentizace zde opravdu není nejlepší snahou. Ve specifikaci Wi-Fi bylo ověřování zcela zrušeno, přestože bylo ve standardu IEEE 802.11.[13]

WEP Šifrování

WEP používá k šifrování dat mezi přístupovým bodem a bezdrátovým zařízením proudové šifrování RC4. WEP používá 8-bitový RC4 a pracuje na 8-bitových hodnotách tím, že vytvoří pole s 256 8-bitovými hodnotami pro vyhledávací tabulku (8 bitů 8-bitových hodnot).

Pro integritu dat WEP používá CRC. Protokol provádí kontrolu kontrolního součtu CRC (*Cyclic Redundancy Check*) na prostém textu a generuje hodnotu CRC. Tato hodnota CRC je spojena s prostým textem. Tajný klíč je spojen s inicializačním vektorem (IV) a přiváděn do RC4. Pak se spočítá pomocí XOR plaintext + CRC. Výsledkem je *ciphertext*. Stejný inicializační vektor, který byl použit dříve, je do výsledného *ciphertextu* vložen v čistém textu. Inicializační + vektor a Ciphertext a záhlaví rámců jsou poté přenášeny vzduchem na základě tajného klíče.[13]

WEP Zranitelnosti

Všechny útoky proti WEP jsou založeny na nedostatcích šifry RC4, jako je možnost inicializace kolizních vektorů a změny rámců. Všechny typy útoků vyžadují odposlech a analýzu bezdrátových rámců. V závislosti na typu útoku se počet rámců potřebných pro hackování liší. U programů jako Aircrack-ng je hacknutí bezdrátové sítě šifrované WEP velmi rychlé a nevyžaduje žádné speciální dovednosti.[9]

I. Útok Flarer-Mantin-Shamir

V roce 2001 jej navrhli Scott Flarer, Itzik Mantin a Adi Shamir. Vyžaduje slabé inicializační vektory v rámcích. V průměru je potřeba při hackování zachytit asi půl milionu snímků. Při analýze se používají pouze slabé vektory. Pokud chybí (například po opravě šifrovacího algoritmu), je tento útok neúčinný.[9]

II. KoreK útok

V roce 2004 jej navrhl hacker, pod jménem KoreK. Jeho zvláštností je, že pro útok nejsou nutné slabé inicializační vektory. Při hackování je potřeba zachytit několik stovek tisíc snímků. Při analýze se používají pouze inicializační vektory.[9]

III. Útok Tevs-Weinman-Pyshkin

V roce 2007 jej navrhli Erik Tews, Ralf-Philipp Weinmann a Andrey Pyshkin. Využívá schopnost vkládat požadavky ARP do bezdrátové sítě. V tuto chvíli je to nejúčinnější útok, při hackování stačí zachytit jen několik desítek tisíc snímků.[9]

2.2.2 WPA

Protokol 802.11i stanoví bezpečnostní mechanismy pro sítě WLAN. IEEE 802.11 původně určuje ekvivalent algoritmu zabezpečení kabelové LAN Wired Equivalent Privacy (WEP). V mnoha výzkumech se však ukazuje, že WEP nemůže dosáhnout požadované důvěrnosti dat, integrity a autentizace. WEP měl mnoho konstrukčních vad a je považován za zcela prolomený. V důsledku toho je použití WEP pro důvěrnost, autentizaci nebo řízení přístupu zastaralé při pozdější revizi normy v roce 2012. Přestože WEP nesplňuje bezpečnostní požadavky standardu, nový standard bude vyžadovat nový hardware. Není praktické snadno zbavit uživatele starých zařízení podporujících pouze WEP. Proto byl WEP následován Wi-Fi Protected Access (WPA), který používá starší hardware. WPA bylo jen přechodným řešením pro pokrytí slabých stránek WEP a bylo později nahrazeno WPA2.

WPA přijímá protokol TKIP (*Temporal Key Integrity Protocol*) pro zachování důvěrnosti a integritu, který pro šifrování dat stále používá Rivest Cipher 4 (RC4). V TKIP je zahrnuta funkce míchání klíčů a rozšířený prostor IV pro konstrukci

nesouvisejících a čerstvých klíčů na pakety. WPA zavedl Michaelův algoritmus pro zlepšení integrity dat. Kromě toho WPA implementuje mechanismus sekvenování paketů tím, že na každý paket naváže monotónně rostoucí číslo sekvence.[14]

WPA Personal a Enterprise

WPA přišel s cílem vyřešit problémy v metodě kryptografie WEP, aniž by uživatelé museli měnit hardware. Standardní WPA specifikuje dva způsoby použití:

1) Osobní WPA nebo WPA-PSK (Key Pre-Shared), které se používají pro ověřování v malých kancelářích a domácnostech pro domácí použití, které nepoužívá ověřovací server.

2) Enterprise WPA nebo Commercial, kde autentizaci provádí autentizační server 802.1x. Tato verze WPA používá pro autentizaci protokol 802.1X a EAP, ale znovu nahrazuje WEP pokročilejším šifrováním TKIP. Zde se nepoužívá žádný sdílený klíč, ale je potřeba zapojit server RADIUS do sítě. Protokol 802.1X s EAP přináší řadu výhod, jako jsou integrace přihlašování procesem Windows a podpory metod autentizace EAP-TLS a PEAP.

Hlavním důvodem, proč je WPA lepší než WEP, je to, že WPA umožňuje složitější šifrování dat na protokolu TKIP (*Temporal Key Integrity Protocol*) a je taky podporováno MIC (*Message Integrity Check*), což je funkce, která zabraňuje útokům typu překlopení bitů snadno aplikovatelné na WEP pomocí hashovací techniky.

TKIP používá stejnou metodu RC4 WEP, ale před zvýšením algoritmu RC4 provede hash. Je provedena duplikace inicializačního vektoru. Jedna kopie je odeslána do následujícího kroku a druhá je hashovaná pomocí základního klíče. Po provedení hashování se vygeneruje výsledný klíč, který se spojí s první kopií inicializačního vektoru a tak dochází k vylepšení algoritmu RC4. Poté dojde k vygenerování sekvenčního klíče s XOR z textu, který je potřeba zašifrovat, a pak proběhne vlastní šifrování dat. Nakonec je zpráva připravena k odeslání. Dešifrování bude provedeno invertováním procesu.[14]

Zlepšení WPA

Ve srovnání mezi TKIP a WEP existují čtyři vylepšení v šifrovacím algoritmu WPA, která přidala do WEP:

1) Kód integrity kryptografické zprávy (MIC) zvaný Michael, který poráží padělání.

2) Nová sekvenční disciplína inicializačního vektoru, která odstraní opakované útoky z arzenálu útočníka.

3) Funkce míchání klíčů na jeden paket k dekorelaci veřejných IV od slabých klíčů.

4) Mechanismus opakování, který poskytuje nové šifrovací klíče a klíče integrity, čímž se zbavuje hrozby útoků způsobených opakovaným použitím klíče.[15]

2.2.3 WPA Zranitelnosti

V listopadu 2003 vydal Robert Moskowitz „*Weakness in Passphrase Choice in WPA Interface*“. V tomto článku vysvětluje vzorec, který by odhalil přístupové heslo provedením slovníkového útoku proti sítím WPA-PSK.

Tato slabina byla založena na párovém hlavním klíči (PMK), který je odvozen od zřetězení přístupové fráze, SSID, délky SSID a once (číslo nebo bitový řetězec použitý v každé relaci pouze jednou). Výsledný řetězec se hashuje 4 096 krát, aby se vygenerovala 256 bitová hodnota, a pak se zkombinuje s hodnotami once. Požadované informace pro generování a ověření tohoto klíče (na relaci) jsou vysílány s běžným provozem a jsou skutečně dostupné, výzvou se pak stává rekonstrukce původních hodnot. Párový přechodný klíč (PTK) je funkce s klíčem-HMAC založená na PMK, po zachycení čtyřcestného ověřovacího handshake má útočník data potřebná k podrobení přístupové fráze útoku ze slovníku.

Ke konci roku 2004 Takehiro Takahashi, student z Georgia Tech, vydal WPA Cracker a Josh Wright, síťový inženýr a známý bezpečnostní lektor, vydal cowpatty přibližně ve stejnou dobu. Oba nástroje jsou napsány pro systémy Linux a provádějí útok slovníkovou silou proti sítím WPA-PSK ve snaze určit sdílenou přístupovou frázi. Oba vyžadují, aby uživatel dodal soubor slovníku a soubor výpisu, který obsahuje čtyřcestný handshake WPA-PSK. Obě fungují podobně, cowpatty však obsahuje automatický analyzátor, zatímco WPA Cracker vyžaduje, aby uživatel provedl manuální extrakci řetězců. Kromě toho cowpatty optimalizovala funkci HMAC-SHA1 a je o něco rychlejší. Každý nástroj používá algoritmus PBKDF2, který řídí hashování PSK k útoku a určení přístupové fráze. Proti větším přístupovým frázím však není ani extrémně rychlý, ani účinný, protože každý musí provést 4 096 HMAC-SHA1 operaci.[15]

2.2.4 WPA-2

Standard WEP je považován za zranitelný vůči útoku, protože použitý síťový klíč lze určit poměrně snadno, jednoduše zaznamenáním a analýzou dat. Standard WPA, který následoval, odstranil tuto chybu zabezpečení zavedením bezpečné autentizace, dynamického klíče a podpory služeb Radius. U WPA2 byl implementován pokročilý šifrovací algoritmus AES a dříve použitá proudová šifra RC4 byla nahrazena algoritmem TKIP. WPA2 odpovídá mnoha základním bezpečnostním prvkům standardu IEEE 802.11i a splňuje přísné bezpečnostní požadavky, jako jsou například požadavky FIPS 140-2, pro výměnu dat v amerických úřadech.

Protože sítě Wi-Fi chráněné pomocí WPA2 jsou zranitelné pouze tehdy, je-li heslo známé, měla by se používat hesla, která jsou co nejdelší se speciálními znaky, číslicemi a velkými a malými písmeny. Kromě toho je vhodné se vyhnout běžným slovům, která se nacházejí ve slovníku.

WPA-2 Personal a Enterprise

V domácnosti a v malých kancelářích se obvykle používá WPA-2 Personal s PSK (*Pre-Shared Key*) - heslo uživatele 8 znaků. Toto heslo je stejné pro všechny a je často příliš jednoduché, takže je citlivé na selekci nebo úniky (chybějící notebook, neúmyslně nalepená nálepka s heslem atd.). Ani nejnovější šifrovací algoritmy při používání PSK nezaručují spolehlivou ochranu, a proto se nepoužívají ve vážných sítích. Firemní řešení používají pro autentizaci dynamický klíč, který mění každou relaci pro každého uživatele. Klíč lze během relace pravidelně aktualizovat pomocí autorizačního serveru - obvykle serveru RADIUS.[12]

WPA2-PSK

Klient komunikuje s přístupovým bodem, autentizuje se s přístupovým bodem pomocí předem sdíleného klíče (PSK), pak přístupový bod vytvoří z PSK 256 bitový párový hlavní klíč (PMK) a identifikátor SSID. Tento PMK se používal k šifrování datového provozu pomocí TKIP nebo CCMP / AES. Je třeba poznamenat, že všichni klienti budou vždy šifrovat svá data se stejným PMK. Pokud tedy útočník prolomí PMK, může dešifrovat všechna data šifrovaná tímto PMK (minulá, současná i budoucí).[12]

WPA2-Enterprise

Klient komunikuje s přístupovým bodem, ověřuje přístupový bod, který předává tyto informace serveru RADIUS pomocí protokolu EAP. Po ověření klienta poskytuje server RADIUS přístup k přístupovému bodu a také k náhodnému 256 bitovému páru hlavního klíče (PMK) pro šifrování datového přenosu pouze pro aktuální relaci. Pokud útočník prolomí konkrétní PMK, získá přístup pouze k jedné relaci na klienta.[12]

Samotný protokol EAP je kontejner, tj. Skutečný mechanismus autorizace je uveden v hloubce interních protokolů. V současné době došlo k následujícímu významnému rozšíření.

EAP-FAST

Flexibilní ověřování prostřednictvím zabezpečeného tunelování - vyvinutý společností Cisco, umožňuje autorizaci pomocí přihlašovacího hesla přeneseného uvnitř tunelu TLS mezi žadatelem a serverem RADIUS.[12]

EAP-TLS *(Transport Layer Security)*

Používá infrastrukturu veřejného klíče (PKI) k autorizaci klienta a serveru prostřednictvím certifikátů vydaných důvěryhodnou certifikační autoritou (CA). Vyžaduje vydávání a instalaci klientských certifikátů pro každé bezdrátové zařízení, takže je vhodný pouze pro spravované podnikové prostředí. Certifikační server Windows má zařízení, která umožňují klientovi generovat certifikát samostatně, pokud je klient členem domény. Blokování klienta lze snadno provést zrušením jeho certifikátu (nebo prostřednictvím účtů).[12]

EAP-TTLS *(Tunneled Transport Layer Security)*

Podobná EAP-TLS, ale klientský certifikát není při vytváření tunelu vyžadován. V takovém tunelu, podobně jako připojení prohlížeče SSL, se provádí další autorizace (pomocí hesla nebo jinak).[12]

PEAP-MSCHAPv2 (Chráněný EAP)

Podobný EAP-TTLS, pokud jde o počáteční vytvoření šifrovaného tunelu TLS mezi klientem a serverem, který vyžaduje certifikát serveru. V budoucnu je takový tunel schválen známým protokolem MSCHAPv2.[12]

2.2.5 WPA-2 Zranitelnosti

Šifrování PSK WPA/WPA2 jsou zranitelné vůči útokům na slovníky. K provedení tohoto útoku je třeba získat čtyřcestné připojení WPA/WPA2 mezi klientem Wi-Fi a přístupovým bodem (AP). Pak zachyceny handshake musíme prolomit hrubou silou. Dalším způsobem prolomení WPA2 sítí je hackerský útok zvaný „Muž uprostřed“ (nebo zkratka MITM), je nejzávažnější hrozbou pro řádně organizovaný WPA2-Enterprise s bezpečnostními certifikáty.

Pro testování průniku v takové síti je možné vytvořit falešný Wi-Fi bod se serverem RADIUS a získat přihlašovací údaje, požadavky a odpovědi, které MS-CHAPv2 používá. To je dost pro další prolomení hesla hrubou silou. Přijaté účty mohou být použity k dalšímu proniknutí do podnikové sítě přes Wi-Fi nebo VPN a také k získání přístupu k podnikové elektronické poště.

Maximální zabezpečení sítě Wi-Fi poskytuje pouze certifikáty WPA2-Enterprise a digitální bezpečnostní certifikáty v kombinaci s protokolem EAP-TLS nebo EAP-TTLS. Certifikát je předem vygenerovaný soubor na serveru RADIUS a klientském zařízení. Klient a ověřovací server tyto soubory vzájemně kontrolují, čímž zajišťují ochranu před neoprávněným připojením z jiných zařízení a chybnými přístupovými body. Protokoly EAP-TTL/TTLS jsou součástí standardu 802.1X a používají infrastrukturu veřejných klíčů (PKI) pro výměnu dat mezi klientem a RADIUS. PKI

pro autentizaci používá tajný klíč (uživatel ví) a veřejný klíč (uložený v certifikátu, potenciálně známý všem). Kombinace těchto klíčů poskytuje spolehlivé ověření. Pro každé bezdrátové zařízení musí být vytvořené digitální certifikáty. Jedná se o pracný proces, proto se certifikáty obvykle používají pouze v sítích Wi-Fi, které vyžadují maximální ochranu. Současně lze snadno zrušit certifikát a uzamknout klienta.

Dnes poskytuje WPA2-Enterprise v kombinaci s bezpečnostními certifikáty spolehlivou ochranu podnikových sítí Wi-Fi. Při správné konfiguraci a používání je hackování takové ochrany téměř nemožné „z ulice“, tj. bez fyzického přístupu k autorizovaným klientským zařízením. Správci sítě však někdy dělají chyby, které útočníkům ponechávají „mezery“ pro proniknutí do sítě. Problém je komplikován dostupností softwaru pro hackování a postupnými pokyny, které mohou použít i amatéři.

Správce musí pravidelně kontrolovat podezření na síťový provoz, včetně zpoždění při přenosu paketů. V oblastech s kritickými transakcemi se doporučuje nainstalovat senzory Wi-Fi pro detekci hackerské aktivity v reálném čase. Zvláštním místem v prevenci MITM je odmítnutí používat filtrování pomocí SSL. V kancelářích se často používá k zákazu přístupu na určité stránky (sociální sítě, zdroje zábavy atd.). [12]

2.3 Bezpečnostní hrozby bezdrátových sítí

Bezdrátové technologie, které fungují bez fyzických a logických omezení svých kabelových protějšků, tedy výrazně zvyšují flexibilitu pracovního toku a produktivitu uživatelů a snižují náklady na nasazení v síti, rovněž vystavují síťovou infrastrukturu a uživatele významným rizikům. V této kapitole jsou uvedena nejznámější bezpečnostní rizika bezdrátových sítí 802.11.[9]

2.3.1 Rogue Devices

Rogue Devices jsou zařízení, která umožňují neoprávněný přístup k podnikové síti, často obcházejí ochranné mechanismy definované v zásadách podnikové bezpečnosti. Nejčastěji se jedná o stejné neautorizované přístupové body. Statistiky po celém světě například poukazují na *rogue devices* jako na hlavní příčinu většiny hacků v sítích organizací. I když organizace nepoužívá bezdrátovou komunikaci a považuje se za chráněnou před bezdrátovými útoky v důsledku takového zákazu, může narušitel (úmyslně či nikoli) tuto situaci snadno napravit. Dostupnost a nízké náklady na zařízení Wi-Fi vedly k tomu, že například ve Spojených státech měla téměř každá síť s více než 50 uživateli čas se s tímto jevem seznámit. Kromě přístupových bodů může jako cizinec fungovat domácí router s Wi-Fi, softwarový přístupový bod Soft

AP, notebook se zapnutým kabelovým i bezdrátovým rozhraním, skener, projektor atd.[9]

2.3.2 Zranitelnosti sítí a zařízení

Některá síťová zařízení mohou být zranitelnější než jiná - mohou být nesprávně nakonfigurována, používat slabé šifrovací klíče nebo používat metody ověřování se známými chybami zabezpečení. Není divu, že na ně počítačoví zločinci útočí. Analytické zprávy tvrdí, že více než 70 procent úspěšných bezdrátových útoků je způsobeno nesprávnou konfigurací přístupových bodů nebo klientského softwaru.[9]

Nesprávně nakonfigurované přístupové body

Jeden nesprávně nakonfigurovaný přístupový bod může způsobit napadení podnikové sítě. Výchozí nastavení většiny přístupových bodů nezahrnuje ověřování ani šifrování ani nepoužívá statické klíče napsané v příručce, a proto jsou obecně známé. V kombinaci s nízkými náklady na přístupové body tento faktor významně komplikuje úkol sledování integrity konfigurace bezdrátové infrastruktury a úrovně její ochrany. Zaměstnanci organizace mohou libovolně přinést přístupové body a připojit je, kdekoli se jim líbí. Je nepravděpodobné, že by současně věnovali dostatečnou pozornost své kompetentní a bezpečné konfiguraci a koordinovali své akce s oddělením IT. To jsou body, které představují největší hrozbu pro kabelové a bezdrátové sítě.[9]

Nesprávně nakonfigurovaní bezdrátoví klienti

Nesprávně nakonfigurovaná uživatelská zařízení představují ještě větší hrozbu než nesprávně nakonfigurované přístupové body. Tato zařízení doslova přicházejí a odcházejí z podniku, často nejsou specificky konfigurována tak, aby minimalizovala bezdrátová rizika, a jsou obsahem s výchozí konfigurací (kterou nelze ve výchozím nastavení považovat za bezpečnou). Tato zařízení jsou neocenitelná, protože pomáhají hackerům proniknout do kabelové sítě a poskytují pohodlný vstupní bod pro skenování sítě a distribuci malwaru v ní.[9]

Zastaralé šifrovací algoritmy

Útočníci již dlouho měli přístup ke speciálním nástrojům ke kompromitaci sítí založených na šifrovacím standardu WEP (viz riziko 4). Tyto nástroje jsou široce hlášeny na internetu a jejich použití nevyžaduje žádné speciální dovednosti. Využívají chyby zabezpečení v algoritmu WEP pasivním shromažďováním statistik provozu v bezdrátové síti, dokud se neshromáždí dostatek dat k obnovení šifrovacího klíče. Pomocí

nejnovější generace nástrojů prolomení WEP, které používají speciální techniky injektování provozu, se doba prolomení bezpečnosti šití pohybuje od 15 minut do 15 sekund. Podobně existují zranitelnosti různé závažnosti a složitosti, které mohou narušit TKIP a dokonce i WPA2. Jedinou „neproniknutelnou“ metodou je zatím použití protokolu WPA2-Enterprise (802.1x) minimálně s certifikátem serveru.[9]

2.3.3 Nové hrozby a útoky

Bezdrátové technologie přinesly nové způsoby implementace starých hrozeb, stejně jako některé nové, dosud nemožné v kabelových sítích. Ve všech případech bylo mnohem obtížnější bojovat s útočníkem, protože není možné sledovat jeho fyzické umístění nebo jej izolovat od sítě.[9]

Průzkum WLAN sítí

Většina tradičních útoků začíná průzkumem, v důsledku čehož útočník určí další cestu útoku. Pro bezdrátový průzkum se používají jak nástroje pro skenování bezdrátové sítě (NetStumbler, Wellenreiter, vestavěný klient JC), tak nástroje pro sběr a analýzu paketů, mnoho řídicích paketů WLAN je nezašifrovaných. Současně je velmi obtížné odlišit stanici, která shromažďuje informace, od běžné stanice, která se pokouší získat autorizovaný přístup k síti, nebo od pokusu o náhodné přiřazení. Mnoho lidí se snaží chránit své sítě skrytím názvu sítě v majácích odeslaných přístupovými body a deaktivací odpovědi na *Broadcast ESSID*. Tyto metody, které patří do třídy *Security through Obscurity*, jsou nepochybně nedostatečné, protože útočník stále vidí bezdrátovou síť na určitém rádiovém kanálu a zbývá mu jen počkat na první autorizované připojení k takové síti, protože v průběhu takového spojení se ESSID přenáší vzduchem v nezašifrované podobě. Poté takové bezpečnostní opatření jednoduše ztratí svůj význam. Některé funkce bezdrátového klienta Windows XP SP2 (revidované v aktualizaci SP3) situaci ještě zhoršily. klient neustále vysílal název takové skryté sítě a pokoušel se připojit. Výsledkem bylo, že útočník nejen obdržel název sítě, ale mohl také „zavěsit“ takového klienta na svůj přístupový bod.[9]

Předstírání jiné identity a krádež identity

Vydávání se za autorizovaného uživatele je vážnou hrozbou pro jakoukoli síť, nejen bezdrátovou. V bezdrátové síti je však ověření uživatele obtížnější. Samozřejmě existují SSID a můžete se pokusit filtrovat podle MAC adres, ale oba jsou přenášeny vzduchem v čistém stavu a oba lze snadno padělat. Existují způsoby vložení nesprávných rámců, aby došlo k porušení autorizované komunikace a taky útoky na síťovou strukturu (například *ARP Poisoning*, jako v případě nedávno objevené chyby zabezpečení TKIP).

Existuje falešná víra, že zosobnění uživatele je možné pouze pomocí ověřování MAC nebo statických klíčů, a že schémata založená na standardu 802.1x jsou zcela zabezpečená. Bohužel tomu tak již není. Některé mechanismy (LEAP) lze snadno prolomit jako WEP. Další schémata, například EAP-FAST nebo PEAP-MSCHAPv2, jsou spolehlivější, ale nezaručují odolnost vůči složitému útoku, který využívá několik faktorů současně.[9]

Odmítnutí služby (DoS)

Cílem útoku *Denial of Service* je buď porušení výkonu síťových služeb, nebo úplné vyloučení možnosti přístupu k nim pro oprávněné uživatele. Síť může být například zaplavena pakety „odpadků“ (s nesprávným kontrolním součtem atd.) Odesílaných z legitimní adresy. V případě bezdrátové sítě není možné jednoduše zjistit zdroj takového útoku bez speciálních nástrojů, může to být kdekoli. Kromě toho je možné uspořádat *DoS* na fyzické vrstvě jednoduše spuštěním dostatečně výkonného rušiče v požadovaném frekvenčním rozsahu.[9]

Specializované útočné nástroje

Nástroje pro organizování útoků na bezdrátové sítě jsou široce dostupné a jsou neustále aktualizovány novými nástroji, od známých *AirCrack* až po cloudové služby pro dešifrování hash. Navíc, jakmile je získán přístup, jsou použity tradiční nástroje vyšších úrovní.[9]

2.3.4 Únik informací z kabelové sítě

Téměř všechny bezdrátové sítě se v určitém okamžiku připojují ke kabelovým sítím. Proto může být jakýkoli bezdrátový přístupový bod použit jako odrazový můstek pro útok. Ale to není vše: některé chyby v konfiguraci přístupových bodů v kombinaci s chybami v konfiguraci kabelové sítě mohou otevřít cesty k úniku informací. Nejběžnějším příkladem jsou přístupové body mostu vrstvy 2 připojené k ploché síti (nebo síti s porušením segmentace VLAN) a vysílání z kabelového segmentu, požadavky ARP, požadavky DHCP, rámce STP atd. Některá z těchto dat mohou být užitečná pro organizování útoků typu *Man-in-The-Middle*, různých útoků *Poisoning* a *DoS*.[9]

Další běžný scénář je založen na specifikách implementace protokolů 802.11. V případě, že je na jednom přístupovém bodu nakonfigurováno několik ESSID najednou, přenos vysílání se rozšíří na všechny ESSID najednou. Výsledkem je, že pokud je v jednom bodě nakonfigurována zabezpečená síť a veřejný hotspot, může útočník připojený k hotspotu například narušit protokoly DHCP nebo ARP v zabezpečené

síti. To lze napravit uspořádáním kompetentní vazby ESS na BSS, kterou podporují téměř všichni výrobci zařízení třídy Enterprise (a několik z třídy Consumer).[9]

2.4 Možnosti zachytávání Wi-Fi provozu a útoky bezdrátové síti

Zachytávání dat v síti je příjem veškerých informací ze vzdáleného počítačového zařízení. Může se skládat z osobních údajů uživatele, jeho zpráv, záznamů o návštěvách webových stránek. Sběr dat lze provádět pomocí spywaru nebo snifferu. Spyware je speciální software, který dokáže zaznamenávat všechny informace přenášené po síti z konkrétní pracovní stanice nebo zařízení. Sniffer je program nebo počítačový hardware, který zachycuje a analyzuje provoz, procházející sítí. Sniffer umožňuje připojit se k webové relaci a provádět různé operace jménem vlastníka počítače.

Pokud informace nejsou přenášeny v reálném čase, spyware generuje záznam provozu do souborů, které jsou vhodné pro prohlížení a analýzu informací později. Odposlech sítě může být legitimní nebo nezákonný. Hlavním dokumentem, který opravuje zákonnost zabavení informací, je Úmluva o počítačové kriminalitě. Byla založena v Maďarsku v roce 2001. Právní požadavky různých zemí se mohou mírně lišit, ale klíčové sdělení je stejné pro všechny země.[10]

2.4.1 Klasifikace a metody zachycování dat v síti

V souladu s výše uvedeným lze odposlech informací v síti rozdělit na dva typy: autorizované a neautorizované. Autorizovaný sběr dat se provádí pro různé účely, od ochrany podnikových informací po zajištění bezpečnosti státu. Důvody pro takovou operaci určují právní předpisy, speciální služby, úředníci donucovacích orgánů, odborníci ze správních organizací a bezpečnostní služby společnosti.

Existují mezinárodní standardy pro provádění zachycování dat. Evropskému institutu pro normalizaci v telekomunikacích se podařilo přivést řadu technických procesů (ETSI ES 201 158 „Telekomunikační bezpečnost, Zákonné odposlechy (LI), Požadavky na funkce sítě) na jednotnou normu, na které je odposlech založen. Ve výsledku byla vyvinuta systémová architektura, která pomáhá specialistům tajných služeb, správcům sítě, legálně převzít data ze sítě. Vyvinutá struktura implementace odposlechu dat přes síť se používá pro kabelové a bezdrátové systémy hlasového volání, stejně jako pro korespondenci poštou, přenos hlasových zpráv přes IP, výměnu informací pomocí SMS.

Neoprávněné zachycení dat v síti provádějí počítačoví zločinci, kteří se chtějí zmocnit důvěrných dat, hesel, podnikových tajemství, adres počítačů v síti atd.

K dosažení svých cílů hackeři obvykle používají analyzátor síťového provozu - sniffer. Tento program nebo zařízení typu hardwaru a softwaru umožňuje podvodníkovi zachytit a analyzovat informace v síti, ke které je uživatel oběti připojen, včetně šifrovaného přenosu SSL prostřednictvím spoofingu certifikátu.

Data lze získat různými způsoby:

1. Poslech síťového rozhraní;
2. Připojení odposlechového zařízení ke kanálové mezeře;
3. Vytvoření větve provozu a jeho duplikování;
4. Provedení útoku snifferem.

Existují také sofistikovanější technologie pro zachycení citlivých informací, které umožňují zasahovat do síťové komunikace a měnit data. Jednou z takových technologií jsou falešné ARP požadavky. Podstatou metody je spoofování IP adres mezi počítačem oběti a zařízením útočníka. Další metodou, kterou lze použít k zachycení dat v síti, je falešné směrování. Spočívá v nahrazení IP adresy síťového routeru jeho vlastní adresou. Pokud počítačový zločinec ví, jak je uspořádána místní síť, ve které se oběť nachází, může snadno uspořádat příjem informací ze zařízení uživatele na jeho IP adresu. Únos TCP spojení je také efektivní způsob, jak zachytit data. Útočník přeruší komunikační relaci generováním a odesláním paketů TCP do počítače oběti. Poté je komunikační relace obnovena, zachycena a pokračuje zločincem místo klienta.[7]

2.4.2 Předmět odposlechu

Objektem odposlechu dat v síti mohou být vládní agentury, průmyslové podniky, komerční struktury, běžní uživatelé. V rámci organizace nebo obchodní společnosti lze implementovat sběr informací k ochraně síťové infrastruktury. Speciální služby a orgány činné v trestním řízení mohou provádět masivní odposlech informací přenášených od různých vlastníků, v závislosti na daném úkolu. Pokud mluvíme o útočnících, pak se každý uživatel nebo organizace může stát předmětem vlivu, aby získal data přenášená přes síť. S autorizovaným přístupem je důležitá informativní část obdržených informací, zatímco útočník se více zajímá o data, která lze použít k získání peněz nebo cenných informací pro jejich následný prodej. Nejčastějšími oběťmi odposlechu informací zločinci jsou uživatelé připojující se k veřejné síti, například v kavárně s hotspotem Wi-Fi. Útočník se připojí k webové relaci pomocí snifferu, zfalšuje data a ukradne osobní údaje.[7]

2.4.3 Zdroj ohrožení

Provozovatelé veřejné síťové infrastruktury se podílejí na autorizovaném odposlechu informací ve společnostech a organizacích. Jejich činnost je zaměřena na ochranu

osobních údajů, obchodního tajemství a dalších důležitých informací. Z právních důvodů může být přenos zpráv a souborů sledován speciálními službami, donucovacími orgány a různými vládními agenturami, aby byla zajištěna bezpečnost občanů a státu. Útočníci se zabývají nelegálním zachycením dat. Aby se uživatelé nestali obětí počítačového zločince, musí dodržovat některá doporučení odborníků. Například by neměli provádět operace, které vyžadují autorizaci a přenos důležitých dat na místech, kde se připojují k veřejným sítím. Je bezpečnější zvolit šifrované sítě, nebo ještě lépe používat osobní modemy 3G a LTE. Při přenosu osobních údajů se doporučuje šifrování pomocí protokolu HTTPS nebo osobního tunelu VPN. Svůj počítač by měli chránit před zachycením síťového provozu pomocí kryptografie a anti-sniffers zařízení.[7]

2.4.4 Přehled metod zachytávání provozu

Odposlech - Sniffing

V praxi jsou sítě IP zranitelné vůči řadě neoprávněných vniknutí do komunikačního procesu. S rozvojem počítačových a síťových technologií (například s příchodem mobilních aplikací Java a ovládacích prvků ActiveX) se seznam možných typů síťových útoků na sítě IP neustále rozšiřuje. Odposlech je v dnešní době jedním z nejčastějších útoků. Odposlech (sniffing) – data se z větší části přenášejí přes počítačové sítě v nechráněném formátu (prostý text), což umožňuje útočníkovi získat přístup k datovým linkám ve vaší síti k odposlechu nebo čtení provozu. K odposlechu počítačových sítí se používá sniffer. Packet sniffer je aplikační program, který zachycuje všechny síťové pakety přenášené přes konkrétní doménu. Sniffery se používají pro řešení problémů a analýzu provozu. Nicméně vzhledem k tomu, že některé síťové protokoly přenášejí data v textovém formátu (Telnet, FTP, SMTP, POP3 atd.), útočník může pomocí sledovače zjistit užitečné a někdy důvěrné informace (například uživatelská jména a hesla). Zachycení hesla ve formátu prostého textu přenášeného po síti odposlouchávánim kanálu je typem odposlechového útoku známého jako *password sniffing*. Zachytávání uživatelských jmen a hesel je velmi nebezpečné, protože uživatelé často používají stejné uživatelské jméno a heslo pro více aplikací a systémů. Pokud aplikace běží v režimu klient-server a ověřovací data jsou přenášena po síti v čitelném textovém formátu, lze tyto informace s největší pravděpodobností použít pro přístup k dalším podnikovým nebo externím prostředkům.

V síti existují dva typy snifferu podle kategorií: win sniffers (linux sniffers), určené k zachycení síťového provozu přes místní kabelové a bezdrátové sítě Wi-Fi a globální pomocí konfigurací Windows (Linux) a http sniffers (jsou také online sniffers), které jsou také určeny k zachycování informací, zejména v globálním internetu, ale s využitím programových prostředků na webových serverech PHP na internetu. Analýza

provozu procházejícího sledovačem umožňuje:

– Zjisit parazitický virus;

– Identifikovat škodlivý a neoprávněný software v síti, například síťové skenery, trojské koně, klienty sítí peer-to-peer;

– Vyhledat nefunkčnost sítě nebo chybu konfigurace v síťových agentech (pro tento účel správci systému často používají sniffery).

Odposlech lze provádět:

– prostřednictvím analýzy rušivých elektromagnetických emisí a obnovením naslouchajícího provozu tímto způsobem;

– útokem na kanál (*MAC spoofing*) nebo síťovou vrstvu (*IP spoofing*), který vede k přesměrování provozu oběti nebo veškerého provozu segmentu na sniffera s následným návratem provozu na správnou adresu.

Existují dva způsoby, jak poslouchat sítě: pasivní a aktivní. S pasivním odposlechem sniffer jednoduše přepne síťovou kartu do promiskuitního režimu a přijme veškerý provoz procházející počítačem, aktivní odposlech vyžaduje přijetí zvláštních opatření, aby se přinutil přenos přenášet na sebe, a to i z jiného segmentu sítě. Aktivní odposlech je další věc, existuje velké množství aktivních metod poslechu, například:

– Zaplavení MAC funguje na mnoha levných a zastaralých modelech Switchů. Přepínač má paměť pro ukládání tabulky adres (korespondence mezi MAC adresou a portem, na který budou data zasílána), pokud tato paměť přeteče falešnými adresami, přepínač přestane ovládat přenos. Tato metoda funguje také na mostech.

– Duplikování MAC – tento útok je jednoduchým spoofováním MAC adresy oběti. Problém je v tom, že zachycená data nedosahují cílového počítače a lze jednoduše identifikovat útočníka v síti, navíc tímto způsobem útočník může zachytit pouze data směřující k oběti, ale ne naopak. Aby uživatelé zabránili ohrožení odposlechů paketů, mohou použít následující opatření a nástroje: použít k ověření jednorázová hesla, instalace hardwaru nebo softwaru, který rozpoznává sniffery, aplikace kryptografické ochrany komunikačních kanálů.[7]

ARP-spoofing

ARP-spoofing (ARP-poisoning) je technika síťového útoku používaná hlavně v Ethernetu, ale je možná v jiných sítích využívajících protokol ARP, založená na využití nedostatků protokolu ARP a umožnění zachycení provozu mezi uzly, které se nacházejí ve stejné vysílací doméně. Je jedním z typů spoofing útoků. ARP je protokol pro převod IP adres na MAC adresy. Nejčastěji mluvíme o převodu na ethernetové adresy, ale ARP se používá také v sítích jiných technologií: Token Ring, FDDI a dalších.

Algoritmus ARP

Protokol lze použít v následujících případech:

– Hostitel A chce odeslat IP paket hostiteli B, který je s ním ve stejné síti;

– Hostitel A chce odeslat IP paket na hostitele B v různých sítích a využívá služby routeru R.

V obou případech bude hostitel A používat ARP, pouze v prvním případě k určení MAC adresy hostitele B a ve druhém k určení MAC adresy routeru R. V druhém případě bude paket předán routeru pro další předávání. Případ, kdy je paket adresován hostiteli za routerem, se liší pouze v tom, že pakety přenášené po dokončení převodu ARP používají IP adresu příjemce, ale MAC adresu routeru, nikoli příjemce.

Problémy s ARP

ARP je zcela nejistá. Nemá žádný způsob, jak ověřit balíčky, požadavky i odpovědi. Situace se stává ještě komplikovanější, když lze použít bezdůvodný ARP (spontánní ARP). Spontánní ARP je chování ARP, když je odeslána odpověď ARP, když to není potřeba (z pohledu příjemce). Spontánní odpověď ARP je paket odpovědi ARP odeslaný bez požadavku. Slouží k detekci konfliktů IP adres v síti: jakmile stanice obdrží adresu prostřednictvím DHCP nebo je adresa přidělena ručně, je odeslána odpověď ARP. Spontánní ARP může být užitečné v následujících případech:

– Aktualizace tabulek ARP;

– Informování přepínače;

– Oznámení o zapojení síťového rozhraní.

Navzdory účinnosti spontánního ARP je obzvláště nejistý, protože jej lze použít k zajištění vzdáleného hostitele, že se změnila adresa MAC systému ve stejné síti, a indikovat, která adresa se nyní používá.

Princip činnosti ARP spoofingu

1. Dva počítače (uzly) M a N v místní síti Ethernet si vyměňují zprávy. Útočník X ve stejné síti chce zachytit zprávy mezi těmito uzly. Předtím, než se ARP spoofing použije na síťové rozhraní uzlu M, obsahuje tabulka ARP adresy IP a MAC uzlu N. Také v síťovém rozhraní uzlu N obsahuje tabulka ARP adresy IP a MAC uzlu M.

2. Během útoku spoofingu ARP hostitel X (útočník) odešle dvě odpovědi ARP (bez požadavku) - na hostitele M a hostitele N. Odpověď ARP na hostitele M obsahuje IP adresu N a MAC adresu X. ARP odpověď na hostitel N obsahuje IP-adresu M a MAC adresu X.

3. Vzhledem k tomu, že počítače M a N podporují spontánní ARP, po přijetí odpovědi ARP změní své tabulky ARP a tabulka ARP M nyní obsahuje adresu MAC X spojenou s adresou IP N a tabulka ARP N obsahuje adresu MAC přidruženou k adrese X s M.

4. Provádí se tedy spoofing útoku ARP a nyní všechny pakety (přenosy) mezi M a N procházejí X. Například pokud M chce poslat paket N, pak M prohlédne svou tabulku ARP, najde položku s IP adresou hostitele N, vybere odtud MAC adresu (a MAC adresa uzlu X již existuje) a odešle paket. Paket dorazí na rozhraní X, analyzuje se a poté se předá do uzlu N.

Pro realizace útoku pomocí ARP spoofing existují programy jako jsou: Ettercap, Bettercap, dsniff, arp-sk ARP Builder a jiné.[7]

Falešný HotSpot a Man-in-the-middle útok

Zachycení nešifrovaných paketů ze vzduchu není jediný způsob, jak může být veřejné Wi-Fi připojení nebezpečné. Jakmile byl vytvořen nepoctivý hotspot, lze se všemi daty protékajícími tímto hotspotem manipulovat. Nejlepší formou manipulace je přesměrování provozu na jiný web, který je klonem populárního webu, ale je falešný. Jediným cílem webu je sběr osobních údajů. Je to stejná technika jako při phishingových e-mailových útocích. Ještě nákladnější je to, že hackeři nepotřebují falešný hotspot, aby mohli manipulovat s vaším provozem. Každé síťové rozhraní Ethernet a Wi-Fi má jedinečnou adresu MAC. Zařízení, včetně routerů, objevují MAC adresy jiných zařízení, pomocí použití ARP, Address Resolution Protocol. V zásadě stanice uživatele odešle žádost s dotazem, které zařízení v síti používá určitou IP adresu. Majitel odpoví svou MAC adresou, aby na něj pakety mohly být fyzicky směrovány.

Problém s ARP je v tom, že může být změněn. To znamená, že zařízení uživatele zeptá na určitou adresu, řekněme adresu routeru Wi-Fi a další zařízení odpoví falešnou adresu. V prostředí Wi-Fi, dokud bude signál z falešného zařízení silnější než signál ze skutečného zařízení, bude síťové zařízení uživatele oklamáno. Po aktivaci spoofingu bude klientské zařízení posílat všechna data do falešného routeru spíše než do skutečného routeru, odtud falešný router může manipulovat s provozem, který však považuje za vhodný. V nejjednodušším případě pakety budou zachyceny a poté přeposlány na skutečný router, ale s návratovou adresou falešného přístupového bodu, aby mohl také zachytit odpovědi.[7]

SSL strip útok

Tento útok může útočníkovi umožnit nenápadně zfalšovat zabezpečené připojení (HTTPS) otevřeným (HTTP) připojením. Při použití tohoto útoku je veškerý provoz z počítače oběti odesílán prostřednictvím serveru proxy vytvořeného útočníkem, který nahradí všechny odkazy HTTPS protokolem HTTP. V tomto příkladu budeme uvažovat o útoku na SSL přes HTTP, známý také jako HTTPS, protože se jedná o nejběžnější model implementace protokolu SSL a používá se téměř ve všech systémech bankovních síťových aplikací, e-mailových služeb k zajištění šifrování komunikačního kanálu. Tato technologie je navržena tak, aby zajistila bezpečnost dat

před zachycením třetími stranami pomocí jednoduchého sledovače paketů.

Uvažujme o procesu komunikace přes HTTPS na příkladu připojení uživatele k účtu Google. Tento proces zahrnuje několik samostatných operací:

– Prohlížeč klienta přistupuje na google.com na portu 80 pomocí protokolu HTTP.

– Server přesměrovává klientskou verzi HTTPS tohoto webu pomocí přesměrování 302.

– Klient se připojí k google.com na portu 443.

– Server předá svůj certifikát veřejného klíče klientovi k ověření webu.

– Klient ověří tento certifikát podle seznamu důvěryhodných CA.

– Vytvoří se šifrované připojení.

Ze všech těchto akcí je nejzranitelnější operace přesměrování na HTTPS prostřednictvím kódu odpovědi HTTP 302. K provedení útoku na přechodový bod z nechráněného do zabezpečeného kanálu byl vytvořen speciální nástroj SSLStrip. Pomocí tohoto nástroje vypadá proces útoku takto:

– Zachytávání provozu mezi klientem a webovým serverem.

– Když je nalezena adresa HTTPS URL, SSLstrip ji nahradí odkazem HTTP, který odpovídá všem změnám.

– Útočící stroj poskytuje certifikáty webovému serveru a vydává se za klienta.

– Provoz je přijímán ze zabezpečeného webu a poskytován klientovi.

Výsledkem je, že útočník získá přístup k datům, která klient odešle na server. Těmito údaji mohou být hesla k účtu, čísla bankovních karet nebo jakékoli jiné informace, které se obvykle přenášejí ve skryté formě. Potenciálním signálem pro tento útok pro klienta může být nedostatek označení chráněného provozu HTTPS v prohlížeči. U serveru tato substituce zůstane zcela bez povšimnutí, protože v provozu SSL nejsou žádné změny.[7]

SSL Strip plus

Toto je nová verze SSL Strip s novou funkcí, jak obejít ochranný mechanismus *HTTP Strict Transport Security* (HSTS). Tato verze, stejně jako originál, mění HTTPS na HTTP plus název hostitele v html kódu, aby se zabránilo HSTS. Aby to fungovalo, útočník potřebuje také server DNS, který obrátí změny provedené serverem proxy.[7]

DNS Spoofing

Spoofing DNS, známý také jako otrava mezipaměti, je typ útoku, při kterém je mezipaměť DNS naplněna falešnými daty, což vede k přesměrování uživatele na škodlivý web. Otrava mezipaměti DNS je výsledkem zranitelností, které zločincům umožňují odesílat falešné odpovědi DNS, které servery DNS (*Domain Name Server*) ukládají do jejich mezipaměti. Prolomený záznam obvykle uživatele přesměruje na falešný

web, který útočníci používají ke spáchání trestných činů, jako je distribuce malwaru nebo krádež podrobností o kreditní kartě, hesel, finančních údajů nebo jiných důvěrných a soukromých informací. Když je mezipaměť DNS otrávena, server mezipaměti DNS uloží nelegitimní adresu poskytnutou útočníkem a poté ji vydá uživatelům požadujícím autentický web. Ve většině případů může vypadat podobně jako autentický web, což návštěvníkům ztěžuje rozlišení falešného webu od skutečného.

Spoofing DNS je obvykle obtížné detekovat a může mít velký negativní dopad, zejména na populární webové stránky nebo webové aplikace s velkým počtem návštěv nebo registrovaných uživatelů. To představuje velké riziko, zejména v některých citlivých odvětvích, jako je bankovnictví, zdravotnictví, online maloobchod, elektronický obchod a další. Například se předpokládá, že se útočníkům podaří změnit záznamy DNS a IP adresy pro Amazon. Poté požadavek předají jinému serveru s falešnou IP adresou, kterou útočníci ovládají nebo vlastní. Každý, kdo se pokusí získat přístup ke skutečnému webu společnosti Amazon, bude přesměrován na nesprávnou adresu, která může obsahovat malware, aby ukradla citlivé informace. Kromě webových stránek může útočník vložit falešnou adresu pro e-mailový server nebo jiné webové aplikace, jako jsou bankovní aplikace. Jelikož se změny DNS pravidelně šíří z jednoho serveru na druhý, může se otrávená mezipaměť šířit na jiné servery a systémy DNS, což způsobí velké škody. Falešný záznam se může například rychle rozšířit na další počítače, například na servery DNS poskytovatelů internetových služeb, které jej poté uloží do své mezipaměti. Odtud se dále rozšiřuje na uživatelské vybavení, jako jsou prohlížeče, mobilní telefony a směrovače, které také do svých mezipamětí uloží falešný záznam.

Princip fungování DNS Spoofing útoku

Zločinci mohou otrávit mezipaměť DNS pomocí různých technik. Během běžných operací se dotazy DNS ukládají do mezipaměti v databázi, na kterou se uživatelé webových stránek mohou dotazovat v reálném čase. Databáze DNS obvykle obsahuje seznam internetových jmen a odpovídajících IP adres. A usnadňuje hledání a přístup na webové stránky pomocí jmen na rozdíl od IP adres, což může být velmi komplikované a matoucí. Například bez systému DNS si uživatelé budou muset pamatovat řetězec čísel, který tvoří adresy IP všech webů, které chtějí navštívit. DNS má bohužel několik bezpečnostních nedostatků, které mohou útočníci zneužít a vložit do systému falešné záznamy adres internetových domén. Zločinci obvykle zasílají falešné odpovědi na server DNS. Server poté odpoví uživateli, který podal požadavek, a zároveň legitimní servery falešnou položku uloží do mezipaměti. Jakmile server mezipaměti DNS uloží falešný záznam, obdrží všechny následné požadavky na prolomený záznam adresu serveru ovládaného útočníkem. Otrava mezipaměti DNS obvykle spočívá v injektování poškozených položek do mezipaměti databáze

jmenného serveru a útočníci používají různé metody. Tyto zahrnují:

– Když uživatel webu nebo webové aplikace odešle požadavek na konkrétní doménu prostřednictvím prohlížeče nebo online aplikace, server DNS nejprve zkontroluje, zda položka existuje v mezipaměti. Pokud není uložen, požádá autoritativní servery DNS o informace a poté počká na odpověď. Útočníci po určitou dobu využijí toto období úzké latence, dočasně převezmou roli původního DNS a vydají falešnou odpověď, než autoritativní server odešle platnou adresu. Protože však čekací doba je obvykle velmi krátká, je úspěšnost velmi nízká.

– Další metoda zahrnuje zasílání falešných odpovědí ze serveru DNS, který se vydává za legitimní. Protože se ověřování DNS obvykle neprovádí, mohou útočníci při dotazování na jmenný server zfalšovat odpověď od překladače DNS. To také umožňuje skutečnost, že servery DNS místo protokolu TCP používají protokol *User Datagram Protocol* (UDP). Komunikace DNS je obvykle nezabezpečená kvůli nezašifrovaným informacím v paketech UDP a nedostatku ověřování. To útočníkům usnadňuje vkládání falešných adres do odpovědí.

Způsoby zabezpečení proti DNS spoofing útoku

Monitorování dat DNS v reálném čase může pomoci identifikovat neobvyklé vzorce, akce uživatelů nebo chování, jako je návštěva škodlivých webů v provozu. I když je detekce otravy mezipaměti DNS obtížná, existuje několik bezpečnostních opatření, která mohou společnosti a poskytovatelé služeb přijmout, aby tomu zabránili. Některá opatření k zabránění otravě mezipaměti DNS zahrnují použití DNSSEC, zakázání rekurzivních dotazů a další.

Vysoká úroveň důvěry

Jednou ze slabých míst v transakcích DNS jsou vysoké vztahy důvěryhodnosti mezi různými servery DNS. To znamená, že servery neověřují záznamy, které dostávají, což umožňuje útočníkům dokonce posílat falešné odpovědi ze svých nelegitimních serverů. Aby útočníci nemohli tuto chybu zneužít, musí skupiny zabezpečení omezit úroveň důvěry jejich serverů DNS vůči ostatním. Konfigurace serverů DNS tak, aby se nespoléhaly na vztahy důvěryhodnosti s jinými servery DNS, znesnadňuje kyberzločincům použití serveru DNS ke kompromitování záznamů na legitimních serverech. Existuje mnoho nástrojů pro kontrolu bezpečnostních hrozeb DNS.

DNS Sec protokol

Rozšíření zabezpečení názvu domény (DNSSEC) používají k podepisování záznamů DNS kryptografii veřejného klíče, takže přidávají ověření a umožňují systémům určit, zda je adresa legitimní či nikoli. To pomáhá ověřit autenticitu požadavků a odpovědí, a tím zabránit neoprávněné manipulaci. Za normálního provozu bude DNSSEC

přidružen jedinečný kryptografický podpis k dalším informacím DNS, jako jsou záznamy CNAME. Překladač DNS poté použije tento podpis k ověření odpovědi DNS před odesláním uživateli. Podpisy zabezpečení zajišťují, že odpovědi na požadavky, které uživatelé obdrží, jsou ověřeny legitimním serverem původu. Zatímco DNSSEC může zabránit otravě mezipaměti DNS, má v dřívějších verzích nevýhody, jako je složité nasazení, zřizování dat a výčet zón.[7]

Captive portal útok

Captive portál je samotné okno, které se zobrazí, když se uživatel připojí k veřejné síti, kde je zpravidla nutné provést některé akce, například kliknout na „Přihlásit“. Tato okna se používají k ověřování, zobrazování reklam a účtování poplatků za přístup k internetu. Útočník může pomocí této technologie ukázat oběti podobnou stránku, která bude obsahovat formulář pro zadání bankovní karty, účtu ze sociální sítě, nebo to může být jednoduše stránka s aktualizací, kterou je nutné urgentně nainstalovat. Instalace takových aktualizací však může útočníkovi poskytnout plný přístup k zařízení nic netušícího uživatele.[7]

2.5 Přehled hardwaru pro odposlech bezdrátové síti

Vzhledem k tomu, že ne všechny adaptéry, jejichž ovladače mohou zachytit bezdrátové přenosy a zároveň je zveřejňovat, je-li to nutné, v kapitole jsou uvedené vhodné bezdrátové síťové adaptéry.

2.5.1 Přehled zařízení pro pasivní odposlech

Alfa AWUS-036NHA

Zařízení s podporou Wi-Fi 2,4 GHz 802.11n. Jedná se o velmi univerzální kartu Wi-Fi za posledních několik let. Podporuje monitorovací schéma pro linuxové distribuční společnosti jako Kali Linux, Debian a další. Podporuje také Windows, který je určen k vytváření AP zařízení pomocí ovladačů a nástrojů. Kali podporuje všechny režimy provozu (falešný hotspot, více hotspotů, režim monitoru) a prakticky každý hackerský nástroj na trhu. Jediným omezením této karty je, že nepodporuje 5 GHz. Technické vlastnosti zařízení jsou uvedené v tabulce 2.1.

Alfa AWUS-036ACH

Zařízení vhodné pro Wi-Fi 802.11n 2,4/5 GHz. Dvoupásmový bezdrátový širokopásmový adaptér USB AWUS036ACH 802.11ac poskytuje až neuvěřitelné vzdálenosti a vysoké rychlosti pro počítače Mac nebo Windows na Wi-Fi – až 300 Mbps pro 2,4 GHz a až 867 Mbps pro 5 GHz. AWUS036ACH se připojuje k počítači přes USB

Obr. 2.1: Alfa AWUS036NHA

Protokoly	IEEE 802.11b/g/n
Rychlost přenosu	802.11b: do 11 Mbps, 802.11g: do 54 Mbps, 802.11n do 150 Mbps
Rozhraní	USB 2.0 mini USB
Anténa konektor	1 x 2,4 GHz RP-SMA connector
Čipová sada	Atheros AR9271
Vestavěná anténa	5 dBi 2,4 GHz Antenna
Frekvence	2,412 - 2,483 GHz
Kanály	1-13
Výstupní výkon	802.11b - 29dBm, 802.11g - 27dBm, 802.11n - 27dBm
Citlivost	11b: 96dBm - 1Mbps, 11g: 91dBm - 6 Mbps, 11n: 91dBm
Modulace	BPSK, QPSK, CCk, OFDM
Napětí	5V+5%
Cena	od 35 Eur

Tab. 2.1: Technické vlastnosti Alfa AWUS-036NHA

3.0 s technologií Wi-Fi AC1200. Zdědil roky zkušeností v bezdrátovém průmyslu, ALFA AWUS036ACH je postaven na nejnovějších standardech 802.11ac a vysoce citlivých dvoupásmových anténách, které poskytují mimořádnou sílu a pokrytí signálu. Podporuje dvoupásmový AC1200. Technické vlastnosti zařízení jsou uvedené v tabulce 2.2.

Obr. 2.2: Alfa AWUS-036ACH

Protokoly	IEEE 802.11a/b/g/n/ac
Rozhraní	USB 3.0 Micro-B
Anténa konektor	RP-SMA connector
Čipová sada	Atheros AR9271
Vestavěná anténa	Dvě vysoce citlivé dvoupásmové dipólové antény
Frekvence	2,4GHz/5GHz
Cena	od 55 Eur

Tab. 2.2: Technické vlastnosti Alfa AWUS-036ACH

Netis WF2190

Netis WF2190 je určen k připojení stolního nebo přenosného počítače k bezdrátové síti a přístupu k vysokorychlostnímu připojení k internetu. Má čipovou sadu Realtek RTL8812AU která podporuje monitorovací mód. Je kompatibilní se zařízeními 802.11a/b/g/n/ac a poskytuje rychlost bezdrátového přenosu až 2,4 GHz 300 Mbps nebo 5 GHz 867 Mbps. Díky technologii 802.11n MIMO a 802.11ac zajišťuje silné a stabilní bezdrátové připojení. Technické vlastnosti zařízení jsou uvedené v tabulce 2.3.

Panda PAU09

PANDA PAU09 je dvoupásmový adaptér s dvěma kmitočty vlnových délek 2,4 GHz

Obr. 2.3: Netis WF2190

Protokoly	IEEE 802.11a/b/g/n/ac
Rozhraní	USB 3.0
Anténa konektor	RP-SMA connector
Čipová sada	Realtek RTL8812AU
Vestavěná anténa	5 dBi
Frekvence	2,4GHz/5GHz
Cena	od 26 Eur

Tab. 2.3: Technické vlastnosti Netis WF2190

a 5 GHz, jakož i příslušné duální antény 5 dB. Maximální rychlost bezdrátového připojení adaptéru se často zvětšuje na 300 Mbps pro obě frekvence. Co je zajímavější na PANDA PAUO9 je to, že pracuje efektivně s protokoly 802.11 ac/b/g/n. Je také kompatibilní s Linuxem včetně Kali a přechází do monitorovacího režimu, který je nezbytný pro testování bezdrátového průniku. Funguje s čipovou sadou Ralink RT5572.

Obr. 2.4: Panda PAU09

GI-Inet AR150

OpenWRT / LEDE router na Pineapple. Tyto malé směrovače založené na operačním systému OpenWRT jsou nejlepší volbou pro ty, kteří hledají velmi malou platformu s nízkým výkonem, na níž běží Linux. Zahrnutý hardware je založen na Qualcomm SOC s rozhraním Wi-Fi kompatibilním s monitorovacím režimem, které umožní vyhledávat přístupové body a stanice Wi-Fi. Procesor nemá působivý výkon, ale je vhodný pro malé projekty, jako jsou senzory, skenery, deauthenticators, MiTM atd. AR150 také používá velmi podobný hardware jako Hak5 Pineapple Nano, ale stojí mnohem méně. Hackeři proto do tohoto zařízení přenesli firmware Pineapple. Technické vlastnosti zařízení jsou uvedené v tabulce 2.4.

GI-Inet USB150 Minirouter

Tyto malé směrovače o velikosti USB flash disku jsou založeny na operačním systému OpenWRT. To je dobrá volba pro vývoj jakékoli aplikace založené na velmi malé linuxové platformě s nízkým výkonem. Zahrnutý hardware je založen na Qualcom SOC, který obsahuje rozhraní Wi-Fi kompatibilní s režimem sledování, které umožní vyhledávat přístupové body a stanice Wi-Fi. Technické vlastnosti zařízení jsou uvedené v tabulce 2.5.

Obr. 2.5: Gl-Inet AR150

CPU	Atheros QCA9331 SoC, 400MHz
Operační paměť	DDR2 64 MB
Paměť	16 MB Flash
Protokoly	IEEE 802.11b/g/n
Rozhraní	1 WLAN, 1 LAN, 1 USB2.0, 1 micro USB (power), UART
Externí úložiště	FAT32/EXFAT/EXT4/EXT3/EXT2/NTFS
Frekvence	2,4GHz - 150 Mbps
Cena	od 27 Eur

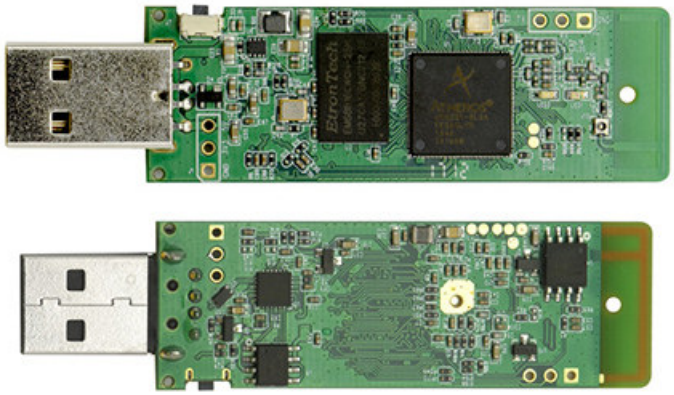
Tab. 2.4: Technické vlastnosti Gl-Inet AR150

CPU	Atheros QCA9331 SoC, 400MHz
Operační paměť	DDR2 64 MB
Paměť	16 MB Flash
Protokoly	IEEE 802.11b/g/n
Rozhraní	USB 2.0
Cena	od 25 Eur

Tab. 2.5: Technické vlastnosti Gl-Inet USB150 Minirouter

Gl-Inet Mifi

Tento malý 4G LTE router je dobrou volbou pro vytvoření hackerského zařízení



Obr. 2.6: Gl-Inet USB150 Minirouter

s připojením k internetu. Hardware je založen na Atheros SOC, který obsahuje rozhraní Wi-Fi, které umožní skenovat a zachytit nezpracované informace Wi-Fi v režimu monitorování. K dispozici jsou také porty GPIO, UART pro připojení GPS nebo jiného zařízení. Možnost připojení 4G je založena na interním portu PCIe, do kterého je vložena karta Quectel EC25 4G WWAN. Veškerý firmware, SDK a kód jsou open source a jsou k dispozici na github. K dispozici je také vestavěná baterie a nabíječka, takže je lze používat offline. K dispozici jsou sloty pro kartu SIM a pro kartu microSD. K dispozici je také volný konektor USB-A pro připojení volitelné karty Wi-Fi nebo jiných periferních zařízení. Technické vlastnosti zařízení jsou uvedené v tabulce 2.6.

CPU	Atheros AR9331 SoC, 400MHz
Operační paměť	DDR2 64 MB
Paměť	16 MB Flash
Protokoly	IEEE 802.11b/g/n
Rozhraní	WLAN, LAN, USB2.0, micro USB (power), SIM/MicroSD card
Rychlost přenosu	150 Mbps
Anténa konektor	SMA connector
Externí úložiště	FAT32/EXFAT/EXT4/EXT3/EXT2/NTFS
Frekvence	2,4GHz
Napětí	5V
Cena	od 110 Eur

Tab. 2.6: Technické vlastnosti Gl-Inet Mifi

Obr. 2.7: Gl-Inet Mifi

WiFi Pineapple Mark VII

Falešný hotspot (Rogue AP) lze snadno vyzvednout na jakémkoli notebooku. V hackerských kruzích je však již dlouho známo dobře promyšlené zařízení, které provádí útok v doslovném smyslu slova „out of the box“. WiFi Pineapple, který se objevil v roce 2008, je nyní v prodeji ve své sedmé modifikaci. První revize zařízení byla maskovaná jako ananas pro vtip - odtud název zařízení. V zásadě se jedná o běžný bezdrátový router (založený na bezdrátovém SoC Atheros AR9331 a procesoru 400 MHz), ale se speciálním firmwarem založeným na OpenWRT, který standardně obsahuje nástroje jako Karma, DNS Spoof, SSL Strip, URL Snarf. Ngrep a ostatní. Stačí tedy zapnout zařízení, nakonfigurovat internet (vše se konfiguruje přes webové rozhraní) - a zachytit uživatelská data. Směrovač potřebuje energii, což narušuje jeho mobilitu; Existuje však obrovské množství možností (které se aktivně diskutuje na oficiálním fóru) používat baterie - tzv. Battery Pack. Dávají zařízení dvě až tři hodiny výdrže baterie. Technické vlastnosti zařízení jsou uvedené v tabulce 2.7.

Obr. 2.8: WiFi Pineapple Mark VII

CPU	Atheros AR9331 SoC, 400MHz
Operační paměť	DDR2 256 MB
Paměť	2 GB EMMC
Protokoly	IEEE 802.11b/g/n/ac
Rozhraní	USB-C Power/Ethernet Port, USB 2.0 Host Port
Frekvence	2,4/5GHz
Cena	od 110 Eur

Tab. 2.7: Technické vlastnosti WiFi Pineapple Mark VII

3 Zachytávání provozu sítě 802.11

Tato kapitola je soustředěna na praktické řešení problémů. Obsahuje popis použitých nástrojů, samotný proces zachytávání provozu a analýzu zachycených rámců.

3.1 Praktické řešení

3.1.1 Testovací prostředí, prostředky, nástroje

Testování probíhalo způsobem simulování reálného případu užití. Pro implementaci testovacího prostředí je potřeba více zařízení, každé zařízení má svoji určitou funkci v testovacím plánu.

Pro legitimní přístupový bod byla použita USB síťová karta TP-Link Archer T2U Plus. Jako testovací klient v síti byl notebook Lenovo, ke kterému byl připojen USB Wi-Fi router Netis WF2190, jenž byl připojen k testovací bezdrátové sítí. V síti jsou také další uživatelé – notebook HP a mobilní telefon. Dalším zařízením je samotný sniffer zachytávající provoz. Snifferem bylo stejné USB Wi-Fi zařízení jako klient, tedy Netis WF2190. Sniffer musí být připojen k počítači s operačním systémem Linux. Celkový seznam použitého hardware je uveden v tabulce 3.1.

Role v testu	**Zařízení**
Sniffer	Netis WF2190
Stanice prvního uživatele	Notebook Lenovo (Windows OS)
Síťové rozhraní prvního uživatele	Netis WF2190
Stanice druhého uživatele	Notebook HP (Windows OS)
Síťové rozhraní druhého uživatele	Vestavěné v notebook síťové rozhraní
Stanice třetího uživatele	Android mobil
Stanice ke kterému připojen sniffer	Desktop PC (VirtualBox Kali Linux OS)
Přístupový bod	TP-Link Archer T2U Plus

Tab. 3.1: Seznam zařízení použitého při testování

Nejjednodušší způsob, jak zachytávat Wi-Fi pakety, je použít linuxovou distribuci zvanou Kali. Existují desítky jiných distribucí Ubuntu, ty ale neobsahují potřebný software. Kali Linux se objevil v důsledku sloučení WHAX a Auditor Security Collection. Projekt vytvořili Mati Aharoni a Max Moser. Určen je především pro provádění bezpečnostních analýz.

V rámci operačního systému Kali byl použit nainstalovaný nástroj Aircrack-ng. Tento nástroj je kompletním řešením pro bezpečnostní analýzu Wi-Fi sítí a obsahuje

v sobě celou řadu funkcí. V této práci jsou využity také monitorovací balíčky od Aircrack-ng jako: airmon-ng pro naslouchání veškerého provozu a airodump-ng pro zachycení provozu určité bezdrátové sítě a uložení zachycených údajů do souboru pro následnou analýzu. Pro analýzu zachyceného provozu byl napsán program Traffic Analyzer v programovacím jazyce Python. Podrobný popis programu je v následující podkapitole.

Dalším použitým programem pro analýzu zachyceného povozu byl Wireshark. Wireshark je analyzátor provozu pro počítačové sítě Ethernet a některé další. Má grafické uživatelské rozhraní. Projekt se původně jmenoval Ethereal, ale kvůli problémům s ochrannými známkami v červnu 2006 byl přejmenován na Wireshark. Funkce, které Wireshark poskytuje, jsou velmi podobné funkcím tcpdump, ale Wireshark má grafické uživatelské rozhraní a mnohem více možností řazení a filtrování. Program umožňuje uživateli zobrazit veškerý provoz procházející sítí v reálném čase, čímž uvede síťovou kartu do monitorovacího režimu.

Pro provedení testování a analýzu byly použity taky nové Python skripty. Jeden skript pro generování určitých datových rámců, druhý skript pro porovnání zachyceného a regulárního provozu. Celkový seznam použitého software je uveden v tabulce 3.2.

Software	**Role v testu**
Airmon-ng	Naslouchání provozu/detekce přístupových bodů
Airodump-ng	Zachycení provozu
Vlastní Traffic Analyzer	Zachycení provozu/analýza
Vlastní generátor provozu	Generování určitého počtu datových rámců
Vlastní analyzátor zachyceného provozu	Srovnání zachyceného a referenčního povozu
Wireshark	Analýza/záchyt referenčního provozu

Tab. 3.2: Seznam použitého software při testování

3.1.2 Traffic Analyzer

Tato kapitola se věnuje popisu programu Traffic Analyzer.

Popis programu

Program je určen pro zachytávání a následnou analýzu naměřených dat Wi-Fi provozu. Traffic analyzer obsahuje celou řadu možností. Uživatel si tak může zvolit, co chce zachytávat pomocí výběru. Kromě toho uživatel má k dispozici sekce detailu o přístupovém bodu. V této sekci najde informace o počtu a typu přenesených rámců

během provozu, MAC adresu přístupového bodu, frekvenci, na které přístupový bod vysílá, velkost přenesených dat a taky sílu vysílání přístupového bodu, díky čemu lze odhadnout vzdálenost přístupového bodu. Kromě toho si lze prohlédnout seznam MAC adres připojených uživatelů do určitého přístupového bodu.

Program uživateli také nabízí několik typů grafů, které se průběžně aktualizují během zachycení provozu, každých 50 ms. Uživatel si tak může zvolit, který typ grafu se má zobrazovat a pro která data. Jedna možnost je výpočet a znázornění statistiky pro všechna data, druhá možnost jen pro data určitého přístupového bodu. Další možnost programu je výpis informace do sekcí konzoly. V této konzoli se zobrazuje výpis informací o zachyceném rámci. Pomocí pomocných tlačítek uživatel může zvolit, jaký výpis chce. Pokud zvolí režim RAW tak se do konzoly bude vypisovat veškerá informace, která se dá zjistit z rámce. Pokud režim výpisu bude Summary, tak se vypíše jen základní informace o rámci, tedy typ rámce, podtyp, zdrojová a cílová MAC adresy apod. Obsah vypsané informace záleží na typu rámce. Různé způsoby zobrazení zachyceného provozu jsou uvedené ve výpisech 3.1 a 3.2.

Výpis 3.1: Příklad výpisu RAW rámce do konzoly.

```
###[ 802.11 ]###
    subtype   = 8
    type      = Data
    proto     = 0
    FCfield   = from-DS+retry
    ID        = 12288
    addr1     = 14:9f:e8:0e:99:cd
    addr2     = 18:f0:e4:d0:f6:71
    addr3     = 18:f0:e4:d0:f6:71
    SC        = 27872
```

Výpis 3.2: Příklad výpisu Summary rámce do konzoly.

```
802.11 Control 8 8c:85:90:6f:a2:ac > da:ff:28:3f:cd:83 / Raw
802.11 Control 8 8c:85:90:6f:a2:ac > da:ff:28:3f:cd:83 / Raw
802.11 Control 8 8c:85:90:6f:a2:ac > da:ff:28:3f:cd:83 / Raw
802.11 Control 8 8c:85:90:6f:a2:ac > da:ff:28:3f:cd:83 / Raw
802.11 Control 8 8c:85:90:6f:a2:ac > da:ff:28:3f:cd:83 / Raw
```

V neposlední řadě je důležité logování provozu. Program nabízí uživateli 2 typy logování. První je zápis výpisu konzoly do log souboru, výhodou takového logu je to, že data se do něj ukládají v čitelné podobě, tedy není potřeba používat další nějaký nástroj na čtení dat zachyceného provozu, např. pcap souboru, je to užitečné, když je potřeba rychle najít nějakou informaci. Druhý typ je ukládání zachyceného provozu do pcap souboru. Výhodou tohoto typu logů je možnost dalšího zpracování

v externím programu, například Wireshark. Program umí detekovat všechny typy rámců a vypočítat statistiku. Podporované typy rámců:

Data Frame – hlavním úkolem WiFi sítě je přirozeně přenos dat. Datové rámce nesou pakety vyšších vrstev, jako jsou webové stránky a podobně, uvnitř těla samotného rámce. Standard WiFi IEEE 802.11 definuje 15 typů datových rámců. Mezi nejčastěji používané patří: Datový rámec (jednoduchý datový rámec), Data + CF-ACK a Data QoS.

Managment Frame – rámce správy 802.11 tvoří většinu typů rámců v síti WLAN. Bezdrátové stanice používají řídící rámce k připojení a opuštění základní sady služeb (BSS). Další název pro rámec správy 802.11 je Správa MAC Protocol Data Unit (MMPDU).

Control Frame – řídicí rámce 802.11 pomáhají s dodáním datových rámců. Řídicí rámce jsou přenášeny jednou ze základních rychlostí. Kontrolní rámce se také používají k: zrušení kanálů, získání kanálů, poskytují potvrzení o jednom snímku. Obsahují pouze informace záhlaví.

Podporované podtypy: Association request, Reassociation request, Association/Reassociation response, Probe request, Probe response, Beacon, Authentication frames, Deauthentication/Disassociate frames, Action frames, Clear to Send, ACK, QoS Data,Announcement traffic indication map (ATIM) a jiné. Kromě typu rámce nástroj může specifikovat protokol. Program rozlišuje tři protokoly: TCP, UDP, ICMP. Pokud rámec obsahuje jiný protokol, bude přidán do skupiny „Other“, pokud se nedá zjistit jeho protokol, rámec se zapíše do skupiny „Unknown“.

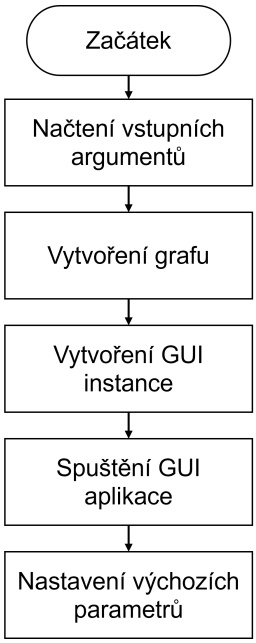
Vývoj

Nástroj je napsán v programovacím jazyce Python 3 a je postaven nad knihovnou Scapy. Scapy je výkonný interaktivní program pro manipulaci s pakety. Je schopen falšovat nebo dekódovat pakety širokého počtu protokolů, posílat je na linku, zachytávat je, odpovídat požadavkům a mnohem více. Scapy snadno zvládne většinu klasických úkolů, jako je skenování, sledování, testování, útoky nebo objevování sítě. Může nahradit hping, arpspoof, arp-sk, arping, p0f a dokonce i některé části Nmap, tcpdump a tshark.

GUI programu je postaveno na knihovně PyQt5. Qt je sada multiplatformních knihoven C++, které implementují API na vysoké úrovni pro přístup k mnoha aspektům moderních stolních a mobilních systémů. Patří sem služby určování polohy, multimédia, připojení NFC a Bluetooth, webový prohlížeč Chromium a také tradiční vývoj uživatelského rozhraní. PyQt5 je komplexní sada vazeb Pythonu pro Qt verze 5. Je implementován jako více než 35 rozšiřovacích modulů a umožňuje použití Pythonu jako alternativního jazyka pro vývoj aplikací k C++ na všech podporovaných platformách včetně iOS a Android. PyQt5 může být také zabudován do

aplikací založených na C++, aby umožnil uživatelům těchto aplikací konfigurovat nebo vylepšit funkčnost těchto aplikací.

Pro výkres grafu se používá matplotlib knihovna a NumPy. Matplotlib je knihovna pro vykreslování programovacího jazyka Python a jeho numerické matematické rozšíření NumPy. Poskytuje objektově orientované API pro vkládání grafů do aplikací pomocí obecných nástrojů GUI jako Tkinter, wxPython, Qt nebo GTK +. Tam je také procedurální "pylab" rozhraní založené na stavovém stroji (jako OpenGL), navržené k blízké podobnosti s MATLAB, ačkoli jeho použití je odrazováno. Matplotlib byl původně napsán Johnem D. Hunterem, od té doby má aktivní vývojovou komunitu a je distribuován pod licencí ve stylu BSD.



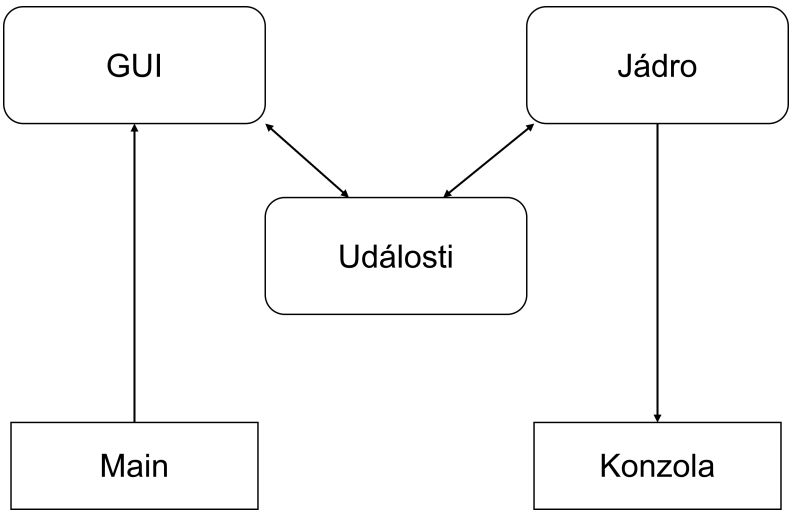
Obr. 3.1: Vývojový diagram procesů naběhnutí programu.

Proces spuštění programu

Po té, co uživatel spustí program, začne proces naběhnutí programu. Vývojový diagram tohoto procesu je znázorněn na obrázku 3.1.

Nejprve proběhne načtení vstupního parametru. Program očekává jeden parametr – název bezdrátové síťové karty. Pokud takový parametr není specifikován, program se ukončí s chybovým hlášením. Dále se spustí proces vytvoření instance grafu. Pro každý typ grafu je určena konkrétní instance třídy `Figure`, z balíčku `matplotlib`. Po vytvoření instance se do objektu grafu vkládají taková výchozí nastavení a hodnoty jako: velikost plochy grafu, typ grafu, název grafu, jeho hodnoty a další. Pak se každá instance grafu ukládá do paměti.

Dalším krokem je vytvoření GUI instance. Když je objekt vytvořen, vkládají se do něho grafy, vytvořené v předchozím kroku. Pak následuje proces spuštění GUI aplikace, tento proces řídí knihovna `PyQt5`. Až doběhne proces vytvoření GUI, spustí se iniciální funkce v jádru programu. Tato funkce nastaví výchozí hodnoty do proměnných (jsou to názvy logovácích souborů, důležité proměnné apod.)



Obr. 3.2: Struktura programu.

Hierarchie programu

Pro jednodušší vývoj, následnou podporu a rozšíření programu, byla vnitřní struktura rozdělena do několika částí. Struktura je znázorněna na obrázku 3.2 a obsahuje tyto prvky:

Hlavní funkce – je to funkce která spouští celý program. Jejím hlavním úkolem je spuštění procesu naběhnutí programu, tento proces je popsán v předchozí kapitole.

GUI – jak napovídá název, obsahuje v sobě funkce pro práci s grafickým uživatelským rozhraním. Načítá soubor `windows.ui`, ve kterém se nachází definice všech prvků GUI. Pokud uživatel stiskne nějaké tlačítko, bude vyvolána určitá událost, spojená s tímto tlačítkem.

Události – jsou to propojení mezi grafickým rozhraním a jádrem programu. Jsou zodpovědné za volání určitých funkcí podle hodnoty příchozí událostí.

Jádro programu – je důležitá část programu, která se nachází ve zvláštním Python souborů. Obsahuje samotnou implementace odposlechů provozu. Vykonává určité funkce dle událostí (aktualizace grafu, parsování zachyceného rámce a jeho analýza a další).

Konzola – simulování příkazového řádku, přijímá text od jádra programu a následně jej zobrazuje.

Program se skládá z několika Python souborů. Funguje to tak, že první musí být spouštěn GUI skript `MainGui.py`. Tento skript připraví grafické rozhraní a data pro grafy, následně načte do paměti skript `TrafficAnalyzerCore.py` který je zodpovědný za jádro programu. Jádro programu má také pomocný Python soubor `AccessPointInfo` - který je v podstatě skříň, obsahující informace o přístupovém bodu.

Funkční bloky

Hlavním funkčním blokem celého nástroje je funkce `real time capturing`. Tato funkce řídí celý proces zachytávání rámců a běží ve zvláštním vlákně. Hned na začátku funkce se snaží detekovat bezdrátové zařízení, které bylo předáno uživatelem jako vstupní parametr. Pokud takové zařízení nenajde nebo nebude možné spustit zachytávání, program skončí. V případě úspěchu, začne samotný proces zachytávání.

Funkce spustí asynchronně zachytávání provozu pomocí knihovny Scapy. Při asynchronním zachytávání program zachytí rámce do bloku a každých 40 milisekund je aktuální blok uzavřen. Po uzavření se tento blok předává do funkce zpracování bloku `process packet list` a hned se spustí další záchyt dat do nového bloku.

Funkce zpracování bloku dat se spouští ve zvláštním vlákně a dělá to, že načítá z bloku dat jednotlivé rámce a předává rámce do další funkce pro zpracování. Funkce zpracování `process packet` dostane do proměnné objekt typu `packet` a dále s tímto objektem pracuje. Nejprve zjistí, od kterého přístupového bodu přišel rámec. Pokud takový přístupový bod ještě není v seznamu nalezených, bude do seznamu přidán a zároveň bude vytvořena instance pomocné třídy `AccessPointInfo`. `AccessPointInfo` je třída vytvořená za účelem uchování informace o provozu určitého přístupového bodu do paměti. Pokud se detekovaný přístupový bod již nachází v seznamu nalezených, bude načten jeho `AccessPointInfo` a následně tento rámec bude analyzován. Informace, kterou se dá zjistit z rámce, bude zapsána do objektu `AccessPointInfo` příslušného přístupového bodu. Na konci se zavolá aktualizace dat.

Dalším, jedním z důležitých funkčních bloků je `update plot data`. Tato funkce se volá každých 50 ms ve zvláštním vlákně a je odpovědná za aktualizace grafu. Podle aktuálně zvoleného grafu, načítá odpovídající údaje ze seznamu statistických dat. Tento seznam obsahuje objekty typu `AccessPointInfo`, každý objekt obsahuje v sobě další data a seznamy. Funkce přečte potřebná data a vloží je do listu, ze kterého se pak skládá graf. Až projde všechna naměřená data, zavolá funkci překreslování grafu.

Použití

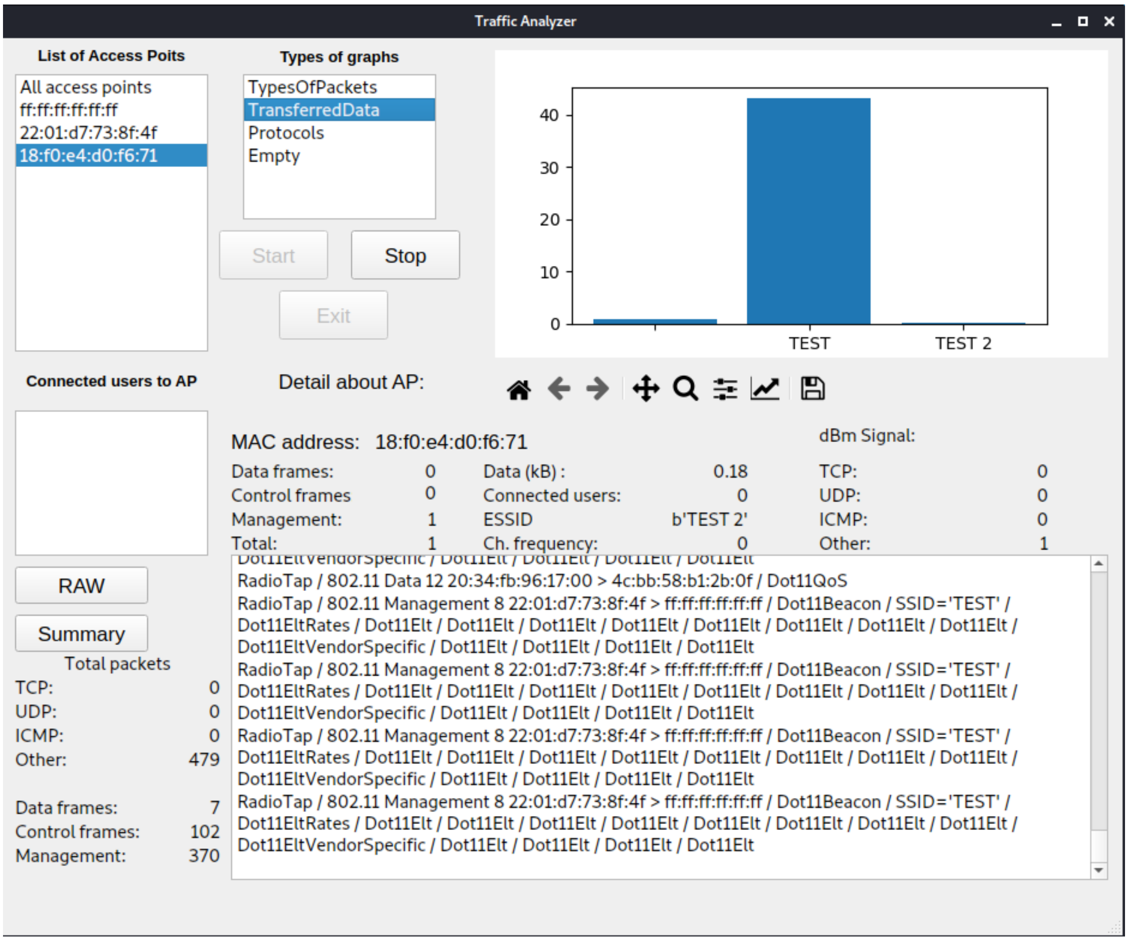
Pro použití programu musí uživatel nainstalovat Python 3 na svůj počítač. Vzhledem

k tomu, že Python balíčky lze nainstalovat na Linux operační systémy, nástroj může být spouštěn i na OpenWrt routeru přes SSH připojení. Dále je potřeba zapnout monitorovací režim na WiFi kartě – pomocí příkazu:

```
airmon-ng start wlan0
```

Airmon-ng převede kartu do „monitorovacího“ režimu, tím se vytvoří nové virtuální rozhraní. V obyčejném režimu přístupový bod funguje tak, že přijímá jen ty pakety, které jsou určené pro něj. V „monitorovacím“ režimu však router přijímá veškerý provoz kolem sebe, což umožňuje načítání rámců do lokální paměti a jejich následnou analýzu. Dále je možné spustit nástroj pomocí příkazu:

```
MainGui.py wlan0mon
```



Obr. 3.3: Příklad prostředí programu Traffic Analyzer

Nástroj vyžaduje jako vstupní parametr název síťového rozhraní zařízení v monitorovacím režimu. Po naběhnutí se zobrazí hlavní okno programu. Podrobnější popis jednotlivých částí je uveden níže.

List of Access Points – sekce nalezených přístupových bodů. Zobrazuje se tady MAC adresa, pokud uživatel zvolí nějaký přístupový bod, zobrazí se mu informace o přístupovém bodě v sekci detailu. Kromě toho se bude zobrazovat statistika, včetně grafů, jen pro provoz zvoleného AP. Pokud uživatel zvolí položku *All access points*, bude se vyhodnocovat statistika pro všechny nalezené přístupové body.

Types of graphs – seznam typů grafů. Grafy se aktualizují každých 50 ms. Program umí vykreslovat další typy grafů:

– TypesOfPackets - znázorňuje počet různých typů rámců v síti.

– TransferedData - zobrazuje velikost přenesených dat v každé síti.

– Protocols - zobrazuje počet rámců s určitým protokolem.

Connected users to AP – sekce, kde se zobrazují MAC adresy uživatelů určitého přístupového bodu.

Detail – sekce pro zobrazení podrobnější informace o přístupovém bodu. Jsou tady jak počty rámců rozdělených do typů a podtypů, tak i název sítí, frekvence, vysílací síla signálu, velikost přenesených dat.

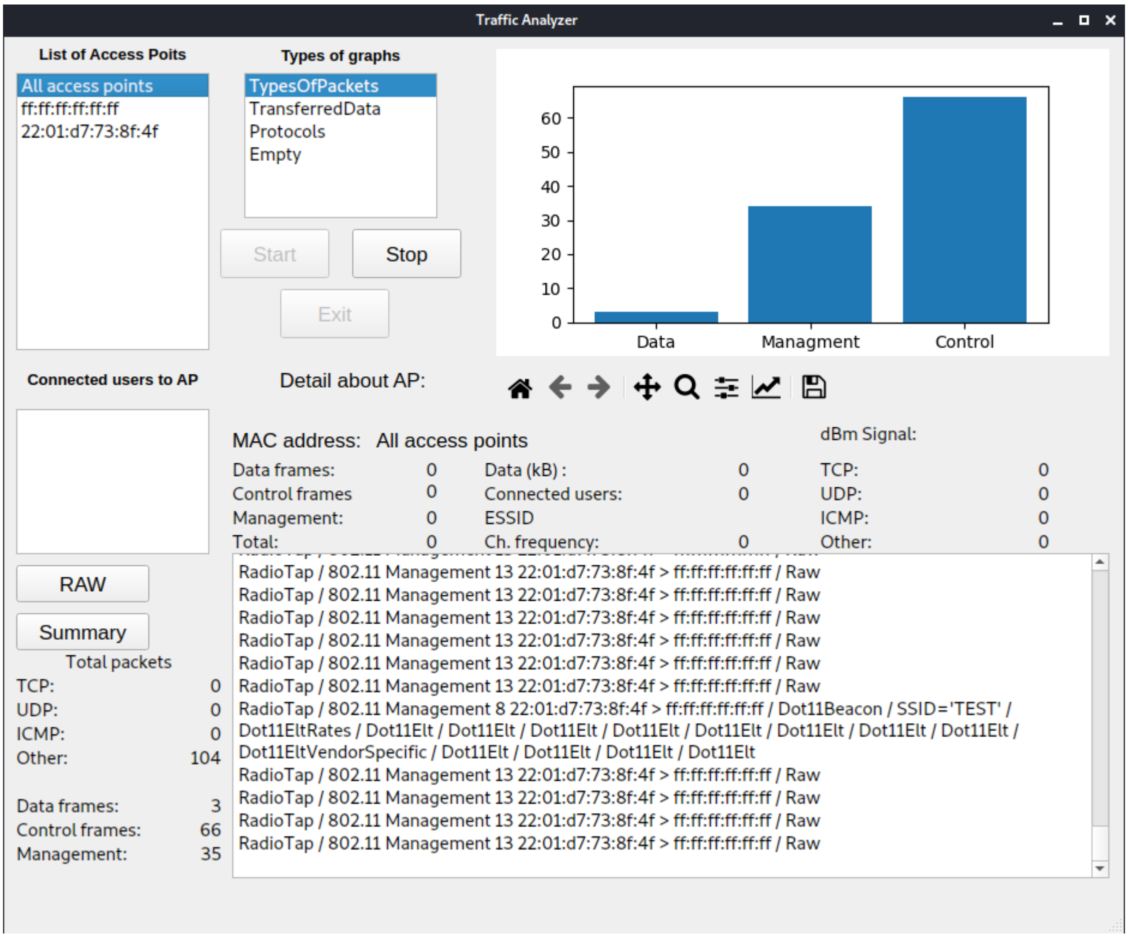
Konzola – část programu, kde se zobrazuje výpis informací o zachyceném rámci. Pomocí pomocných tlačítek si uživatel může zvolit, jaký výpis chce. Pokud zvolí režim *RAW*, tak se do konzoly budou vypisovat veškeré informace, které se dají zjistit z rámce. Pokud režim výpisu bude *Summary*, tak se vypíše jen základní informace o rámci, tedy typ rámce, podtyp, zdrojová a cílová MAC adresy apod. Obsah vypsané informace záleží na typu rámce.

Logování – program nabízí uživateli 2 typy logování. První je zapsání výpisu konzoly do log souboru, výhodou takového logu je to, že data se do něj ukládají v čitelné podobě, není tedy potřeba používat další nástroj na čtení dat zachyceného provozu, např. pcap souboru. Je to užitečné, když je potřeba rychle najít nějakou informaci. Druhý typ je ukládání zachyceného provozu do pcap souboru. Výhodou tohoto typu logů je možnost dalšího zpracování.

Požadavky

Operační systém – program by měl fungovat na všech operačních systémech: Windows, Linux, MacOS.

Síťová karta – hlavní požadavek na síťovou kartu je možnost fungování v monitorovacím režimu, aby se dalo vůbec spustit program a zachytit data. Kvalita a počet zachycených rámců záleží na výkonnosti síťové karty. Pokud zařízení podporuje změnu nebo konfiguraci nastavení, například pracovní frekvence, je potřeba tyto nastavení měnit před spuštěním programu. Samotný proces záchytu rámců není závislý na typu modulace, je tedy možné zachytávat provoz různých Wi-Fi standardů `(a\b\g\n\ac\ad)`, které používají různé modulace (OFDM , MIMO, DSSS).



Obr. 3.4: Příklad fungování programu Traffic Analyzer

Operační paměť – vzhledem k tomu, že program zpracovává obrovské množství dat v režimu reálného času, je program náročný na operační paměť, hlavně kvůli vykreslování grafů. Implementace programu byla vylepšena přidáním vícevláknového zpracování dat, ale stejně program potřebuje alespoň 3 GB operační paměti.

Závislosti na SW – pro spuštění programu musí na zařízení být nainstalován Python verze 3.4 nebo vyšší. Další požadavky jsou nainstalované python knihovny Scapy a Matplotlib. Pro instalaci je potřeba spustit další příkazy v python konzoli:

```
pip install -pre scapy[basic]

pip install matplotlib
```

Výhody Trafic Analyzer

Vzhledem k tomu, že program je napsán v programovacím jazyce Python 3, lze jej spustit skoro na jakémkoliv zařízení, které podporuje GUI. Díky využití vícevláknového programování je program dost rychlý a navíc není moc náročný na HW

zařízení. Oproti ostatním softwarům se dá program jednoduše modifikovat, vylepšovat a přidávat další části pro analýzu dat, např. další typy grafů apod.

3.1.3 Generátor provozu

Pro provedení přesnějšího testování bylo potřeba navrhnout nějaký způsob, pomocí kterého, testovací zařízení uživatele odešle přesný počet rámců a ani jeden navíc. K řešení tohoto problému byl napsán Python skript, používající knihovnu Scapy. Obsah celého skriptu je uveden v příloze A.1.

Skript je v podstatě jednoduchý sestavovač rámců 802.11. Pro generování datového rámce typu `QoS Data` je potřeba zaprvé vygenerovat objekt typu `Dot11`. Pro vygenerování se dá použít konstruktor, který očekává 5 parametrů na vstupu.

Výpis 3.3: Generování rámce Dot11.

```
dot11=Dot11(type=2,
            subtype=8,
            addr1='ff:ff:ff:ff:ff:ff',
            addr2=sender,
            addr3=sender)
```

První parametr je `type`. Tento parametr vlastně určuje typ rámce. Protokol 802.11 určuje 3 typy rámce: *Control, Management, Data*. Datový rámec je typu 2. Druhý parametr je `subtype`. Jedná se o podtyp určitého typu rámce. Existuje hodně různých podtypů rámce, v tomto případě je zajímavý podtyp `QoS Data`, což je 8. Třetí parametr `addr1` je cílová cílová MAC adresa. Při provedení testování má hodnotu všesměrové adresy, tedy `ff:ff:ff:ff:ff:ff`. Čtvrtý a pátý prametery jsou `addr2` a `addr3`. Obsahují hodnotu MAC adresy zařízení, které rámec odesílá. V případě testovacího scénáře, má MAC adresu USB Wi-Fi zařízení Netis WF2190.

Dalším důležitým krokem při generování rámce je samotné generování datového *frame*.

Výpis 3.4: Sestavení frame QoS Data.

```
frame = RadioTap()/dot11/Dot11QoS()/"Some␣test␣payload␣ABCD"
```

Knihovna Scapy umožňuje jednoduše sestavit jakýkoliv rámec. Při prvním pokusu záchytu rámců se sestavovali rámce typu *Management*, ale prakticky se prokázalo, že záchyt takového typu rámce je problematický. Při záchytu *Management* rámců byla pozorována velká ztrátovost dat oproti záchytu datového rámce. Datový rámec se skládá z několika částí, díky knihovně Scapy se tyto části dají jednoduše sestavit pomocí lomítka.

`RadioTap` je formát záhlaví a mechanismus, který poskytuje další informace o rámcích. `Dot11` je důležitá část rámce, která obsahuje další informace o rámci,

jako typ a podtyp rámce. `Dot11QoS` je samotná část rámce `QoS Data`, v aktuálním příkladu se vygeneruje základní část rámce pomocí Scapy, protože nemusíme specifikovat nějaké parametry kromě testovacího payloadu, který určíme za dalším lomítkem. Poté, co je rámec vygenerován, se dá předat do vysílající funkce `sendp`, která ho odešle prostřednictvím síťového rozhraní.

Výpis 3.5: Odeslání datového rámce

```
sendp(frame, iface=iface, inter=0.2, loop=1, count=100)
```

Scapy definuje dvě funkce pro odeslání rámců. Funkce `send` odešle pakety na třetí vrstvě. To znamená, že knihovna sama zpracuje směřování a vrstvu 2. Funkce `sendp` bude fungovat ve vrstvě 2. Díky tomu můžeme specifikovat rozhraní a správný protokol vrstvy spojení. Funkce `send` a `sendp` také vrátí seznam odeslaných paketů, pokud je jako parametr předán příznak `returnPackets = True`. Při provedení testování byla použita funkce `sendp`. Tato funkce vyžaduje několik parametrů.

Jako první parametr funkce očekává samotný rámec, který bude odeslán. Dalším parametrem je `iface`, zde je potřeba uvést název rozhraní, na kterém se bude odesílat rámec. Třetí parametr je `inter`, určuje časové zpoždění mezi odesíláním rámců. Bylo prozkoumáno různé zpoždění a nejlepší variantou bude odesílat rámce každých 20 milisekund. Další parametr je `loop`, ten určuje, zda je potřeba odesílat rámce periodicky nebo po jednom. A poslední parametr je `count`, který jak napovídá název, určuje počet rámců, které budou odeslané, jedná se tedy o kopii rámce *frame*. Funkce `sendp` má řadu dalších parametrů ale v aktuálním testovacím scénáři jiné parametry nemají žádný vliv.

Vygenerovaný datový rámec byl během testu zachycen pomocí sondy a jeho struktura zobrazená ve Wireshark na obrázku 3.5.

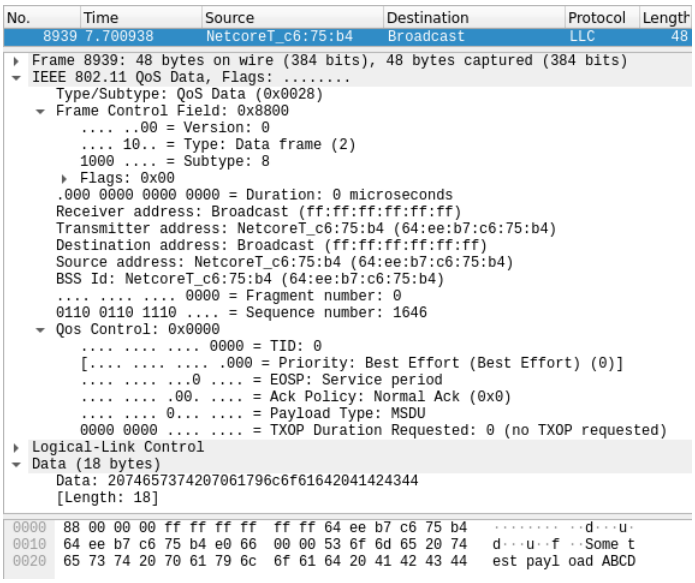
3.1.4 Skript pro porovnání zachyceného a regulárního provozu

Pro analýzu zachycených dat a prokázání úspěšného zachytávání dat, bylo potřeba vymýšlet, jakým způsobem data porovnávat. Tento problém se podařilo vyřešit implementováním jednoduchého Python skriptu, který automatizuje proces porovnání vzorku dat a navíc přináší určitou přesnost výpočtu výsledků. Zdrojový kód celého skriptu je uveden v příloze A.2.

Skript je postaven na knihovně Scapy a taky s použitím balíku *argparse* pro práce s argumenty příkazového řádku.

Výpis 3.6: Definice vstupních parametrů

```
parse.add_argument ("ref", help = "Cesta␣do␣referenčních␣dat")
parse.add_argument ("cap", help = "Cesta␣do␣zachycených␣dat")
```



Obr. 3.5: Vygenerovaný QoS datový rámec ve Wireshark.

Skript očekává 2 povinné vstupní parametry, bez kterých nebude fungovat. První parametr je cesta do souboru zachyceného provozu referenčních dat. Program by měl umět zpracovávat různé formáty vstupního souboru zachycených dat, doporučuje se však použít formát *.cap*. Druhým povinným parametrem je cesta do souboru zachycených dat sondou taky ve formátu *.cap*. Důležité je pořadí parametrů, protože soubor zachycených referenčních dat má jinou strukturu, než data v souboru, které zachytila sonda. Při nedodržování pořadí vstupních souboru program spadne na chybu.

Výpis 3.7: Čtení souborů *cap*

```
referenceData = rdpcap(str(args.ref))
capturedData = rdpcap(str(args.cap))
```

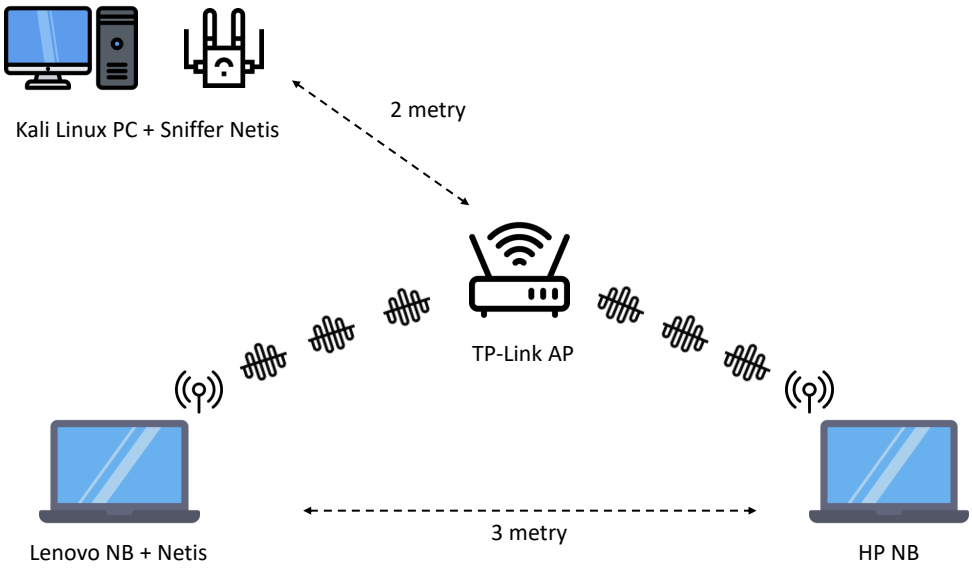
Dalším důležitým krokem skriptu je samotné čtení souboru zachycených dat. Čtení souboru zajistí knihovna Scapy, hlavně funkce `rdpcap`. Tato funkce parsuje soubor dat na seznam objektů `Packet`, díky tomu se dá uvnitř skriptů zpracovávat jednotlivé rámce po jednom. Po úspěšném načtení dat, následuje výpočet velikosti přenášených dat. To se dělá tak, že se pomocí cyklu skriptů prochází seznam zachycených rámců po jednom a přidává velikost dat do celkového počtu přenášených dat v bajtech. Na konci skript vypočítá celkovou velikost ztracených dat porovnáním zachycených a regulárních dat. Na základě celkové velikosti ztracených dat, určí ztrátovost v procentech a vypíše výsledek do konzoly.

3.1.5 Záchyt provozu v závislosti na protokolu

Tato kapitola se věnuje prvnímu testovacímu scénáři. Cílem scénáře je provést záchyt provozu bezdrátové sítě a porovnat výsledky v závislosti na nejčastěji používané protokoly rodiny IEEE 802.11 v testovací síti.

Popis testovacího plánu a prostředí

Pro provedení testování byla použita zařízení uvedená dříve v tabulce 3.1. Testování probíhalo v jedné místnosti a zařízení byla zapojena podle obrázku 3.6.



Obr. 3.6: První testovací scénář.

V daném testovacím scénáři byl sniffer připojen do Linux PC, na kterém byl nainstalován potřebný software. Další zařízení jsou dva notebooky, které jsou připojené do testovací Wi-Fi sítě. Vzdálenost mezi uživateli, kteří spolu vzájemně komunikují, je přibližně 3 metry. Vzdálenost mezi snifferem a přístupovým bodem je přibližně 2 metry. Testovací plán spočívá v následujících krocích:

1. Nastavit protokol IEEE 802.11 na přístupovém bodu TP-Link.
2. Připojit uživatele do testovací sítě.
3. Nastavit a spustit sniffer.
4. Spustit sledování odesílaných dat na stanici, která bude vysílat data.
5. Zahájit přenos dat mezi uživateli.
6. Uložit soubory zachycených a regulérních dat po dokončení přenosu.

První bod testovacího plánu byl realizován systémovým nastavením zařízení TP-Link, kde se dají měnit různé parametry a jedním z nich je nastavení protokolu 802.11. Dalším krokem je připojení uživatele. Tady je potřeba zmínit, že kvůli vlastnostem notebooku Lenovo, jeho síťové rozhraní nepodporuje všechny potřebné verze protokolu 802.11 pro úspěšné provedení testu. Kvůli tomu bylo použito další zařízení Netis, které bylo připojeno k notebooku a zároveň na počítači byla vypnuta integrovaná síťová karta, aby celý provoz dat určitě probíhal přes externí Netis. Druhý notebook HP je modernější a podporuje všechny potřebné verze protokolu 802.11. Třetím krokem je příprava a spouštění snifferu. V tomto testovacím scénáři byl sniffer spouštěn pomocí následujících příkazů:

1. Vypnutí rozhraní:

```
ip link set wlan0 down
```

2. Kontrola a vypnutí procesů na pozadí, které mohou mít špatný vliv na záchyt dat:

```
airmon-ng check kill
```

3. Po volání `airmon-ng` je potřeba provést vypnutí rozhraní ještě jednou, nyní pomocí jiné metody:

```
ifconfig wlan0 down
```

4. Nastavení monitorovacího režimu síťového rozhraní, které zajistí odposlech provozu:

```
iw wlan0 set type monitor
```

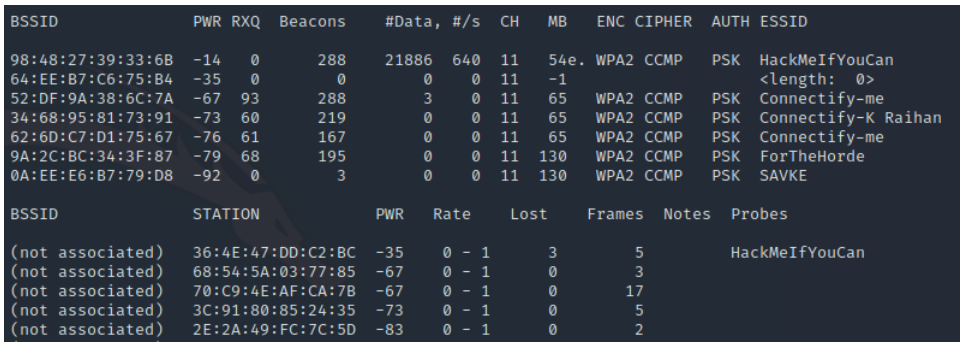
5. Zapnutí síťového rozhraní:

```
ifconfig wlan0 up
```

Je potřeba uvést, že v uvedeném postupu zapnutí síťového rozhraní, parametr názvu rozhraní je `wlan0`, jeho název se ale může lišit, například na jiném operačním systému.

Po povedení těchto pěti kroků je zajištěno, že síťové rozhraní je připraveno pro záchyt provozu. Teď je možné spustit samotný záchyt provozu, ale ještě předtím je potřeba ověřit detekce přístupového bodu, jehož provoz se bude odchytávat. Pro detekci přístupového bodu se dá použít následující příkaz:

```
airodump-ng wlan0
```



```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

98:48:27:39:33:6B  -14   0      288    21886  640  11   54e. WPA2 CCMP   PSK  HackMeIfYouCan
64:EE:B7:C6:75:B4  -35   0        0        0    0  11   -1                    <length:  0>
52:DF:9A:38:6C:7A  -67  93      288        3    0  11   65   WPA2 CCMP   PSK  Connectify-me
34:68:95:81:73:91  -73  60      219        0    0  11   65   WPA2 CCMP   PSK  Connectify-K Raihan
62:6D:C7:D1:75:67  -76  61      167        0    0  11   65   WPA2 CCMP   PSK  Connectify-me
9A:2C:BC:34:3F:87  -79  68      195        0    0  11  130   WPA2 CCMP   PSK  ForTheHorde
0A:EE:E6:B7:79:D8  -92   0        3        0    0  11  130   WPA2 CCMP   PSK  SAVKE

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   36:4E:47:DD:C2:BC  -35    0 - 1      3         5         HackMeIfYouCan
(not associated)   68:54:5A:03:77:85  -67    0 - 1      0         3
(not associated)   70:C9:4E:AF:CA:7B  -67    0 - 1      0        17
(not associated)   3C:91:80:85:24:35  -73    0 - 1      0         5
(not associated)   2E:2A:49:FC:7C:5D  -83    0 - 1      0         2
```

Obr. 3.7: Příklad výpisu programu airodump-ng.

Po spuštění příkazu se v konzoli zobrazí seznam přístupových bodů, jedním z nich je `HackMeIfYouCan`, který je testovací přístupový bod. Příklad výpisu je znázorněn na obrázku 3.7.

Na základě výpisu programu `airodump-ng` můžeme jednoduše zjistit MAC adresu testovacího přístupového bodu. Poté, co je ověřena funkčnost monitorovacího režimu a detekce přístupového bodu, je možné spustit samotné zachytávání provozu testovací bezdrátové síti. To se dá udělat následujícím příkazem:

```
airodump-ng -bssid 98:48:27:39:33:6B -w zachycenaData wlan0
```

Program `airodump-ng` může přijímat spoustu různých parametrů, ale v aktuálním testovacím scénáři postačuje použití jen některých. První parametr je BSSID testovacího přístupového bodu, protože není potřeba zbytečně zachytávat provoz jiné sítě. Druhý parametr je název souboru, do kterého bude uložen zachycený provoz. Poslední argument je název síťového rozhraní v monitorovacím režimu. Po spuštění programu se začne zachytávání provozu testovací sítí a tím pádem třetí bod testovacího plánu je splněn.

Dalším krokem testovacího plánu je spouštění sledování dat na stanici, která bude odesílat data jinému uživateli. Díky takovému sledování odesílaných dat je možné s vysokou přesností určit velikost skutečně přenesených dat. Dá se to zajistit spuštěním programu Wireshark a nastavením zachytávání provozu na síťovém rozhraní, které je připojeno do testovací bezdrátové síti.

Předposledním krokem v testovacím plánu je skutečný přenos dat. Po vyzkoušení různých metod, byl tento přenos dat realizován překopírováním souborů z jednoho notebooku do jiného. Dá se to udělat pomocí nastavení sdíleného síťového adresáře na jedné stanici a připojením jiné stanice do tohoto adresáře. Pak se dá spustit překopírování souboru z jedné stanice na druhou, tím bude zajištěno to generování provozu, které chceme odchytit, a navíc lze takový test jednoduše opakovat vícekrát

se stejným kopírovacím souborem, který zajistí zhruba stejnou velikost přenášených dat v každém měření.

Posledním krokem je uložení zachycených a regulárních dat po dokončení přenosu. Tento testovací plán byl splněn při provedení každého měření pro každý protokol 802.11 zvlášť. Podrobnější popis záchytu provozu jednotlivých protokolů je uveden v dalších kapitolách.

Výsledky záchytu provozu

Záchyt provozu probíhal podle dříve uvedeného testovacího plánu. Jedna stanice kopírovala soubor ze sdíleného síťového adresáře na jiné stanici. Velikost souboru byla zhruba 29 MB. Výsledek testu je uveden v tabulce 3.1.5.

Protokol	Pořadí testu	Odesláno bajtů	Zachyceno bajtů	Ztrátovost
802.11a	1	29 432 106	28 267 680	3,956%
802.11a	2	29 437 522	28 110 224	4,509%
802.11b	1	29 398 043	24 590 858	16,352%
802.11b	2	29 412 459	24 544 656	16,55%
802.11g	1	29 403 839	25 414 100	13,569%
802.11g	2	29 392 139	25 583 886	12,957%
802.11n	1	29 470 972	25 780 424	12,522%
802.11n	2	29 403 885	26 209 654	10,863%
802.11ac	1	29 396 219	27 275 740	7,213%
802.11ac	2	29 394 931	27 249 041	7,3%

Tab. 3.3: Výsledky záchytu provozu v závislosti na protokolu

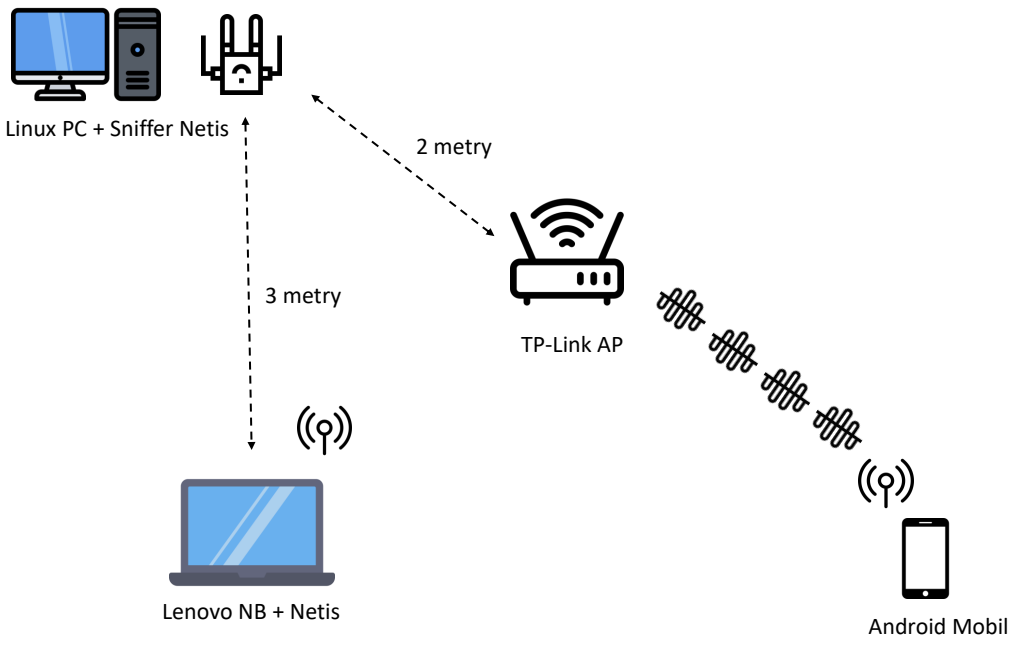
Bylo provedeno zachytávání provozu sítí pro nejčastěji používané standardy protokolu IEEE 802.11, jsou to verze a/b/g/n/ac. Pro větší přesnost, záchyt provozu se prováděl dvakrát pro každý protokol, tedy celkově v prvním testovacím scénáři bylo provedeno 10 testů. Takové údaje jako počet zachycených bajtů, počet odeslaných bajtů a ztrátovost, jsou uvedené na základě výpočtů pomocí skriptů pro analýzu, podrobný popis tohoto skriptu byl uveden dříve. Výsledky testů budou analyzované v následujících kapitolách.

3.1.6 Záchyt provozu v závislosti na frekvence a vytíženost sítí

Tato kapitola se věnuje druhému testovacímu scénáři, tedy záchytu provozu sítě 802.11 v závislosti na frekvenci a vytíženosti sítě. Cílem testovacího scénáře je určit závislost záchytu provozu na použité frekvenci a vytíženosti sítě, například pro případy když v je v síti více uživatelů, kteří generují provoz.

Popis testovacího plánu a prostředí

Záchyt provozu ve druhém testovacím scénáři byl proveden ve stejné místnosti jako při testování prvního scénáře. Rozdíl ale byl ve struktuře testovací sítě, tato struktura je znázorněna na obrázku 3.8.



Obr. 3.8: Druhý testovací scénář.

Testovací síť druhého scénáře se skládá z několika zařízení. První je Linux PC s připojenou sondou která se nachází na vzdálenosti přibližně 2 metry od přístupového bodu. Cílem sondy je záchyt provozu jako v prvním scénáři. Dalším zařízením je Android mobil, který je připojen k testovací síti. Tento mobil má za úkol se chovat jako legitimní uživatel v síti. Mobil měl spouštěné přímé online vysílání, aby zatížit testovací síť. Další důležité zařízení je notebook s připojeným Netis. Tento notebook má za úkol posílat datové rámce pomocí Python skriptů, popis skriptu byl uveden dříve. Poslední zařízení v síti je samotný přístupový bod TP-Link. Tento přístupový bod se měnil nastavení protokolu 802.11 kvůli změně frekvence testovací WiFi sítě. Testovací plán druhého scénáře se skládá z následujících bodů:

1. Nastavit frekvence pro testovací WiFi síť na přístupovém bodě TP-Link.
2. Připojit Android mobil k testovací síti a spustit sledování živého vysílání.
3. Spustit odposlech provozu snifferem.
4. Převést Netis na vysílající stanici do režimu monitorování.
5. Spustit Python skript na testovací stanici.

6. Po dokončení vysílání datových rámců skriptem, uložit zachycená data snifferem.

Pro nastavení frekvence sítě, byla využita možnost systémového nastavení přístupového bodu TP-Link v ovladači. Dalším krokem bylo připojení Android mobilu a spuštění sledování živého vysílání. Po splnění tohoto bodu testovacího plánu, máme zajištěno, že v síti se bude generovat velký provoz dat, tím se dá simulovat vytíženost sítí. Třetím krokem bylo spuštění odposlechu provozu snifferem. Postup spuštění snifferu je úplně stejný jako v prvním testovacím scénáři. Nastavení režimu monitorování na vysílající stanici Netis se dá udělat stejně jako u snifferu, jen není potřeba na konci postupu spouštět záchyt provozu. Monitorovací režim je potřeba spustit, aby Python skript byl schopen posílat vygenerované datové rámce. Podle dokumentace knihovny Scapy, posílání vlastních rámců 802.11 na bezdrátové rozhraní by mělo fungovat i v obyčejném, tedy `managed` režimu. Ale prakticky se prokázalo, že takový způsob je problematický a občas se nechová podle očekávání. Pátý krok je spouštění Python skriptů pro generování datových rámců, lze je spustit pomocí příkazu:

```
python3 scapyPacketSender.py
```

Po spouštění skriptů by sonda, která funguje v režimu odposlechu, měla zachytit datové rámce generované skriptem.

Výsledky druhého testovacího scénáře

Testování druhého scénáře probíhalo následujícím způsobem: zaprvé se provedl záchyt rámců v síti s frekvencí 2,4 GHz, pak pro frekvence 5 GHz. Bylo provedeno 6 testů pro každou frekvenci takovým způsobem, že 3 testy záchytu provozu v síti s minimální vytížeností a 3 testy při větším provozu v síti. Celkově tedy bylo provedeno 12 testů, výsledky testů v síti 2,4 GHz jsou uvedené v tabulce 3.4.

Frekvence	**Pořadí testu**	**Vytíženost sítě**	**Odesláno rámců**	**Zachyceno rámců**
2,4 GHz	1	Bez provozu	100	84
2,4 GHz	2	Bez provozu	100	83
2,4 GHz	3	Bez provozu	100	87
2,4 GHz	1	S provozem	100	47
2,4 GHz	2	S provozem	100	38
2,4 GHz	3	S provozem	100	41

Tab. 3.4: Výsledky záchytu provozu v síti 2,4 GHz.

Frekvence	Pořadí testu	Vytíženost sítě	Odesláno rámců	Zachyceno rámců
5 GHz	1	Bez provozu	100	92
5 GHz	2	Bez provozu	100	99
5 GHz	3	Bez provozu	100	87
5 GHz	1	S provozem	100	68
5 GHz	2	S provozem	100	75
5 GHz	3	S provozem	100	93

Tab. 3.5: Výsledky záchytu provozu v síti 5 GHz.

Stejná sada testů byla provedena pro síť 5 GHz, výsledky testů jsou uvedené v tabulce 3.5.

Třetí sloupec označuje, zda bylo spouštěno sledování živého vysílání na mobilu nebo ne, tím se určuje vytíženost sítě v tomto testovacím scénáři. Tento způsob je dost efektivní, protože při spouštěném sledování živého vysílání bylo v síti posláno cca 20 tisíc rámců, což je dostačující vytíženost pro provedení testu. Počet odeslaných rámců ve vytížené síti lze vidět ve sloupci `Data` na obrázku 3.9.

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

98:48:27:39:33:6B  -14   0      288    21886  640  11   54e. WPA2 CCMP   PSK  HackMeIfYouCan
64:EE:B7:C6:75:B4  -35   0        0        0    0  11   -1                   <length:  0>
52:DF:9A:38:6C:7A  -67  93      288        3    0  11   65   WPA2 CCMP   PSK  Connectify-me
34:68:95:81:73:91  -73  60      219        0    0  11   65   WPA2 CCMP   PSK  Connectify-K Raihan
62:6D:C7:D1:75:67  -76  61      167        0    0  11   65   WPA2 CCMP   PSK  Connectify-me
9A:2C:BC:34:3F:87  -79  68      195        0    0  11  130   WPA2 CCMP   PSK  ForTheHorde
0A:EE:E6:B7:79:D8  -92   0        3        0    0  11  130   WPA2 CCMP   PSK  SAVKE

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   36:4E:47:DD:C2:BC  -35    0 - 1      3         5         HackMeIfYouCan
(not associated)   68:54:5A:03:77:85  -67    0 - 1      0         3
(not associated)   70:C9:4E:AF:CA:7B  -67    0 - 1      0        17
(not associated)   3C:91:80:85:24:35  -73    0 - 1      0         5
(not associated)   2E:2A:49:FC:7C:5D  -83    0 - 1      0         2
```

Obr. 3.9: Příklad vytíženosti sítě 2,4 GHz s provozem.

Při provedení stejného testu v síti bez provozu bylo na pozadí generováno jen málo rámců, vytíženost sítě lze vidět ve sloupci `Data` na obrázku 3.10.

3.1.7 Obecný záchyt provozu naslouchánímokolního prostředí

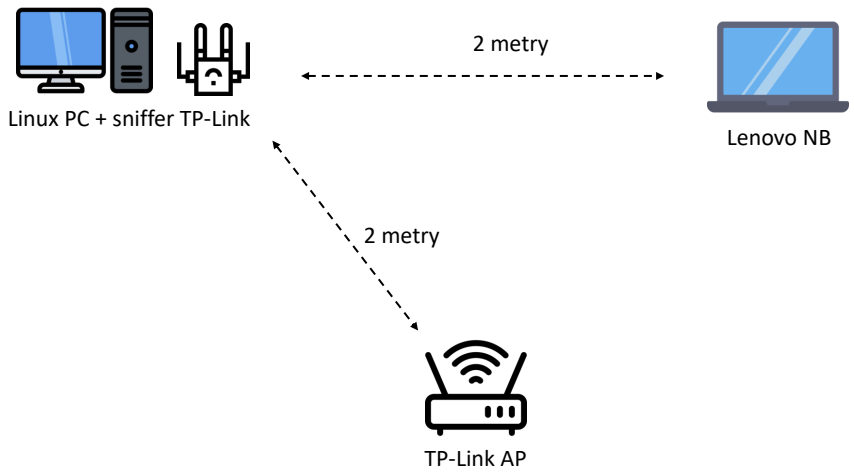
V kapitole je popsán třetí testovací scénář, který se věnuje obecnému pasivnímu odposlechu sítí 802.11. Cílem scénáře je prakticky ověřit, která data se dají odchytit a které informace se dají zjistit pomocí pasivního odposlechu jak zabezpečené tak i otevřené sítě.

```
BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

98:48:27:39:33:6B  -17 100      360       30    0  11   54e. WPA2 CCMP   PSK  HackMeIfYouCan
64:EE:B7:C6:75:B4  -48  37        0        0    0  11   -1                    <length:  0>
C2:91:33:C3:1F:71  -54 100      201     1392   82  11  130   WPA2 CCMP   PSK  Connectify-Yaygo
52:DF:9A:38:6C:7A  -68 100      360        0    0  11   65   WPA2 CCMP   PSK  Connectify-me
34:68:95:81:73:91  -70  93      350        0    0  11   65   WPA2 CCMP   PSK  Connectify-K Raihan
62:6D:C7:D1:75:67  -76  58      287      622    0  11   65   WPA2 CCMP   PSK  Connectify-me
9A:2C:BC:34:3F:87  -80  66      283        0    0  11  130   WPA2 CCMP   PSK  ForTheHorde
0A:EE:E6:B7:79:D8  -91   0       14        1    0  11  130   WPA2 CCMP   PSK  SAVKE

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

(not associated)   20:16:B9:40:D2:EC  -81    0 - 6      0         1
(not associated)   60:6D:C7:D1:7D:67  -81    0 - 1     11         3
(not associated)   12:FC:F8:C3:8B:DB  -39    0 - 1      0         6
(not associated)   70:C9:4E:AF:CA:7B  -67    0 - 1     18        15
(not associated)   70:28:8B:8C:41:E6  -65    0 - 1      0         9
(not associated)   68:54:5A:03:77:85  -73    0 - 1      0         5
```

Obr. 3.10: Příklad vytíženosti sítě 2,4 GHz bez provozu.

Popis testovacího plánu a prostředí

Při provedení testu třetího scénáře, bylo použito jiné zařízení pro sniffer, protože v obou provedených testech, USB WiFi Netis, který byl použit v prvních dvou scénářích, nebyl k dispozici. Pro roli sniffera bylo tedy použito jiné USB WiFi rozhraní, které taky podporuje monitorovací režim – TP-Link WN727N. Testovací prostředí bylo zapojené podle obrázku 3.11.



Obr. 3.11: Třetí testovací scénář.

Vzhledem k tomu, že třetí testovací scénář se věnuje obecnému odposlechu, bez zaměření na konkrétní kritéria, bylo rozhodnuto provést záchyt provozu sítě protokolu IEEE 802.11n, který funguje ve frekvenčním pásmu 2,4 GHz, protože je to asi nejčastěji běžně používaný protokol, se kterým se setkáváme prakticky každý den. Testovací plán je následující:

1. Nastavit protokol 802.11 pro testovací síť na přístupovém bodě.
2. Převést sondu do režimu odposlechu a spustit Traffic Analyzer.
3. Připojit notebook do testovací sítě a vygenerovat provoz (například prohlížením různých webů).
4. Zastavit Traffic Analyzer.

Jak lze vidět z testovacího plánu, tento scénář očekává použití Python programu Traffic Analyzer, jehož popis byl uveden dřív. Díky tomuto programu lze hned v konzoli sledovat zachycený provoz a to jak ve zkráceném formátu výpisů, tak i v podrobnějším formátu.

První krok testovacího plánu je úplně stejný jako u předchozích scénářů. Ve druhém bodě je potřeba přepnout rozhraní do monitorovacího režimu, i když v aktuálním scénáři bylo použito jiné zařízení, nastavení monitorovacího režimu je úplně stejné jako u Netis. Dalším krokem je spuštění Traffic Analyzer a generování provozu. Generovat provoz je možné například sledováním živého vysílání nebo prohlížením webu, během testování byly kombinovány oba způsoby, aby zachycená data byly různá a provoz se více podobal běžnému provozu v síti. Nakonec, po skončení generování provozu, je možné vypnout program. Výsledky odposlechů provozu, tedy jednotlivé rámce, je možné prohlídnout hned v Traffic Analyzer nebo exportovat do externího programu.

Výsledky třetího testovacího scénáře

Po úspěšném provedení všech kroků testovacího plánu, program zachytil potřebná data. Testování probíhalo dvakrát, první pro síť 802.11n se zabezpečením WPA-2, druhý test byl pro otevřenou síť, tedy bez zabezpečení, se stejným protokolem 802.11n. Podrobnější popis zachycených dat a jednotlivých rámců je v kapitole analýzy třetího testovacího scénáře.

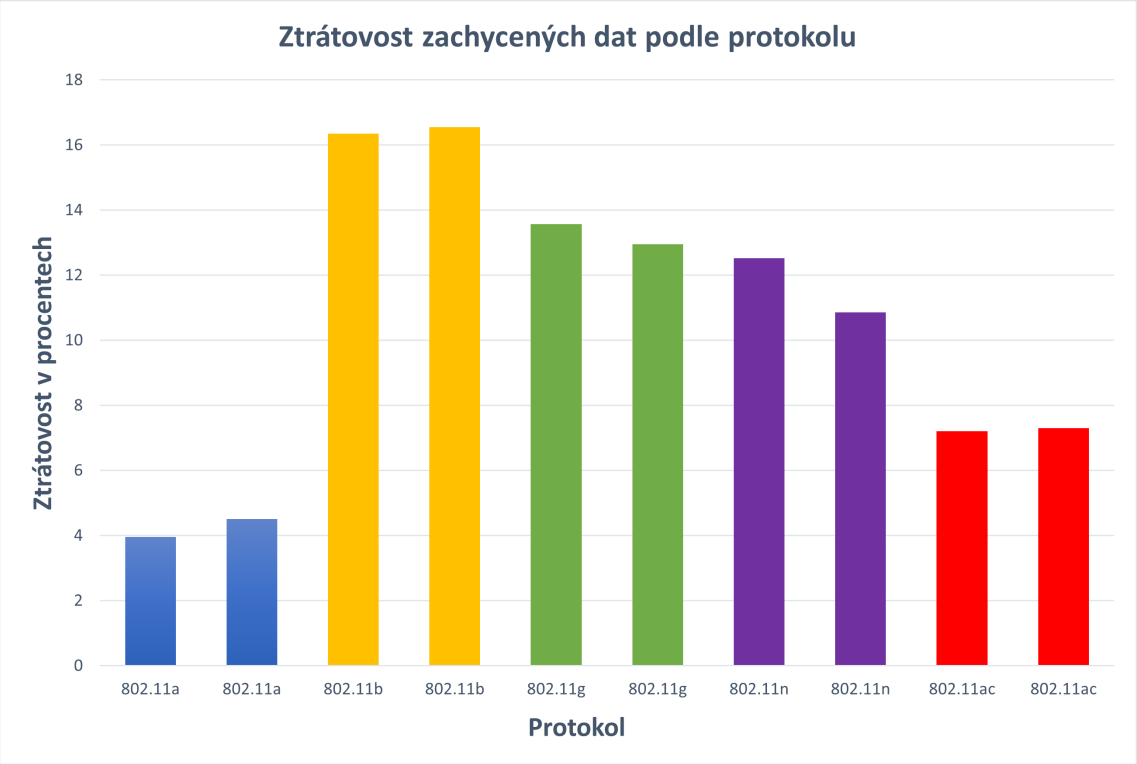
3.1.8 Analýza výsledků měření

Kapitola se věnuje podrobnějšímu popisu výsledku. Každý testovací scénář je začleněn do samostatné podkapitoly.

Analýza zachyceného provozu dle jednotlivých protokolů

Cílem testovacího scénáře bylo prozkoumat pasivní odposlech nejčastěji používaných

protokolů 802.11 a určit závislost přesnosti zachycených dat na použitém protokolu. Bylo provedeno 10 testovacích záchytů provozu pro různé protokoly, výsledky testů jsou uvedené v tabulce 3.1.5. Pro lepší přehlednost, na základě výsledků testování, byl vytvořen graf znázorněný na obrázku 3.12.



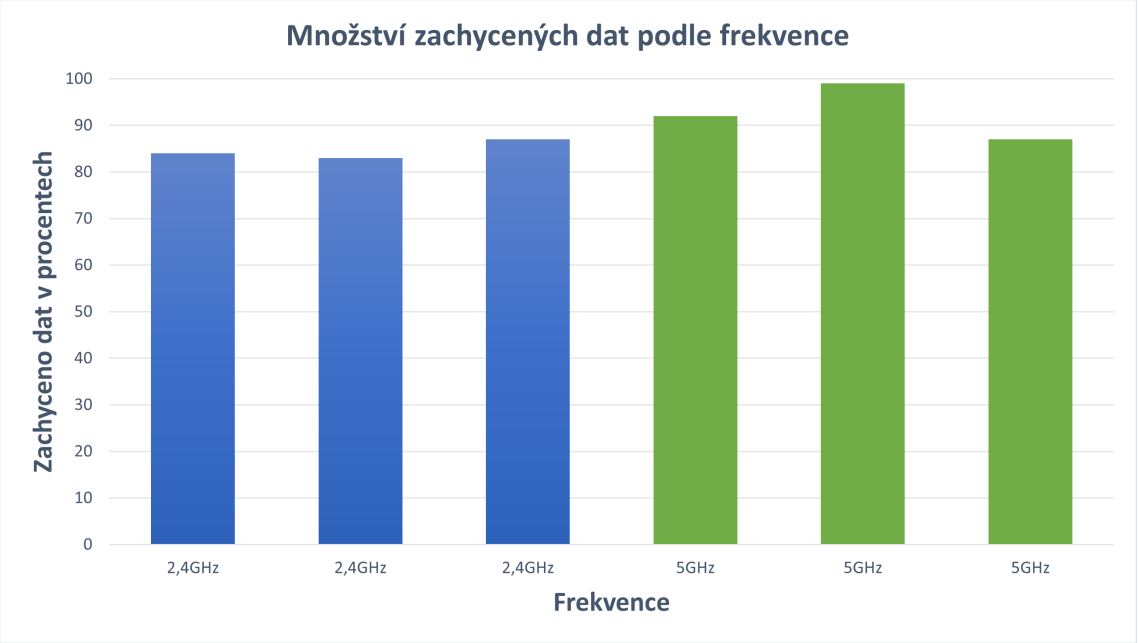
Obr. 3.12: Ztrátovost dat podle protokolu.

V grafu lze vidět, že záchyt povozu sítě některých protokolů 802.11 je mnohem efektivnější než jiných protokolů, jsou to například protokoly 802.11a a 802.11ac, kde ztrátovost dat u protokolu 802.11ac je kolem 8% a pro 802.11a až 4%, což je dost málo. Někde uprostřed se nachází dva, asi nejčastěji používané, protokoly, jsou to 802.11n se ztrátovostí kolem 11% a 13% u 802.11g. Největší ztrátovost dat při pasivním odposlechu měl protokol 802.11b, kolem 16%.

Na efektivitu odposlechů provozu mohou mít vliv různé faktory, jako například rušení nebo vytíženost kanálů, ovšem z výsledků testů je možné říct že pasivní odposlech bezdrátové sítě protokolu 802.11a nebo 802.11ac zachytí mnohem více dat než u jiné sítě, nejspíš je to dáno tím, že tyto protokoly fungují na frekvenci 5 GHz, která není moc vytížená. Takový předpoklad lze ověřit podle výsledku druhého testovacího scénáře, který právě porovnával odposlech provozu ve závislosti na použité frekvenci v síti.

Analýza zachyceného provozu dle frekvence a vytíženosti sítí

Jedná se o druhý testovací scénář, cílem kterého bylo určit závislost efektivity pasivního odposlechů provozu sítě na použité frekvenci a vytíženosti sítě. Výsledky testů jsou uvedené v tabulkách 3.4 pro síť 2,4 GHz a 3.5 pro 5 GHz. Z naměřených dat jsou vytvořené grafy. Na prvním grafu číslo 3.13 lze vidět množství zachycených dat podle použité frekvence v síti.

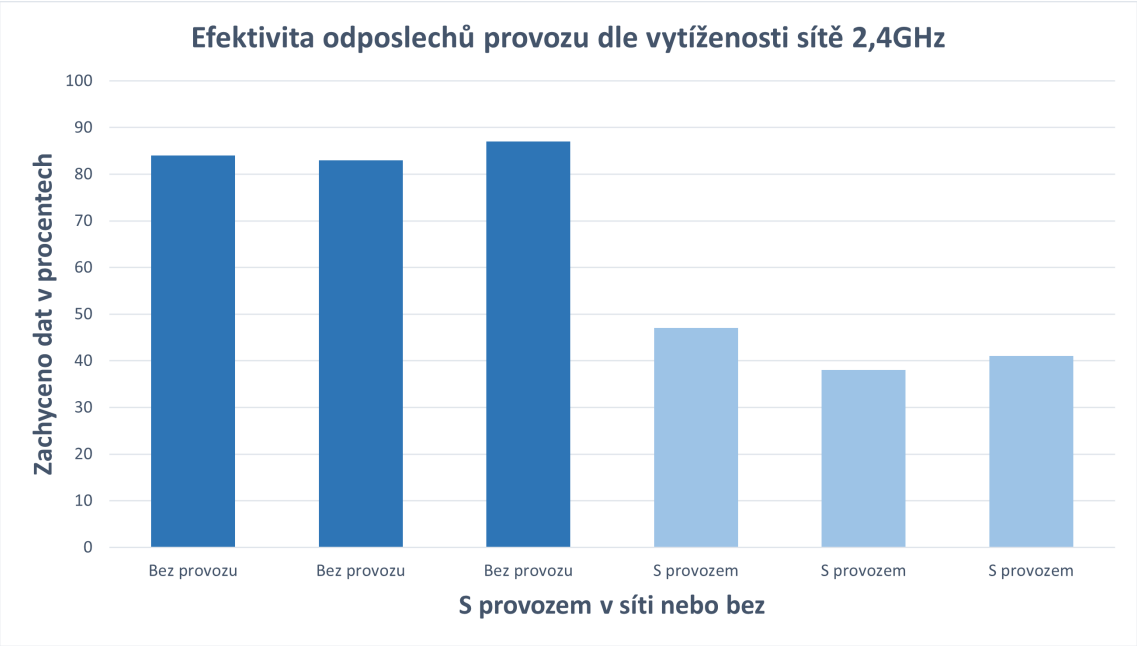


Obr. 3.13: Efektivita odposlechů provozu podle frekvence.

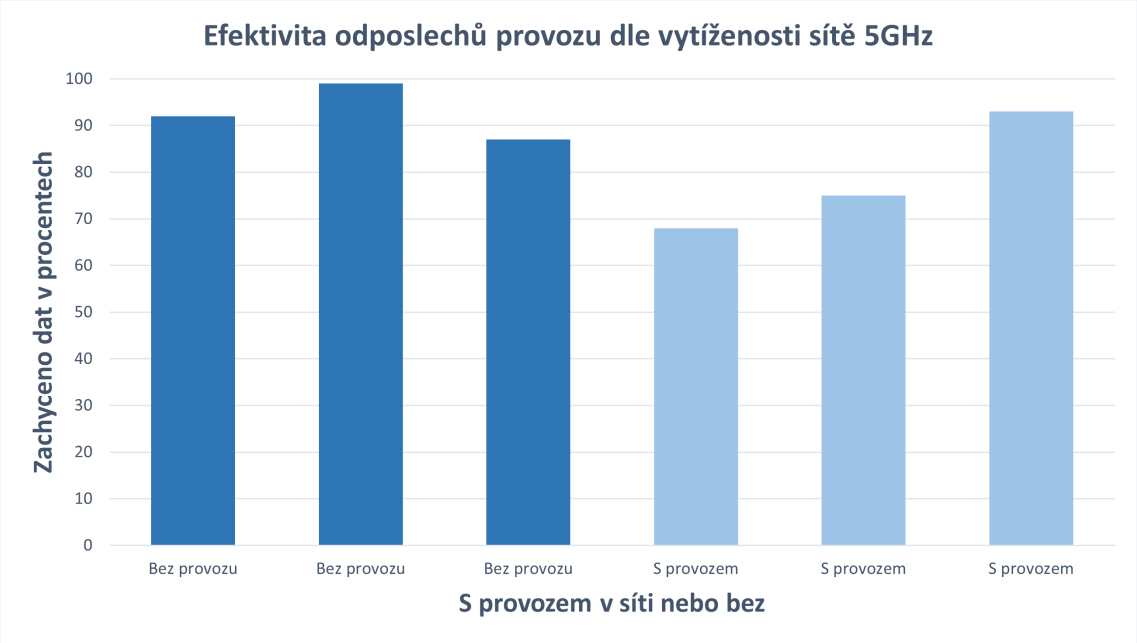
Na základě naměřených dat v grafu lze říct, že efektivnější odposlech provozu sítě bude na frekvenci 5 GHz. Nicméně, když spočítáme průměrnou ztrátovost odposlechů v obou sítích a porovnáme mezi sebou, rozdíl ztrátovosti dat v síti 2,4GHz a 5 GHZ stanoví 8%, tedy při odposlechu sítě 5 GHz lze ve většině případů zachytit o 8% dat více, než u sítě 2,4 GHz.

Další graf číslo 3.14 umožňuje porovnávat efektivitu odposlechů provozu sítě vzhledem k vytíženosti sítě. Z naměřených dat lze vidět, že při odposlechu provozu vytížené sítě 2,4 GHz se ztrátovost dát zvýšila zhruba o 40%. Na základě toho lze tvrdit, že při odposlechu sítě 2,4 GHz, ke které je připojeno více uživatelů, generujících provoz, je dost obtížné odchytit provoz určitého připojeného zařízení.

Následující graf 3.15 znázorňuje obdobnou situaci pro síť s použitou frekvenci 5 GHz. Podle naměřených hodnot lze usoudit, že při odposlechu provozu vytížené sítě 5 GHz se ztrátovost zvyšuje přibližně o 14%, takže ten rozdíl není tak extrémní, jako například u sítě 2,4 GHz.



Obr. 3.14: Efektivita odposlechů provozu dle vytíženosti sítě 2,4 GHz.



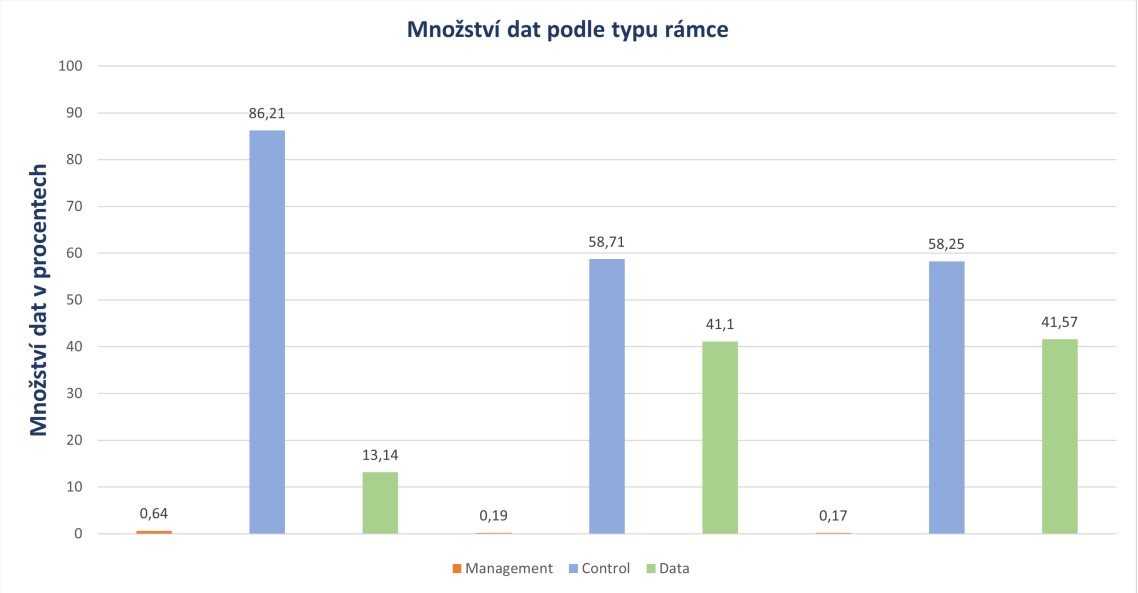
Obr. 3.15: Efektivita odposlechů provozu dle vytíženosti sítě 5 GHz.

Analýza zachycených dat naslouchánim okolního prostředí

Cílem třetího testovacího scénáře bylo určit, která data lze odchytit a jaké informace lze zjistit při pasivním odposlechu zabezpečené a otevřené sítě. Obecně platí, že sí-

tový provoz bezdrátové sítě 802.11 obsahuje hodně různých informaci, jako například rámce nesoucí údaje o přístupovém bodě. Nejprve začneme analýzou provozu nezabezpečené sítě, protože provoz takové sítě obsahuje poměrně velkou sadu informací.

Graf číslo 3.16 znázorňuje počet rámců různého typu z celkového provozu sítě.



Obr. 3.16: Množství dat podle typu rámce.

Odposlech provozu sítě byl proveden třikrát a podle naměřených dat lze vidět, že ve všech případech většinu provozu sítě stanoví kontrolní rámce. Je to logické, protože kontrolní rámce pomáhají s dodáním datových rámců. To znamená, že jejich počet stanoví většinu zachyceného provozu.

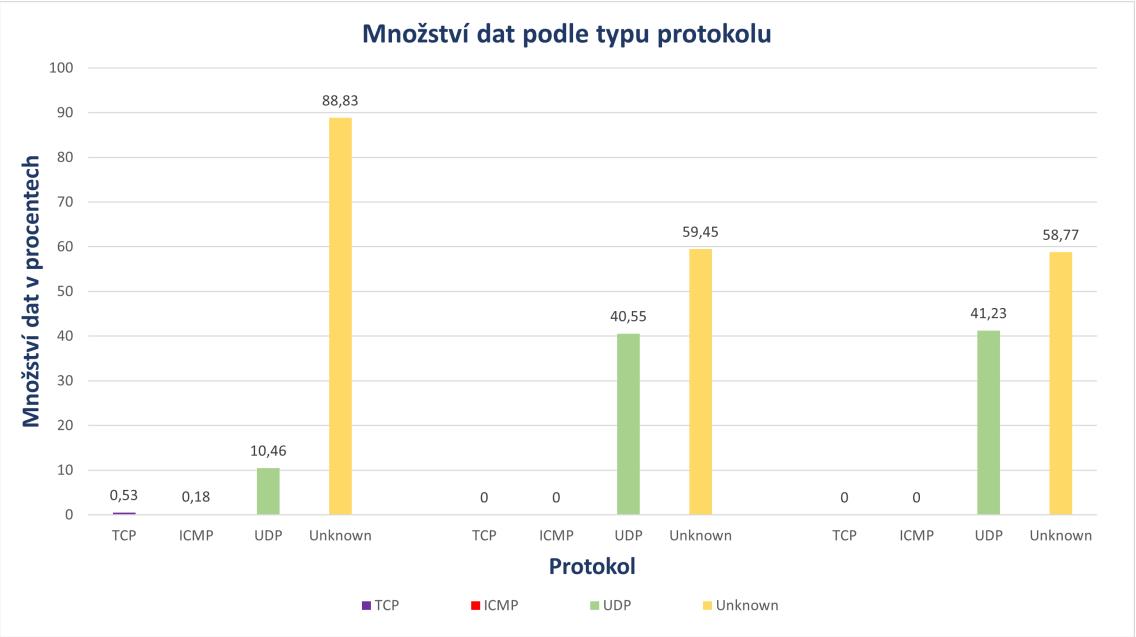
Následující graf 3.17 znázorňuje počet výskytů jednotlivých protokolů při každém měření. Vzhledem k tomu, že většinu provozu stanoví řídící rámce, které neobsahují hlavičku s definicí protokolu, v tomto grafu většina rámců spadá do skupiny `Unknown`.

Při odposlechu provozu zabezpečené sítě, je situace téměř stejná, ale s jedním rozdílem. Ze zachyceného provozu zabezpečené sítě nelze zjistit použitý protokol kvůli šifrovanému provozu, jinak pro zabezpečenou síť platí stejná situace, že většinu provozu stanoví kontrolní rámce.

Data ve veřejné síti

Ze zachyceného provozu nezabezpečené sítě se dá zjistit celkem hodně informací. Nástroj Traffic Analyzer spuštěný v RAW režimu vypíše do konzoly všechno, co se dá zjistit. Například hlavička kontrolního rámce sítě 802.11 vypadá následovně:

Výpis 3.8: Hlavička kontrolního rámce



Obr. 3.17: Množství dat podle protokolu.

```
###[ 802.11 ]###
     subtype   = 12
     type      = Control
     proto     = 0
     ID        = 29696
     addr1     = 14:9f:e8:0e:99:cd
```

Pouze z jedné hlavičky se dá zjistit spoustu informací, například typ a podtyp rámce, použitý protokol, ID rámce a cílovou MAC adresu. Dále ve výpisu 3.9 je znázorněna struktura hlavičky pro jiné rámce, například `QoS`, `LLC` a `SNAP`.

Výpis 3.9: Struktura hlavičky rámců `QoS`, `LLC` a `SNAP`

```
###[ 802.11 QoS ]###
     Reserved  = 0
     Ack_Policy= 0
     EOSP      = 0
     TID       = 0
     TXOP      = 0
###[ LLC ]###
     dsap      = 0xaa
     ssap      = 0xaa
     ctrl      = 3
###[ SNAP ]###
```

```
    OUI         = 0x0
    code        = IPv4
```

Zajímavá je hlavička IP rámce, mezi nejdůležitější položky patří verze IP protokolu, délka, použitý protokol, zdrojová a cílová IP adresa. Příklad hlavičky IP rámce je uveden ve výpisu 3.10.

Výpis 3.10: Struktura hlavičky IP rámce.

```
###[ IP ]###
    version   = 4
    ihl       = 5
    tos       = 0x0
    len       = 59
    id        = 26205
    flags     = DF
    frag      = 0
    ttl       = 64
    proto     = udp
    chksum    = 0xfcc5
    src       = 192.168.43.61
    dst       = 192.168.43.1
```

Taky je možné zjistit důležité informace z rámce použitého protokolu. Výpis 3.11 znázorňuje hlavičku rámce UDP.

Výpis 3.11: Struktura hlavičky UDP rámce.

```
###[ UDP ]###
    sport     = 28988
    dport     = domain
    len       = 39
    chksum    = 0xc8a7
```

Díky hlavičce rámce UDP je možné zjistit zdrojový a cílový port. Na základě čísla portu pak lze předpokládat, s jakou službou na internetu komunikuje zařízení uživatele. Velmi zajímavou informaci je také možné zjistit z DNS rámce, výpis takového rámce je uveden pod číslem 3.12.

Výpis 3.12: Struktura rámce DNS.

```
###[ DNS ]###
    id        = 3585
    qr        = 0
    opcode    = QUERY
    aa        = 0
```

```
    tc        = 0
    rd        = 1
    ra        = 0
    z         = 0
    ad        = 0
    cd        = 0
    rcode     = ok
    qdcount   = 1
    ancount   = 0
    nscount   = 0
    arcount   = 0
    ###[ DNS Question Record ]###
        qname     = 'www.avast.com.'
        qtype     = A
        qclass    = IN
        an        = None
        ns        = None
        ar        = None
```

Například z uvedeného rámce lze zjistit, že uživatel navštívil webovou stránku `www.avast.com`.

Je zřejmé, že ze zachyceného provozu otevřené sítě se dají zjistit hodně užitečné informace, například: typ a podtyp rámce, zdrojovou a cílovou MAC adresy, použitý protokol, QoS data, informace o IP, UDP a DNS, případně kterou webovou stránku uživatel navštívil. V některých rámcích se dá najít zařízení, ze kterého byl připojen uživatel.

Data v zabezpečené síti

V zabezpečené síti kvůli šifrování nelze zjistit podrobnější informace, ale jen základní. Výpis 3.13 znázorňuje strukturu datového rámce zabezpečené sítě.

Výpis 3.13: Datový rámec zabezpečené sítě.

```
###[ 802.11 ]###
  subtype   = 8
  type      = Data
  proto     = 0
  FCfield   = to-DS+protected
  ID        = 12288
  addr1     = c8:3d:d4:6d:4a:4d
  addr2     = 18:f0:e4:d0:f6:71
  addr3     = c8:3d:d4:6d:4a:4d
```

```
  SC         = 64992
###[ 802.11 QoS ]###
     Reserved  = 0
     Ack_Policy= 0
     EOSP      = 0
     TID       = 0
     TXOP      = 0
###[ 802.11 TKIP packet ]###
        PN0       = 224
        PN1       = 63
        res0      = 0
        key_id    = 0
        ext_iv    = 1
        res1      = 0
        PN2       = 0
        PN3       = 0
        PN4       = 0
        PN5       = 0
        data      = '\xb5\x7f\xdd\xe1\xe3Nj,\x90\x9d\xc...'
```

Podle výpisu 3.13 lze vidět, že z datového rámce zabezpečené sítě je možné zjistit takové informace, jako typ a podtyp rámce, zdrojovou a cílovou MAC adresu, hlavičku `QoSData` a také `TKIP packet`, který obsahuje samotná data ve zašifrovaném formátu.

Závěr

Bakalářská práce je zaměřena na standard IEEE 802.11 pro rodinu bezdrátových protokolů. V teoretické části je popsán design sítí postavených na protokolu 802.11 a jednotlivé vrstvy komunikace. Taky teoretická část se věnuje různým standardům protokolů 802.11, jejich výhodám a nevýhodám. Následně se práce věnuje bezpečnosti protokolu 802.11. V části věnované bezpečnosti jsou popsané bezpečnostní protokoly WEP, WPA, WPA2 a jejich odlišnosti. V neposlední řadě jsou popsané možnosti prolomení každého protokolu a možností pasivního odposlechu. Taky jsou uvedena dostupná hardwarová zařízení pro pasivní odposlech bezdrátové sítě.

Praktická část je zaměřena na implementaci programu pro analýzu zachyceného provozu. První návrh programu byl v programovacím jazyce JAVA. Vzhledem k tomu, že se nepodařilo vyřešit chyby při použití specifických knihoven pro práci se zachyceným provozem, byl napsán nástroj v jazyce Python 3. Pro zachytávání provozu byla použita knihovna Scapy. Pro vykreslování grafů Matplotlib a PyQt5 pro GUI.

Program je určen pro zachytávání a následnou analýzu naměřených dat Wi-Fi provozu. Traffic Analyzer obsahuje celou řadu možností. Uživatel si tedy může zvolit, co chce zachytávat pomocí výběru. Kromě toho má uživatel k dispozici sekci detailů o přístupovém bodu. V této sekci najde informace o počtu a typu přenesených rámců během provozu, MAC adresu přístupového bodu, frekvenci, na které přístupový bod vysílá, velikost přenesených dat a taky sílu vysílání přístupového bodu, díky čemu lze odhadnout vzdálenost přístupového bodu. Kromě toho je uživateli umožněno si prohlédnout seznam MAC adres připojených uživatelů do určitého AP.

Program uživateli nabízí také několik typů grafů, které se průběžně aktualizují během zachycení provozu, každých 50 ms. Uživatel si tak může zvolit, který typ grafu se má zobrazovat a pro která data, jedna možnost je výpočet a znázornění statistiky pro všechna data, druhá možnost jen pro data určitého přístupového bodu.

Další možnost programu je výpis informace do sekcí konzoly. V této konzoli se zobrazuje výpis informací o zachyceném rámci. Pomocnými tlačítky uživatel může zvolit, jaký výpis chce. Pokud uživatel zvolí režim `RAW`, do konzole se bude vypisovat veškerá informace, kterou se dá zjistit z rámce. Pokud režim výpisu bude `Summary`, tak se vypíše jen základní informace o rámci, tedy typ rámce, podtyp, zdrojová a cílová MAC adresy apod. Obsah vypsané informace záleží na typu rámce.

Kromě samotného programu byly napsány dva Python skripty které jsou užitečné při analýze provozu. Jeden skript je určen pro porovnání zachyceného a regulérního provozu. Na základě vzorku dat skript určí celkovou ztrátovost dat při odposlechu. Další skript je určen pro vygenerování a odeslání datových rámců 802.11.

V rámci praktické části bylo taky provedeno měření podle třech testovacích scé-

nářů. V prvním testovacím scénáři byl proveden odposlech provozu bezdrátové sítě pro nejčastěji používané protokoly 802.11. Tak bylo prakticky ověřeno že efektivita odposlechů provozu sítě je závislá na použitém protokolu v síti. Také prokázáno úspěšné zachytávání provozu porovnáním zachycených a regulérních dat.

Ve druhém testovacím scénáři bylo ověřeno, jaký vliv má použitá frekvence bezdrátové sítě a vytíženost sítě na ztrátovost při pasivním odposlechu provozu.

Třetí testovací scénář byl zaměřen na obecný odposlech provozu bezdrátové sítě a zjišťování, které informace lze zjistit ze zachyceného provozu. Tak se prakticky ukázalo, že při odposlechu otevřené sítě lze zjistit velké množství informací, oproti tomu při odposlechu zabezpečené sítě je možné vyčíst jen základní údaje o provozu.

Literatura

[1] GONG, Michelle, Brian HART a Shiwen MAO. *Advanced Wireless LAN Technologies: IEEE 802.11AC and Beyond. GetMobile: Mobile Computing and Communications* . ACM, 2015, 18(4), 48-52 [cit. 2019-09-15]. DOI: 10.1145/2721914.2721933. ISSN 15591662.

[2] RIGELSFORD, Jon. *802.11 Wireless Networks: The Definitive Guide. Sensor Review* Emerald Group Publishing Limited, 2003, 23(2) [cit. 2019-09-15]. DOI: 10.1108/sr.2003.08723bae.003. ISSN 0260-2288.

[3] IEEE *IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications in IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)* , vol., no., pp.1-3534, 14 Dec. 2016, doi: 10.1109/IEEESTD.2016.7786995.

[4] GEIER, Jim. *Wireless LANs: implementing high performance IEEE 802.11 networks. 2nd ed.* Indianapolis: SAMS, 2002. ISBN 0-672-32058-4.

[5] SANTAMARIA, A. a F. J. LOPEZ-HERNANDE *Z. Wireless LAN standards and applications*, Boston: Artech House, c2001. Artech House mobile communications series. ISBN 0-89006-943-3.

[6] Bruce Potter and Bob Fleck, *802.11 Security*, O'Reilly and Associates, 2002; ISBN: 0-596-00290-4.

[7] Jon Edney and William A. Arbaugh, *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*, Addison Wesley, 2003, ISBN: 0-321-13620-9

[8] Rob Flickenger, *Wireless Hacks: 100 Industrial-Strength Tips & Tools*, O'Reilly and Associates, September 2003, ISBN: 0-596-00559-8

[9] Hossein Bidgoli *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management Handbook of Information Security* John Wiley & Sons, 2006 ISBN 0470051213, 9780470051214

[10] POTTER, Bruce a Bob FLECK. *802.11 security*. Sebastopol, Calif.: O'Reilly, c2003. ISBN 0-596-00290-4.

[11] SANKAR, Krishna. *Cisco wireless LAN security*. Indianapolis, IN: Cisco Press, c2005. Cisco Press networking technology series. ISBN 1-58705-154-0.

[12] T. Radivilova and H. A. Hassan, *Test for penetration in Wi-Fi network: Attacks on WPA2-PSK and WPA2-enterprise*, 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Odessa, 2017, pp. 1-4. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8095429&isnumber=8095353

[13] A. H. Lashkari, M. Mansoor and A. S. Danesh, *Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)*, 2009 International Conference on Signal Processing Systems, Singapore, 2009, pp. 445-449. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5166826&isnumber=5166728

[14] Xiaona Liao, Shaoqing Meng and Kaining Lu, *Security issues and solutions of WPA encrypted public wireless Local Area Network*, 2011 International Conference on Multimedia Technology, Hangzhou, 2011, pp. 3655-3657. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6002258&isnumber=6001647

[15] A. H. Adnan et al., *A comparative study of WLAN security protocols: WPA, WPA2*, 2015 International Conference on Advances in Electrical Engineering (ICAEE), Dhaka, 2015, pp. 165-169. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7506822&isnumber=7506780

[16] A. Kavianpour and M. C. Anderson, *An Overview of Wireless Network Security*, 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 306-309. URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7987214&isnumber=7987154

A Python skripty použité při řešení práce

A.1 Generátor datových rámců

Výpis A.1: Zdrojový kód skriptu generující datové rámce v jazyce Python.

```
from __future__ import print_function
from scapy.layers.dot11 import Dot11, RadioTap, Dot11QoS
from scapy.sendrecv import sendp

#Název testovací síti, je nutné pro frame typu Management
SSID = 'Test SSID'
#Název rozhraní přes které budou se posílat rámce
iface = 'wlan0'
#MAC adresa rozhraní wlan0
sender = '64:ee:b7:c6:75:b4'

# Zakomentovaný kód pro generování rámce typu Management
# dot11 = Dot11(type=0,
                subtype=8,
                addr1='ff:ff:ff:ff:ff:ff',
                addr2=sender,
                addr3=sender)
# beacon = Dot11Beacon()
# essid = Dot11Elt(ID='SSID',info=SSID, len=len(SSID))
#
# frame = RadioTap()/dot11/beacon/essid

#Generování rámce typu QoS Data
dot11=Dot11(type=2,
            subtype=8,
            addr1='ff:ff:ff:ff:ff:ff',
            addr2=sender,
            addr3=sender)
frame = RadioTap()/dot11/Dot11QoS()/"Some test payload ABCD"

print("Start sending 100 packets on wlan0 interface...")

#Předáme rámce do funkce, která ho odešle na síťové rozhraní
sendp(frame, iface=iface, inter=0.2, loop=1, count=100)

print("Finish...")
}
```

A.2 Analýza zachycených dat

Výpis A.2: Zdrojový kód skriptu pro určení ztrátovosti dát v jazyce Python.

```
from scapy.all import *
from scapy.layers.inet import TCP
from scapy.layers.dot11 import Dot11, Dot11QoS
import argparse

#Vytvoříme instance parseru,
#který umožní pracovat se vstupními parametry
parse = argparse.ArgumentParser ()

#Definujeme které argumenty podporuje script
#a očekává od uživatele
parse.add_argument ("ref", help = "Cesta do referenčních dat")
parse.add_argument ("cap", help = "Cesta do zachycených dat")

#Zapíšeme argumenty do slovníku
args = parse.parse_args()

#Zkontrolujeme počet argumentů,
#pokud méně než 2, script skončí
if len(args.__dict__) <= 1:
    print("Nejsou zadané argumenty")
    exit()

#Převede soubory ze vstupu na seznam rámců
referenceData = rdpcap(str(args.ref))
capturedData = rdpcap(str(args.cap))

#Iniciální velikost dat
referenceDataBytes = 0
capturedDataBytes = 0

#Procházíme referenční rámce,
#spočítáme celkocou velikost přenášených dat
for pkt in referenceData:
    try:
        referenceDataBytes += len(pkt[TCP])
    except:
        pass
```

```
                                                                    39
#Procházíme zachycené rámce,                                        40
#spočítáme celkocou velikost přenášených dat                        41
for pkt in capturedData:                                            42
    capturedDataBytes += len(pkt[Dot11])                            43
                                                                    44
#Spočítáme velikost ztracených dat a určíme ztrátovost              45
ztracenoDat = referenceDataBytes - capturedDataBytes                46
ztratovost =  (ztracenoDat / referenceDataBytes) * 100              47
                                                                    48
#Výpis výsledků                                                    49
print("Odeslano:␣" + str(referenceDataBytes) + "␣bajtů.")           50
print("Zachyceno:␣" + str(capturedDataBytes) + "␣bajtů.")           51
print("Ztrátovost:␣" + str(round(ztratovost, 3)) + "␣%")            52
}                                                                   53
```