VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 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
AUTHOR

Denys Partnov

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Jan Pospíšil

BRNO 2020

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:*** 2019/20

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: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: Ing. Jan Pospíšil
Konzultant: Ing. Radek Fujdiak, Ph.D.

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 vrsty, 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, 2020, 68 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. Jan Pospíšil. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

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 implmentovan 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 ověřená funkcionalita nástroje a ukázáno jakou informaci se dá zjistit během pasivnho odposlechů. Na základě naměřených dat byla provedena analýza provozu s využitím statistických údajů a grafů nově vytvořeného programu.

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 sítí. IEEE 802.11 je soustředěn na dvě poslední vrstvy OSI modelu, to jsou fyzická (PHY) a linková (MAC).

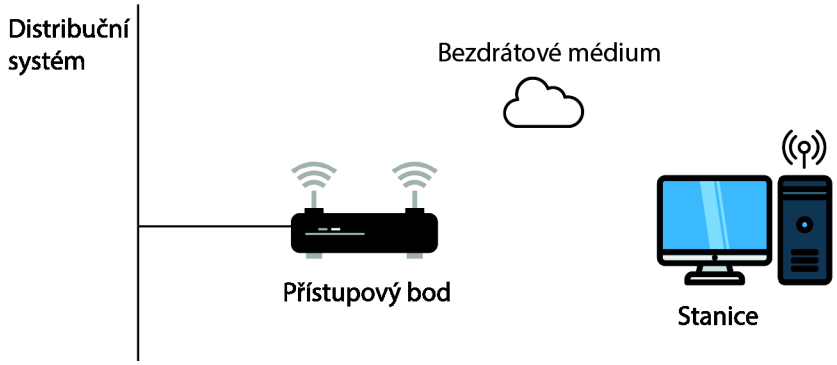
Fyzická vrstva definuje fyzikální vlastnosti všech zařízení jako jsou například napěťové úrovně a vlastnosti kabelů.

Linková vrstva uspořádá data z fyzické vrstvy do logických celků, rámců. Mezi jiné úkoly linkové vrstvy taky patří 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 s 802.3 což je Ethernet, z toho důvodu že byl vyvíjen z cílem zpětné kompatibility. V podstatě 802.11 je adaptace klasického Ethernetu pro bezdrátové prostředí. Například pro MAC adresy bezdrátových karet síťového rozhraní jsou přiřazeny 48bitové adresy, které pro praktické účely vypadají stejně jako adresy kart síťového rozhraní Ethernet. Ve skutečnosti přiřazení MAC adresy se 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 Design sítí 802.11

Sítí 802.11 obsahují čtyři hlavní fyzické prvky které jsou zobrazené na obrázku.



Obr. 1.1: Komponenty sítí 802.11

Distribuční systém

Pokud je připojeno několik přístupových bodů, aby vytvořili velkou oblast pokrytí, oni musí navzájem komunikovat. Distribuční systém je logickou součástí protokolu 802.11 používanou k předávání dál rámců do jejich cíle. 802.11 nespecifikuje žádnou konkrétní technologii pro distribuční systém. Ve většině komerčních produktů je distribuční systém implementován jako páteřní sítí používanou k přenosu rámců mezi přístupovými body, to je často nazýváno jednoduše páteřní sítí. Téměř ve všech komerčních produktach Ethernet je používán jako páteřní síťová technologie.[2]

Přístupový bod

Rámce v 802.11 sítí musí být převedené na jiný typ rámce aby bylo možné ho posílat rádiovým signálem. Zařízení Access point (Přístupový bod) provádí funkce konverze typu rámce, samozřejmě že přístupový bod má spoustu dalších důležitých funkcí ale tato patří mezi nejdůležitější.[2]

Bezdrátové médium

Pro přesun rámců ze stanice na stanici používá bezdrátové médium. Je definováno několik různých fyzických vrstev. Zpočátku dvě rádio frekvenční (RF) fyzické vrstvy a jedna infračervená fyzická vrstva byly standardizovány, i když se vrstvy RF ukázaly mnohem populárnější.[2]

Stanice

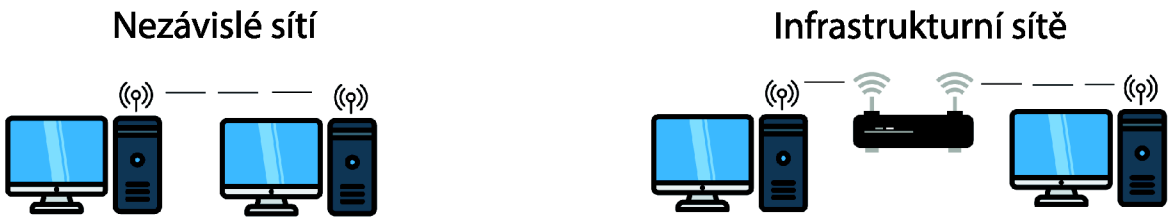
V sítí 802.11 stanici může být jakýkoliv počítač z síťovou kartou podporující bezdrátový přenos. Obvykle pod tímto pojmem si představujeme mobil nebo notebook ale neexistuje žádný důvod proč stanice musí být přenoste, to může být i klasický PC.[2]

1.1.2 Typy sítí

Základem jakékoliv sítí 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.

Nezávislé sítí

Nezávislé síti nebo *independent BSS* (IBSS), jsou to sítí kde stanice komunikují přímo mezi sebou bez přístupového bodu. Nejmenší IBSS síť může být vytvořena



Obr. 1.2: Typy sítí 802.11

pomocí dvou stanic. Zpravidla tento typ sítí se 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 rozpuštěn. Vzhledem k jejich krátkému trvání a malé velikosti IBSS jsou někdy označovány jako Ad-hoc BSS nebo Ad-hoc sítě.[2]

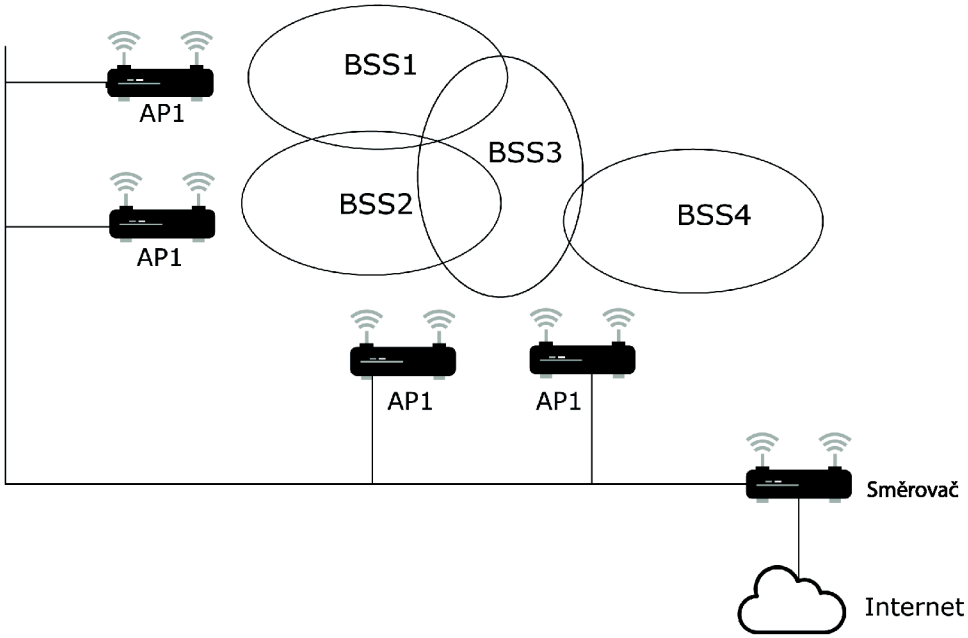
Infrastrukturní sítě

Infrastrukturní sítě nebo infrastructure BSS, jsou to šití jádrem kterých je přístupový bod. Pomocí přístupového bodu probíhá všechna komunikace uvnitř sítí, včetně komunikace mezi stanicemi.

V infrastrukturní sítí stanice musí být spojeny s přístupovým bodem, aby bylo možné získat síťové služby. *Association* je proces, kterým se mobilní stanice připojí k 802.11 sítí, tento proces není symetrický. Mobilní stanice vždy zahájí proces připojení a přístupové body se mohou rozhodnout udělit nebo zamítnout přístup na základě obsahu žádosti.[2]

Rozšířené oblasti služeb

Extended service areas (ESS) nebo rozšířené oblasti služeb, jsou to síti založené na principu spojení několika infrastrukturnich sítí do jedné velké sítě. Funguje to tak že každá z menších sítí je nakonfigurována stejně a všechny jsou připojené do jedné páteřní síti 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 jedenou MAC adresu pro komunikaci se stanicí někde v ESS. Na obrázku 1.3 je směrovač který používá jednou MAC adresu k doručování rámců do mobilní stanice. Přístupový bod s kterým je mobilní stanice přidružena, dodá rámec.[2]



Obr. 1.3: Rozšířené oblasti služeb

1.1.3 Jednotlivé standardy 802.11

Tato podkapitola popisuje jednotlivé standardy protokolu 802.11 a jejich rozdíly. Postupem času bylo vyvíjeno desítky různých standardů ale tady jsou popsané jenom nejčastěji používané.

802.11-1997

Původní standard protokolu, byl vyvíjen v roce 1997. On definoval dvě základní části protokolů které jsou platné i v dnešních, modernějších protokolech, a to jsou MAC vrstva a PHY vyrstva. PHY vyrstva měla dvě možnosti fugovani: 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. Taky on stanovil alternativní technologie modulací na fyzické vrstvě: DSSS a FHSS.[3]

802.11a

Tato verze používá stejný protokol vrstvy datového spojení a formát rámce jako původní standard ale vzdušné rozhraní založené na OFDM modulaci. Dalším rozdílem oproti původnímu standartu je pracování v pásmu 5 GHz s maximální datovou rychlostí 54 Mbps což v reálném životě dosahuje rychlost přibližně 20 Mbps. Vzhledem k tomu, že pásmo 2,4 GHz je do současnosti přeplněné, je použití relativně nevyužitého pásma 5 GHz významnou výhodou. Nevýhodou však je i tato vysoká nosná

frekvence: efektivní celkový rozsah 802.11a je nižší než 802.11b/g. Teoreticky jsou signály 802.11a vstřebávány snadněji stěnami a jinými pevnými předměty v jejich dráze kvůli jejich menší vlnové délce. V praxi má 802.11b obvykle vyšší rozsah při nízkých rychlostech. 802.11a také trpí rušením, ale na místě může být méně signálů, které by rušily, což má za následek menší rušení a lepší propustnost.[3]

802.11b

Standard 802.11b má maximální rychlost prenosudat 11 Mbps a používá stejnou metodu přístupu k médiím, jak je definována v původním standardu (DSSS). Dramatický nárůst propustnosti 802.11b (ve srovnání s původním standardem) spolu se současným podstatným snížením ceny vedl k rychlému přijetí 802.11b jako definitivní technologie bezdrátové LAN. 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.[3]

802.11g

802.11g funguje v pásmu 2,4 GHz (jako 802.11b), ale používá stejné přenosové schéma založené na OFDM jako 802.11a. Pracuje při maximální bitové rychlosti fyzické vrstvy 54 Mbps nebo průměrné propustností přibližně 22 Mbps. Hardware 802.11g je plně zpětně kompatibilní s hardwarem 802.11b, a proto je zatížen starými problémy, které snižují propustnost přibližně o 20% ve srovnání s 802.11a. Stejně jako 802.11b, i zařízení 802.11g také ruší jiné produkty pracující v pásmu 2,4 GHz, například bezdrátové klávesnice.[3]

802.11n

802.11n je dodatek, taky je označován jako Wi-Fi 4, který vylepšuje předchozí standardy 802.11 přidáním vícenásobných vstupních a vícenásobných výstupních antén (MIMO). S pomocí MIMO se provádí prostorové multiplexování: současný přenos několika informačních toků na jednom kanálu, jakož i použití vícecestného způsobu doručení signálu, což minimalizuje účinek rušení a ztráty dat, ale vyžaduje několik antén. Tato shopnost současně vysílat a přijímat data, zvyšuje propustnost zařízení 802.11n. Protokol pracuje v pásmech 2,4 GHz a 5 GHz. Podpora pásem 5 GHz je volitelná. Jeho čistá datová rychlost se pohybuje od 54 Mbps do 600 Mbps. IEEE tuto změnu schválila a byla zveřejněna v říjnu 2009.[3]

802.11ac

IEEE 802.11ac (Wi-Fi 5) je v podstatě vylepšení protokolu 802.11n. Změny oproti 802.11n zahrnují širší kanály (80 nebo 160 MHz versus 40 MHz) v pásmu 5 GHz, více prostorových toků (až osm versus čtyři), modulace vyššího řádu (až 256-QAM vs. 64-QAM) a přidání víceuživatelského MIMO (MU-MIMO). Od října 2013 podporují špičkové implementace kanály 80 MHz, tři prostorové toky a 256-QAM, což přináší datovou rychlost až 433,3 Mbps na prostorový proud, celkem 1300 Mbps, v 80 MHz kanálech pásma 5 GHz.[3]

802.11ad

IEEE 802.11ad je dodatek, 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. Produkty implementující standard 802.11ad jsou uváděny na trh pod značkou WiGig. IEEE 802.11ad je protokol používaný pro velmi vysoké přenosové rychlosti (asi 8 Gbps) a pro komunikaci na krátkou vzdálenost (asi 1–10 metrů).[3]

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 4x propustnost 802.11ac ve uživatelské vrstvě. V předchozím dodatku 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. Aby bylo k dispozici dostatečné množství pomocných nosných pro splnění požadavků OFDMA, počet pomocných nosných se zvyšuje o faktor 4 (ve srovnání se standardem 802.11ac).[3]

1.2 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 ob-

vykle vyskytují v protokolu WLAN. Poté jsou popsané standartizovane přístupové metody, distribuovaná koordinační funkce (DCF) a handshakem nebo bez a bodová koordinační funkce (PCF).

1.2.1 Vlastnosti vrstvy MAC

Skupina 802.11 stanovuje některé požadavky na protokol MAC. Tyto vlastnosti jsou shrnuty v této podkapitole, lze obecně považovat za funkce očekávané v jakékoli WLAN, nejen sítí IEEE 802.11

Propustnost

Protože spektrum je vzácným zdrojem, propustnost je rozhodně jedním z nejdůležitějších aspektů při navrhování protokolu MAC. Kapacita WLAN by se měla ideálně přiblížit kapacitě jejich kabelových protějšků. Vzhledem k fyzickým omezením a omezené dostupné šířce pásma jsou však WLAN v současné době zaměřeny na přenosové rychlosti 1-20 Mbps. Nejrozšířenější protokoly s náhodným přístupem patří do rodiny ALOHA, včetně vícenásobného přístupu (CSMA). Rodina ALOHA trpí problémy se stabilitou. To znamená, že špičkový výkon je doprovázen obrovským zpožděním. S Ethernetem a jeho fyzickým přenosem 10 Mbps a více než 80 procentou propustnosti pro CSMA/CD. je možné dodat více než 8 Mbps teoretického výkonu, ale v praxi měření ukazují, že je dosaženo výkonu pouze 3 až 3,5 Mbps. Měli bychom uvažovat nejen o teoretické propustnosti, ale také o provozní propustnosti (což je prakticky důležitější). Jedním ze způsobů, jak zvýšit propustnost, je použití technik rozprostřeného spektra, které podporují více přenosů současně.

Dalším důležitým hlediskem propustnosti je dopad neoprávněného přístupu k síti. Ani MAC ani funkce správy sítě nemohou identifikovat žádný neoprávněný přístup před přijetím jeho přenosu, takový přístup nevyhnutelně ovlivňuje propustnost a zpoždění sítě. Úspěšný systém zabezpečení MAC a sítě by měl takový neoprávněný přístup odmítnout a minimalizovat jeho dopad.[1]

Zpoždění

Charakteristiky zpoždění jsou důležité v každé aplikaci, ale zejména ve WLAN, protože by měly sloužit nejen povinné asynchronní datové službě, ale také časově omezeným multimediálním aplikacím, jako jsou hlas a video. Zpoždění může také způsobit problémy pro všechny datové služby, kde je zachování sekvence paketů nesmírně důležité.[1]

Průhlednost různých vrstev fyzického přenosu

Jedním ze zvláštních požadavků na WLAN MAC je průhlednost různých vrstev fyzického přenosu. U sítí IEEE 802.11 LAN zahrnují fyzické vrstvy přenosu přímé spektrum rozprostřeného spektra (DS-SS), frekvenčně skokové rozprostřené spektrum (FH-SS) a difúzní IR. Tyto fyzické přenosové vrstvy se liší nejen konstrukcí systému, ale také charakteristikami šíření. Jeden MAC však musí všechny zpracovat. Jedním ze způsobů, jak tohoto cíle dosáhnout, je mít fyzickou závislou vrstvu, fyzickou konvergenční vrstvu a odpovídající rozhraní MAC-PHY v každé stanici. Na základě architektury, která je v současné době přijímána komisí IEEE 802.11, si může jeden MAC vyměňovat data s různými PHY přes rozhraní MAC-PHY. S touto položkou je přímo spojeno omezení složitosti PHY (středně závislá vrstva, konvergenční vrstva PHY a rozhraní MAC-PHY) na minimum. Návrh sítě WLAN je integrovaný problém, od PHY po vrstvu správy sítě. Návrh MAC, který způsobuje potíže v jiných částech / vrstvách systému, je nežádoucí.[1]

Spravedlivost přístupu

Vlastnosti vyblednutí vnitřních kanálů mohou způsobit nerovnoměrný přijímaný výkon v základnové stanici, i když je vynuceno řízení výkonu. Taková situace může vést k nespravedlivému přístupu k síti. To znamená, že jeden mobilní uzel může přijímat mnohem méně energie v základnové stanici než jiný mobilní uzel. Pokud protokol MAC pracuje v konfliktním režimu (nezbytném pro počáteční registraci a často používaném pro uplinkový provoz), nemusí disadvanovaný mobilní uzel na chvíli mít přístup ke kanálu. Protokol MAC by měl být schopen tuto situaci vyřešit, protože je možné, že k zachycení může dojít s malým rozdílem výkonu 6 až 9 dB, zatímco dynamický rozsah vyblednutí může být stejně velký jako několik dB.[1]

Spotřeba energie baterie

Obvykle je elektrické napájení 110 V (nebo 220 V) dodávané v budově napájejícím zařízení připojené k kabelové síti. Bezdrátová zařízení však mají být přenosná a/nebo mobilní a obvykle jsou napájena z baterií. Z tohoto důvodu musí být zařízení navržena tak, aby byla velmi energeticky účinná a měla za následek „spánkové“ režimy a displeje s nízkou spotřebou, které uživatelům umožní komparace nákladů a výkonu a nákladů versus schopnost. Mnoho navržených protokolů vyšší úrovně vyžaduje, aby mobilní uzly neustále sledovaly přístupové body nebo handshake se základnovými stanicemi za účelem synchronizace, řízení ukazatele nebo výměny informací o stavu. Proto by měl být pro přenos paketů používán velmi omezený výkon. Režim spánku by měl být možný na přední straně přijímače. Aktivní přijímací režim může spotřebovat více energie baterie než provoz v režimu přenosu, protože moderní komerční

digitální komunikační systémy mohou mít obvykle přenosový výkon 100 mW, ale potřebují 100 mA proudu, aby podporovaly provoz procesoru digitálního signálu v přijímači.[1]

Maximální počet uzlů a maximální oblast pokrytí

Podle studií trhu musí síť WLAN podporovat stovky uzlů. MAC by proto neměl omezovat maximální počet uzlů, aby udržel uspokojivý výkon. Tato funkce neznamená, že máme neomezenou oblast pokrytí, která je omezena zpožděním.

Typická oblast pokrytí pro WLAN se pohybuje od $10m^2$ do $100m^2$, což způsobuje zpoždění šíření menší než 1 000 ns. Zpoždění v rozsahu 500-1 000 ns může způsobit některé problémy pro některé MAC: například synchronní systém CDMA. Tuto vlastnost můžeme shrnout jako schopnost pracovat v širokém spektru systémů s návrhem MAC, který dokáže zpracovat geografickou velikost a počet uzlů v LAN.[1]

Robustnost vs. přístup a interferenční kanál

Velkou výzvou při navrhování sítě WLAN MAC je úspěšná práce v případě sítí umístěných v koloně, což může způsobit vážné rušení pomocí *co channelu*. Je docela pravděpodobné, že dva nebo více WLAN bude fungovat ve stejné oblasti nebo v některých oblastech, kde může docházet k rušení mezi různými LAN. Některé protokoly nemohou v této situaci fungovat normálně. Zvažte například dva WLAN pracující ve dvou okolních budovách. Pro některé části těchto sítí LAN může být obtížnější komunikovat s jinými částmi jejich vlastní sítě LAN než s ostatními sítěmi LAN. Z této situace mohou vyplynout vážné potíže, pokud MAC používá předávání tokenů. Je možné chybně předat token uzlu v jiné síti.

Obvykle existují dvě obavy, které jsou popsány takto:

Z pohledu zabezpečení: Ostatní uživatelé se mohou nelegálně do sítě vloupat a způsobit tak bezpečnostní upozornění. To lze vyřešit vhodným ověřovacím postupem pro nové uživatele.

Z pohledu rušení z jiných sítí: Například pokud v WLANs použijeme tradiční protokoly CSMA, rušení z jiné sítě může způsobit katastrofální problémy se skrytými uzly.

Tyto dvě obavy by měly být řešeny hlouběji. Rušení bezdrátové komunikace může být způsobeno současnými přenosy (tj. Kolizemi) dvěma nebo více zdroji sdílejícími stejné frekvenční pásmo. Srážky jsou obvykle výsledkem několika stanic, které čekají na nečinnost kanálu a poté začnou vysílat současně. Kolize jsou také způsobeny problémem „skrytého uzlu“, kdy stanice, která věří, že kanál je nečinný, začne vysílání, aniž by úspěšně detekovala přítomnost již probíhajícího přenosu. Tento problém je

podrobněji popsán v kapitole 1.2.3 . Rušení je také způsobeno vícestupňovým vyblednutím, které je charakterizováno náhodnými amplitudami a fázovými fluktuacemi v přijímači. Spolehlivost komunikačního kanálu je obvykle měřena průměrným BER. Pro paketizovaný hlas jsou obecně přijatelné míry ztráty paketů řádově $10^{-}1$; pro nekódovaná data je BER $10^{-}5$ považována za přijatelnou. Ke zvýšení spolehlivosti se používá automatický požadavek na opakování (ARQ) a dopředná korekce chyb (FEC).

Dalším důležitým aspektem jsou kolize v ESS (Extended service areas). Pokrytí každé buňky by mělo správně překrývat sousední buňky, to znamená, že se překrývající se oblast má minimalizovat, aby se zvýšila kapacita systému, ale také se udržuje v určité míře, takže je možné hladké plnění. Tato společná oblast mezi buňkami přináší další problémy. Tyto problémy jsou shrnuty následovně:

Vlastní rušení: Když se dva AP (například dva opakovače) pokusí vyslat paket do uzlu ve společné oblasti současně To způsobí rušení a paket bude pravděpodobně ztracen.

Vlastní kolize: Uzel ve společné oblasti vysílá paket, který přijímá více než jeden přístupový bod. To způsobuje kolizi nebo plýtvání šířkou pásma při směrování tohoto paketu na místo určení.

Up-down kolize: Uzel (A) v jedné buňce vysílá uplink, zatímco jiný uzel (B) v jiné buňce přijímá downlink. Je možné, že uzel B bude schopen slyšet (přijímat) přenos uzlů A a tato situace povede ke kolizi, pokud nebudeme moci dokonale naplánovat všechna vysílání. Naštěstí tato situace, která je podobná skrytému terminálovému problému a je problémem dosud nevyřešeným v multibuňkové infrastruktuře LANS, je velmi nepravděpodobná, pokud jsou buňky dobře odděleny. Vzhledem k tomu, že kolize dolů jsou velmi destruktivní, měl by to jakýkoli MAC vzít v úvahu pečlivě.

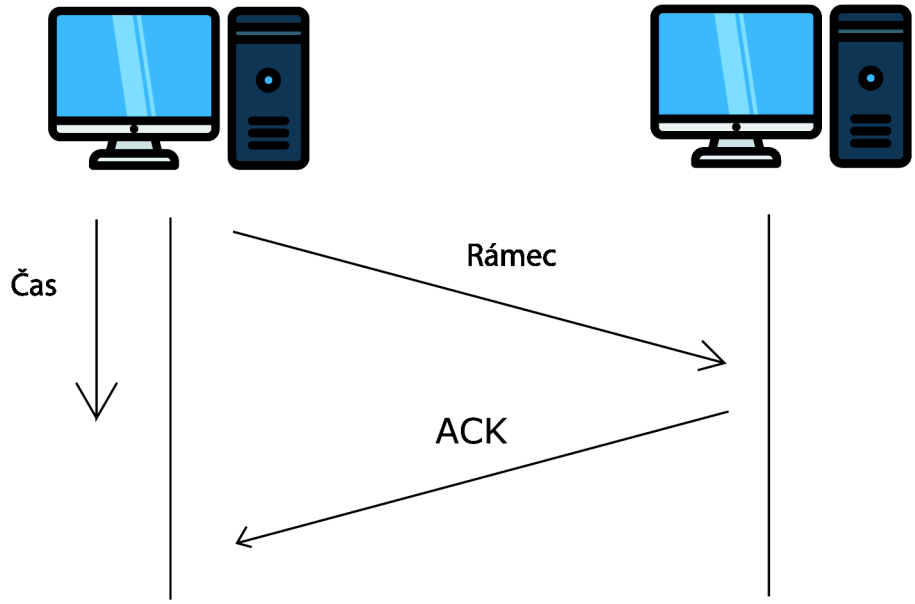
Dalším problémem je bezpečnost. Ve drátové síti může být přenosové médium fyzicky zabezpečeno a přístup k síti je snadno řízen. Zabezpečení bezdrátové sítě je obtížnější, protože přenosové médium je otevřeno komukoli v geografickém dosahu vysílače. Ochrana osobních údajů se obvykle provádí v rádiovém médiu pomocí šifrování. I když lze dosáhnout šifrování bezdrátového provozu, je to obvykle na úkor zvýšených nákladů a sníženého výkonu MAC.[1]

Navázání peer-to-peer konektivity

Při navázání připojení typu peer-to-peer bez předchozího vědomí MAC sítě WLAN by měl podporovat síť ad hoc. Proto by nemělo být vyžadováno apriorní informace o topologii sítě (např. Zda existuje komunikace mezi všemi uzly).

1.2.2 Kvalita rádiového přenosu

Na kabelovém Ethernetu po vyslání rámece se předpokládá to, že cíl přijímá ho správně, oproti tomu u rádiového spojení je jiná situace, hlavně z důvodu rušení nemůžeme předpokládat bezproblémové doručení do cíle, zejména pokud jsou použité nelicencované 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 toho. 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.



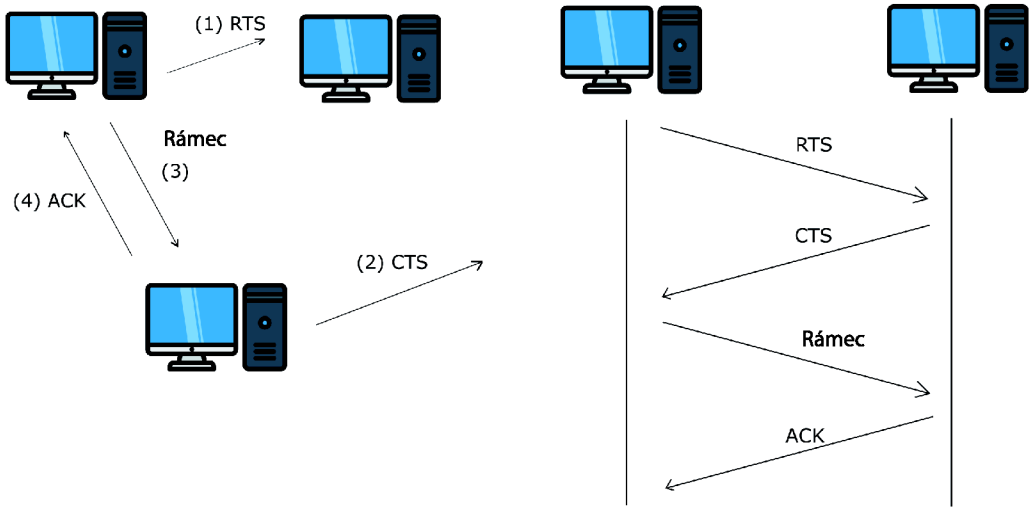
Obr. 1.4: Kontrola doručení zprávy

Z toho důvodu na rozdíl od mnoha jiných protokolů, na linkové vrstvě 802.11 byl zaváděn mechanizmus pro kontrolu doručení zprávy. Po té co stanice vyslala rámec, ona nějakou dobu čeká na potvrzující odpověď ACK, a až potom začne vysílat další rámec. Tento potvrzovací mechanizmus je znázorněn na obrázku 1.4. Pokud některá část přenosu selže, rámec je považován za ztracený.

1.2.3 Problém skrytecho uzlů

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 rozhodou začít vysílat svůj rámec. V tuto chvíli nastává kolize kterou pomáhá vyřešit mechanizmus RTS/CTS.



Obr. 1.5: 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 3-3 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 probihajivi přenos, tak pošle CTS zprávu a tím podvtrdi že může přijímat zprávu. Následně odesílatel pošle rámec a čeká na zprávu povrzujici úspěšný příjem (ACK). Poté když ACK byl přijat, spojení se ukončí.[2]

1.2.4 Struktura rámce 802.11

Rámec protokolu 802.11 na MAC vrstvě obsahuje 9 položek.

Frame Control – je dvou bajtová buňka která definuje typ rámce a taky obsahuje nějakou doplňující informace jako naproklad version, subtype, To/From DS a další.

Duraction/ID – je to pole délkou 4 bajty, které obsahuje hodnotu určující dobu pro kterou bude médium obsazeno (v µs).

Address 1 - 4 – jsou to 4 polí o 6 bajtů každý, které obsahují standardní MAC adresy IEEE 802. Význam každé adresy závisí na DS bitech v kontrolním poli rámce.

SC (Sequence control) – Je pole délkou 16 bitů, které je rozděleno na dvě části: Sequence number (12 bitů) a Fragment number (4 bity). Protože rámce potvrzovacího mechanismu mohou být duplikovány, používá se pro filtrování duplicitních rámců pořadové číslo.

Data – Jedná se o pole s proměnnou délkou, které obsahuje informace specifické pro jednotlivé rámce, které se transparentně přenášejí z odesílatele do přijímače.

CRC (Cyclic redundancy check) – Pole o 4 bajty, které obsahuje 32 bitovou sekvenci detekce chyb CRC k zajištění bezchybného rámce.

1.3 Fyzická vrstva 802.11

Druhou hlavní součástí architektury 802.11 je fyzická vrstva, která je často zkrácena PHY. V rámci definice fyzické vrstvy IEEE 802.11 existují dvě specifikace pro rádiové systémy: fyzická vrstva FH-SS a fyzická vrstva DS-SS. Oba 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, provozovatelé vysílání a vládní agentury), ale nelze jej účinně použít, pokud by počet potenciálních uživatelů konkrétní aplikace mohl být miliony. To neplatí pouze pro WLAN, ale také pro jiné aplikace, jako je všudypřítomný otvírač garážových vrat.[3]

1.3.1 Techniky rozprostřeného spektra (SS)

Systémy rozprostřeného spektra využívají větší šířku pásma, než je potřeba pro přenos. Pro určení, kolik šířky pásma je zapotřebí pro přenos, je nutné zvážit formát modulace. Mnoho lidí by souhlasilo s tím, že by systém mohl být považován za rozšířené spektrum, pokud by byla obsazená šířka pásma záměrně zvýšena, než je potřeba, vzhledem k bitové rychlosti a formátu modulace. Pokud systém používá zhruba potřebnou šířku pásma, nejedná se o systém s rozšířeným spektrem a měl by být považován za úzkopásmový. (Úzkopásmové připojení bude v tomto kontextu použito jako opak rozprostřeného spektra.)

Pro dosažení větší šířky pásma používají systémy s rozprostřeným spektrem kód ve vysílači, nezávislý na datech, před modulací, který 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.[3]

1.3.2 Typy rozprostřeného spektra

Fyzické vrstvy založené na rádiu v 802.11 používají tři různé techniky rozprostřeného spektra:

1) Frekvenční skok (FH nebo FHSS)

Systémy s frekvenčním skokem náhodně přecházejí z jedné frekvence na druhou.

2) Přímá sekvence (DS nebo DSSS)

Systémy s přímým sledováním šíří energii pomocí širšího frekvenčního pásma matematické kódovací funkce.

3) Ortogonální multiplexování s frekvenčním dělením (OFDM)

OFDM dělí dostupný kanál na několik subkanálů a kóduje a část signálu paralelně přes každý subkanál. Technika je podobná na techniku Diskrétní více tónů (DMT) používanou některými modemy DSL.[3]

1.3.3 Frekvenční skok

FH (frequency hopping) systémy používají konvenční modulační techniky, ale nosná frekvence se mění danou rychlostí, sledující danou sekvenci. Tato posloupnost je kódem těchto systémů. Přijímač, který nezná kód, nemůže sledovat frekvenční skoky a může detekovat pouze občas některá data. Pokud je přeskakovací rychlost rychlejší než bitová rychlost, systém je rychlý FH (FFH). Pokud je přeskakovací rychlost pomalejší než bitová rychlost, je systém pomalý FH (SFH). Komerční systémy jsou vždy SFH kvůli složitosti systémů FFH.

V systému SFH je bitový tok rozdělen do paketů, z nichž každý je vysílán v dávce s jinou nosnou frekvencí. V rámci dané dávky je přenos úzkopásmový, používá pouze šířku pásma potřebnou podle bitové rychlosti a formátu modulace. Bez ohledu na momentální problém s generováním kmitočtu ve vysílači a přijímači a jejich synchronizací je zřejmé, že neexistují základní rozdíly ve výkonu v hlučných prostředích ve srovnání s úzkopásmovými systémy. Ve skutečnosti je přenos sám o sobě úzkopásmovým.

V prostředí existují dva typy rušení, které jsou popsány takto:

1) Pokud existuje úzkopásmový rušivý vysílač, rušení ovlivní pouze ty impulzy, jejichž nosič se shoduje s nosičem druhého vysílače. Na druhé straně rušení s jinými úzkopásmovými systémy je zmírněno skutečností, že přenos ne vždy zabírá stejnou šířku pásma. K rušení dochází pouze občas.

2) Pokud dva systémy FH pracující ve stejném pásmu mají překrývající se oblasti pokrytí, dojde k rušení pokaždé, když se záblesky obou systémů shodují ve stejném nosiči.

V důsledku toho tyto systémy obvykle předpokládají, že některé shluky jsou přijímány s velmi nízkou kvalitou (vysoká BER) nebo jsou zcela ztraceny kvůli poruchám šíření nebo kvůli silnému rušivému signálu. Ovlivňuje to však jen malé procento přenosu a lze jej obnovit buď kódováním chyb dopředu, nebo opakovaným přenosem. Systémy FH jsou obvykle považovány za fungující na základě vyhovění. Některé dávky jsou přijaty dokonale a jiné jsou ztraceny.[3]

1.3.4 Přímé sekvenční systémy

V systémech DS (direct sequence systems) je záměrně zvýšena modulační rychlost, aby se rozšířilo spektrum. Toho je dosaženo kombinací bitové sekvence s vyšší rychlostí binární sekvence (nazývané čipová sekvence) k získání nové sekvence s čipovou rychlostí. Ten se pak používá k modulaci nosiče. Inverzní operace se provádí na straně přijímače. Signál je demodulován a potom je rekombinován se stejnou čipovou sekvencí pro obnovení původních dat. Ačkoli to jsou základní myšlenky konceptu systémů DS, praktické implementace vyžadují další úvahy o druhu použitých čipových sekvencí, způsoby, jak je kombinovat s datovou sekvencí, použité modulační formáty, techniky demodulace signálu, problémy s synchronizací a obnovovače dat. Výhody těchto systémů ve srovnání s úzkopásmovými systémy jsou popsány takto:

1) Spektrální hustota výkonu, měřená ve výkonu na jednotku šířky pásma, je mnohem nižší kvůli větší šířce pásma, po které je výkon rozložen. To má vliv na nízkou pravděpodobnost zachycení a nižší kapacitu rušení s jinými systémy.

2) Pro obnovení dat musí příjemce znát sekvenci čipu a provést operaci kombinování přijaté sekvence se sekvencí čipu. To zvyšuje soukromí komunikace, protože

každý nevítaný posluchač by nebyl schopen obnovit bitovou sekvenci, pokud je čipová sekvence udržována v soukromí.

3) V přijímači operace spojující signál se sekvencí čipu obnoví data na jejich původní bitovou rychlost, která je mnohem menší než rychlost čipu. V důsledku toho se zmenší šířka pásma signálu a komponenty ležící mimo tuto malou šířku pásma mohou být odfiltrovány. Protože všechny ostatní signály, včetně šumu a rušení jakéhokoli druhu, budou mít po kombinaci s čipovou sekvencí velkou šířku pásma, bude většina jejich výkonu filtrována. Důležité je, že úzkopásmové rušení by se šířilo po celém pásmu po kombinaci s čipovou sekvencí. Přijímače DS tedy představují určitý stupeň potlačení šumu a rušení.

4) Několik komunikací může sdílet stejné spektrum s přímou sekvenční komunikací, pokud používají nekorelovanou čipovou sekvenci. Toto je základ CDMA, systému s vícenásobným přístupem, ve kterém je každému uživateli přidělen rozprostírací kód, takže nemůže vzájemně ovlivňovat, nebo může být vzájemné rušení udržováno na kontrolovaných nízkých úrovních.

Ne všechny tyto výhody se používají ve standardu 802.11. Zejména se nejedná o systém CDMA. Metoda DS nehraje roli ve vlastnostech ochrany osobních údajů, protože sekvence čipů je veřejná a kauzální pro všechny uživatele. Hlavním důvodem pro výběr této metody přenosu je její schopnost sdílet spektrum s jinými systémy při nízkých úrovních vzájemného rušení.[3]

1.3.5 OFDM

Je metoda kódování digitálních dat na více nosných frekvencích. OFDM se vyvinul v populární schéma pro širokopásmovou digitální komunikaci, které se používá v aplikacích, jako je digitální televizní a zvukové vysílání, přístup k internetu DSL, bezdrátové sítě, sítě elektrického vedení a mobilní komunikace 4G.

V kódovaném ortogonálním multiplexování s frekvenčním dělením (COFDM) se na vysílaný signál aplikují korekce dopředné chyby (konvoluční kódování) a časové / frekvenční prokládání. To se provádí za účelem překonání chyb v mobilních komunikačních kanálech ovlivněných množením cest a Dopplerovými efekty.

OFDM je schéma multiplexování s kmitočtovým dělením (FDM), které se používá jako metoda modulace digitální více nosičů. K přenosu dat je vysíláno mnoho úzce rozmístěných ortogonálních subnosných signálů s překrývajícími se spektry. Demodulace je založena na algoritmech rychlé Fourierovy transformace. Každá pomocná nosná (signál) je modulována konvenčním modulačním schématem (jako je kvadraturní amplitudová modulace nebo klíčování fázovým posunem) při nízké symbolové rychlosti. To udržuje celkové datové rychlosti podobné konvenčním schématům modulace s jednou nosnou ve stejné šířce pásma.

Hlavní výhodou OFDM oproti schématům s jednou nosnou je jeho schopnost vyrovnat se s vážnými podmínkami kanálu (například útlum vysokých frekvencí v dlouhém měděném drátu, úzkopásmové rušení a frekvenčně selektivní vyblednutí v důsledku vícenásobných cest) bez složitých vyrovnávacích filtrů. Vyrovnávání kanálů je zjednodušeno, protože OFDM lze považovat za použití mnoha pomalu modulovaných úzkopásmových signálů spíše než jednoho rychle modulovaného širokopásmového signálu. Nízká rychlost symbolů umožňuje použití ochranného intervalu mezi symboly cenově dostupným, což umožňuje eliminovat intersymbolovou interferenci (ISI) a používat ozvěny a časové rozpětí (v analogové televizi viditelné jako přízraky a rozmazání) pro dosažení zisku rozmanitosti, tj. zlepšení poměru signál-šum. Tento mechanismus také usnadňuje navrhování jednofrekvenčních sítí (SFN), kde několik sousedních vysílačů vysílá stejný signál současně na stejné frekvenci, protože signály z více vzdálených vysílačů mohou být konstruktivně znovu kombinovány, čímž se šetří rušení tradičního systému s jedním nosičem.[3]

2 Bezpečnost 802.11

V dnešní společnosti jsou informace pro náš život stále důležitější, od věcí jednotlivců až po národní bezpečnost. Stejně jako technologie pokračuje v pokroku, zařízení směřují k mobilním a bezdrátovým připojením mimořádně. Tato nová éra technologické flexibility může také nabídnout otevřenou výzvu k ohrožení bezpečnosti sítě nejen v podnikovém světě, ale také v soukromí uživatelů doma. Naše schopnost zůstat stejně informovaná a ostražitá, jak se objevují novější technologie, bude mít významný dopad na to, jak navrhujeme a plánujeme strategii obrany sítě proti neautorizovaným narušením budoucnosti.

Tato kapitola se věnuje bezpečnostní stránce protokolu 802.11.

2.0.1 Obecný pohled na bezpečnost Wi-Fi

Parametry bezdrátové sítě, zejména její název (SSID), jsou pravidelně oznamovány přístupovým bodem v paketech vysílacího majáku. Kromě očekávaného nastavení zabezpečení jsou přenášena přání kvality služeb (QoS), parametry 802.11x, podporované rychlosti, informace o ostatních sousedech atd. Ověření určuje, jak je klient prezentován v daném bodě. Možné možnosti: otevřená tzv. Otevřená síť, ve které jsou všechna připojená zařízení okamžitě autorizována; sdílená autentičnost připojeného zařízení musí být ověřena pomocí klíče / hesla; EAP (Extensible Authentication Protocol) - autentičnost připojeného zařízení musí být ověřena pomocí EAP s externím serverem.

Otevřenost sítě neznamená, že s ní může někdo pracovat beztrestně. Pro přenos dat v takové síti je nutné použít použitý šifrovací algoritmus a odpovídajícím způsobem správně navázat šifrované spojení. Šifrovací algoritmy jsou následující:

Žádné - žádné šifrování, data jsou přenášena v čistém textu;

The Wired Equivalent Privacy (WEP) - je šifra založená na algoritmu RC4 s různými délkami statického nebo dynamického klíče (64 nebo 128 bitů);

CKIP - patentovaná náhrada WEP od společnosti Cisco, dřívější verze protokolu Temporal Key Integrity Protocol (TKIP);

TKIP - vylepšená náhrada WEP s dalšími kontrolami a ochranou;

AES / CCMP - je nejpokročilejší algoritmus založený na pokročilém šifrovacím standardu (AES256) s dalšími kontrolami a ochranou.

Kombinace Open Authentication, No Encryption je široce používána v systémech pro přístup hostů, jako je poskytování Internetu v kavárně nebo hotelu. Chcete-li se připojit, musíte znát pouze název bezdrátové sítě. Toto spojení je často kombinováno s dodatečnou kontrolou na Portálu Captive Portal přesměrováním požadavku HTTP

uživatele na další stránku, kde můžete požádat o potvrzení (přihlašovací heslo, dohoda s pravidly atd.). Šifrování WEP je ohroženo a nelze jej použít (ani v případě dynamických klíčů). Pojmy WPA a WPA2, které se často vyskytují, ve skutečnosti určují šifrovací algoritmus (TKIP nebo AES). Vzhledem k tomu, že klientské adaptéry již nějakou dobu podporují WPA2 (AES), nemá smysl používat šifrování pomocí algoritmu TKIP.[4]

2.0.2 WEP

Na začátku se věřilo, že „The Wired Equivalent Privacy“ (WEP) nabízí neproniknutelnou odolnost proti odposlouchávání / hackerům. S rostoucí popularitou bezdrátových sítí však mnoho analytiků a vědců z krypty objevilo nedostatky v původním designu WEP. Mnozí se domnívají, že v protokolu WEP bylo provedeno jen malé vzájemné hodnocení. Mnoho nedostatků WEP by bylo zachyceno v počáteční fázi návrhu, pokud by specifikace návrhu a implementace byly důkladně přezkoumány. Pro většinu uživatelů bezdrátových sítí (zejména domácích uživatelů). WEP je jedinou dostupnou volbou, dokud nebudou do standardu IEEE 802.11 přidány nové bezpečnostní mechanismy. Ale jak lidé říkají „něco je lepší než nic“, i když je známo slabé místo, WEP je stále účinnější než vůbec žádné zabezpečení, alespoň poskytne určitou bezpečnost proti neoprávněnému použití vlastní bezdrátové sítě a pohlcení šířky pásma.

WEP bylo navrženo tak, aby poskytovalo zabezpečení kabelové LAN šifrováním pomocí algoritmu RC4 se dvěma stranami datové komunikace.

Standard obsahuje dvě části pro zabezpečení WEP. První je fáze autentizace a druhá fáze šifrování. Myšlenka jde zhruba takto: Když se nové mobilní zařízení chce připojit k přístupovému bodu, musí nejprve prokázat svou totožnost. V ideálním případě by mobilní zařízení také chtělo, aby se přístupový bod také osvědčil. Tato fáze se označuje jako autentizace navzájem.[7]

WEP Autentizace

Zabezpečení WEP zahrnuje dvě části, autentizaci a šifrování. Ověřování v WEP zahrnuje ověření zařízení při prvním připojení k síti LAN. 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 bezdrátovému přístupovému bodu, poté bezdrátový přístupový bod odešle 128bitovou náhodnou výzvu ve formě prostého textu klientovi, který požaduje. Bezdrátové zařízení používá sdílený tajný klíč k podepsání výzvy a odešle ji bezdrátovému přístupovému bodu. Bezdrátový 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.[7]

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).

WEP používá CRC pro integritu dat. 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. IV + Ciphertext a záhlaví rámců jsou poté přenášeny vzduchem na základě tajného klíče a IV.[7]

WEP Zranitelnosti

Implementace mechanismů IV v WEP učinila protokol zranitelným, protože zesílila encrypci. IEEE 802.11 neurčuje, jak generovat IV. Účelem IV v algoritmu RC4 je zajistit, aby se klíče neopakovaly. Ale v WEP není jasné vedení, jak zvolit IV, mělo by být vybráno náhodně? Nebo by měl být spuštěn nulou a zvýšen o 1? WEP, používá buď 40 nebo 104 bitovou ochranu s 24 bitovým IV. Celý 24 bitový IV prostor lze spotřebovat během několika hodin a IV se opakují znovu. Když je sdílený klíč pevný, klíč k generátoru klíčového proudu RC4 se opakuje, pokud se opakují IV. Tím se porušuje pravidlo RC4, že klíče nikdy nebudou opakovány. Jak je IV zasíláno čistým textem, útočník může identifikovat, kdy dojde ke IV kolizi. IV kolize pomáhají útočníkovi určit klíčový proud. Analýzou dvou paketů odvozených od stejného IV lze získat keystream.

Předpokládejme, že plaintexty jsou Pl a P2, klíčové toky KI a K2 a výsledné šifrové texty jsou C1 a C2. Předpokládejme, že útočník vybere dva pakety odvozené od stejného IV a pokud zná jeden prostý text, může získat další neznámý prostý text.

$$C1\ XOR\ C2 = P1\ XOR\ P2$$

Je-li známo Pl nebo P2, lze pomocí výše uvedené rovnice odvodit další neznámý prostý text. Opakování klíče nebo IV je hlavní vadou při navrhování / implementaci WEP Jakmile je znám tok klíčů, může být nový ciphertext být vytvořen XORem nového prostého textu a známého proudu klíčů.

Standard IEEE 802.11 nevyžaduje změnu IV s každým paketem, stejný IV lze použít s každým paketem. Šifrovací zprávy útočníka lze poslat do sítě provedením výše uvedené operace. Přístupový bod nebo bezdrátové zařízení nemůže rozlišovat mezi pakety útočníka a skutečnými původními pakety.

Stejný klíč je sdílen mezi přístupovým bodem a bezdrátovým zařízením. Pokud stejný klíč používá více uživatelů / zařízení, pomůže to, aby útoky na WEP byly praktičtější a zvýšila se šance na IV kolizi. Změna klíče v přístupovém bodu vyžaduje, aby každý uživatel odpovídajícím způsobem změnil svůj klíč. Správa klíčů je tedy obtížné provádět ručně. Většina uživatelů proto často nemění klíče přístupového bodu. Udržují stejný klíč po mnoho měsíců nebo let nebo navždy. Tím si útočník koupí více času na analýzu provozu a identifikaci opětovného použití klíčového proudu a IV.

Ve WEP je integrita dat ověřována pomocí operace kontrolního součtu CRC. Záměrem CRC je zabránit tomu, aby někdo manipuloval s přepravovanou zprávou. CRC se provádí na prostém textu, ale ne na šifrovém textu. CRC byl navržen tak, aby detekoval náhodné chyby ve zprávě, ale nezabránil škodlivým útokům. Je možné provést změny v šifru bez ovlivnění kontrolního součtu. To ukazuje, že kontrolní součet WEP nedokázal chránit integritu dat (jeden z hlavních cílů WEP). Pokud útočník zná prostý text, může snadno spočítat kontrolní součet a vložit padělané zprávy do sítě. Útočník může také změnit cílovou adresu paketu a nahradit starý CRC modifikovaným CRC a také přepočítat kontrolní součet IP. Přístupový bod si nebude moci všimnout změn v původním paketu a předat je na vybranou IP adresu.

Fluhrer, Mantin a Shamir objevili chybu v algoritmu plánování klíčů WEP. Hlavní funkcí RC4 je pseudonáhodné generování. RC4 pracuje nastavením 256 bajtového pole obsahujícího 0 až 255 hodnot. Každá hodnota v poli se zobrazí pouze jednou. Pořadí hodnot může být randomizováno, známé jako permutace. Takže pokaždé dojde k jiné permutaci pole. Existuje tedy mnoho permutací, tj. $512 * 256!$ možnosti. Tato vlastnost posiluje implementaci RC4. Ve WEP je tajný sdílený klíč zřetězený s viditelnou hodnotou IV. Tato slabost se nazývá „slabost IV“. Tato metoda byla použita k obnovení původního klíče v reálných sítích WEP. Mnoho lidí napsalo a publikovalo software, který přeruší WEP tím, že zachytí síťový provoz, aby viděl opakované IV a používal výše uvedené metody.

Protokol WEP poskytuje určitou úroveň zabezpečení bezdrátové komunikace

mezi bezdrátovým přístupovým bodem a bezdrátovými zařízeními. Má však mnoho slabostí kvůli malému IV prostoru a špatnému výběru CRC32 pro ověření integrity dat. Místo toho, abychom se spoléhali pouze na zabezpečení WEP, je třeba přijmout další opatření k zajištění lepší bezpečnosti mezi bezdrátovými zařízeními.[5]

2.0.3 WPA

Dodatek 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 zlomený. 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 starými zařízeními podporujícími 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. To pomáhá při detekci paketů.[8]

WPA Personal a Enterprise

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

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 a klíč kryptografie dat, mohou dosáhnout až 256 bitů. Na rozdíl od WEP to může být libovolný alfanumerický řetězec a používá se pouze k vyjednávání počáteční relace s přístupovým bodem. Protože klient i přístupový bod již tento klíč vlastní, poskytuje WPA vzájemnou autentizaci a klíč není nikdy přenášen vzduchem.

2) Enterprise WPA nebo Commercial, autentizaci provádí autentizační server 802.1x, který generuje vynikající kontrolu a zabezpečení v provozu uživatelů bezdrátové sítě. Tato WPA používá pro autentizaci 802.1X + EAP, ale znovu nahrazuje WEP pokročilejším šifrováním TKIP. Zde se nepoužívá žádný sdílený klíč, ale budete potřebovat server RADIUS. A získáte všechny další výhody, které poskytuje 802.1X + EAP, včetně integrace s přihlašovacím procesem Windows a podpory metod autentizace EAP-TLS a PEAP.

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

Jak vidíte, 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 (smíšená) pomocí základního klíče.

Po provedení hašování vygeneruje výsledek klíč k balíčku, který se chystá spojit s první kopií inicializačního vektoru a dochází k přírůstku algoritmu RC4. Poté dojde k vygenerování sekvenčního klíče s XOR z textu, který chcete kryptografovat, a pak vygenerováním kryptografického textu. Nakonec je zpráva připravena k odeslání. Šifrování a dešifrování bude provedeno invertováním procesu.[8]

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 IV sekvenční disciplína, 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.[9]

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 nonces (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 nonce. 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. Vysvětluje, že 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.[9]

2.0.4 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 nejdéle 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 (odpálení zaměstnance, 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.[6]

WPA2-PSK: klient komunikuje s přístupovým bodem, autentizuje se s přístupovým bodem pomocí předem sdíleného klíče (PSK), pak přístupový bod vytvoří z PSK 256bitový párový hlavní klíč (PMK) a identifikátor SSID. Tento PMK 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 hackne PMK, může dešifrovat všechna data šifrovaná tímto PMK (minulá, současná i budoucí).

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 hackne konkrétní PMK, získá přístup pouze k jedné relaci na klienta.

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.

EAP-TLS (Transport Layer Security). Používá infrastrukturu veřejného klíče (PKI) k autorizaci klienta a serveru (příjemce a server RADIUS) 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).

EAP-TTLS (Tunneled Transport Layer Security) je 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).

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.

PEAP-GTC (Generic Token Card) - podobná předchozí, ale vyžaduje jednorázové karty hesel (a odpovídající infrastrukturu).

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 můžeme vytvořit falešný Wi-Fi bod se serverem RADIUS a získat přihlašovací údaje, požadavky a odpovědi, které MS-CHAPv2 používá. To je dost pro další hrubou sílu hesla.

Přijaté účty mohou být použity k dalšímu proniknutí do podnikové sítě přes Wi-Fi nebo VPN a také k získání přístupu k podnikové poště.

Jak se ukázalo, nemůžete vždy zachytit hashe uživatele. Desktop OS (Windows, MacOS, Linux) a uživatelé systému iOS jsou nejlépe chráněni. Při prvním připojení se operační systém zeptá, zda důvěřujete certifikátu používanému serverem RADIUS v této síti Wi-Fi. Pokud nahradíte legitimní přístupový bod, operační systém požádá o důvěru v nový certifikát, který používá server RADIUS. To se stane, i když používáte certifikát vydaný důvěryhodnou certifikační autoritou.

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 vyhotoveny 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 vetřelcům 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.).

Nedávno byla oznámena nová funkce Wi-Fi Finder pro uživatele zařízení se systémem Android. Pomáhá posoudit zabezpečení Wi-Fi sítí: soukromých i veřejných. Vyhledávač Avast Wi-Fi Finder dokáže nejen najít nejrychlejší a nejbezpečnější přístupové body, ale také určit připojená zařízení, posoudit zabezpečení routeru a zjistit zranitelnost připojených zařízení. Po připojení k domácí síti vám funkce Wi-Fi Finder pomůže vyřešit problémy se zabezpečením tím, že nabídne například spolehlivější heslo pro ochranu vaší sítě a souvisejících zařízení. Kromě toho vám tato funkce řekne o používání sítě neoprávněnými zařízeními, která ohrožují kybernetickou bezpečnost.[6]

2.0.5 Možnosti zachytávání Wi-Fi provozu

Tato kapitola se věnuje zachytávání prozovu v sítích založených na protokolu 802.11.

Snooping and Sniffing

Pokud si chcete přečíst webovou stránku, zařízení se připojí k webovému serveru a požádá o webovou stránku. To se provádí pomocí protokolu nazvaného HyperText Transfer Protocol (HTTP). Na otevřeném routeru Wi-Fi tyto požadavky a odpovědi vidí kdokoli, kdo poslouchá. S drátovým připojením k síti je pak poslouchání datových paketů rušivé. Díky bezdrátové síti jsou však všechna data odesílána vzduchem ve všech směrech, aby bylo možné přijímat jakékoli zařízení Wi-Fi.

Adaptér Wi-Fi je obvykle nastaven do „spravovaného“ režimu, což znamená, že funguje pouze jako klient a připojuje se k jedinému routeru Wi-Fi pro přístup k internetu. Některé adaptéry Wi-Fi však lze nastavit do jiných režimů. Například,režim „monitor“. V „spravovaném“ režimu síťové rozhraní Wi-Fi ignoruje všechny datové

pakety kromě těch, které jsou na něj konkrétně určeny. V režimu „monitor“ však adaptér Wi-Fi zachytí veškerý provoz bezdrátové sítě (na určitém kanálu Wi-Fi) bez ohledu na cíl. Ve skutečnosti v „monitorovacím“ režimu může Wi-Fi rozhraní zachytit pakety, aniž by bylo připojeno k jakémukoli přístupovému bodu (routeru), je to volný agent, sniffing a snooping všech dat ve vzduchu.

Ne všechny dostupné adaptéry Wi-Fi to dokážou, protože je levnější, aby výrobci vyráběli čipové sady Wi-Fi, které zpracovávají pouze „spravovaný“ režim, ale některé tam mohou být umístěny do „monitorovacího“ režimu .

Wi-Fi používá rádio a jako každé rádio, které musí být nastaveno na určitou frekvenci. Wi-Fi využívá 2,4 GHz a 5 GHz (v závislosti na použité variantě). Rozsah 2,4 GHz je rozdělen do několika „kanálů“, které jsou od sebe vzdáleny 5 MHz. Aby bylo možné získat dva kanály, které se vůbec nepřekrývají, musí být rozmístěny ve vzdálenosti přibližně 22 MHz (to však také závisí na tom, která varianta standardu Wi-Fi se používá). Proto jsou kanály 1, 6 a 11 nejčastějšími kanály, protože jsou dostatečně daleko od sebe, aby se nepřekrývaly.

Falešné HotSpot a Man-in-the-middle útok

Zachycení nešifrovaných paketů ze vzduchu není jediný způsob, jak může být veřejné Wi-Fi 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.

Co je 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.

3 Zachytávání rámců

Tato kapitola je soustředěna na praktické řešení problémů. Obsahuje popis použitých nástroje, 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. Používal jsem USB Wi-Fi TP-Link zařízení pro zachytávání provozu který byl připojen do počítače. Na počítači bylo spuštěno virtualizovane prostředí Kali Linux 2019 v programu VirtualBox. Zařízení od TP-Link podporuje protokoly 802.11b/g/n a pracuje na frekvenci 2,4 GHz. Dulezity faktor je taky chipset Ralink MT7601U který podporuje monitorovací režim síťového rozhraní.

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

V rámci operačního systému Kali použil jsem nainstalovaný nástroj Aircrack-ng. Tento nástroj je komplentim řešením pro bezpečnostní analýzu Wi-Fi sítí a obsahuje v sobě celou řadu funkcí. V této práce využil jsem také monitorovací balíčky od Aircrack-ng jako: airmon-ng pro naslouchání veškerého provozu a airodump-ng pro zachycení provozu určitě bezdrátové síti a uložení zachycených údajů do souboru pro následnou analýzu. Kromě toho pro analýzu zachyceného provozu napsal jsem program „Traffic Analyzer“ v programovacím jazyce Python. Podrobný popis programu je v následující podkapitole.

Pro simulace přístupového bodu byl vytvořen HotSpot na počítači ke kterému byl připojen mobil který fungoval jako legitimní uživatel.

3.1.2 Traffic Analyzer

Popis programu

Program je určen pro zachytávání a následnou analýzu naměřených dat Wi-Fi provozu. Traffic analyzer obsahuje celou řadu možností. Tak uživatel si 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 uživatel může si prohlídnout seznam MAC adres pripojinych uživatelů do určitého AP.

Program taky nabízí uživatelovi 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 konzole se zobrazuje výpis informací o zachyceném rámců. Pomocí pomocných tlačítek uživatel může zvolit jaký výpis chce. Pokud zvolí režim RAW tak se do konzoly 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.

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
```

QoS část rámce:

```
###[ 802.11 QoS ]###
    Reserved  = 0
    Ack_Policy= 0
    EOSP      = 0
    TID       = 0
    TXOP      = 0
```

IP část rámce:

```
###[ IP ]###
    version   = 4
    ihl       = 5
    tos       = 0x0
    len       = 60
```

```
id          = 403
flags       = DF
frag        = 0
ttl         = 64
proto       = udp
chksum      = 0x618f
src         = 192.168.43.1
dst         = 192.168.43.61
\options    \
```

Protokol:

```
###[ UDP ]###
     sport     = domain
     dport     = 14675
     len       = 40
     chksum    = 0x5194
```

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 jsou důležité logovani. Tak program nabízí uživatelovi 2 typy logovani. První je zápis výpisu konzoly do log souboru, výhodou takového logu je to že data do něho se 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 informace. Druhý typ je ukládání zachyceného provozu do pcap souboru. Výhodou tohoto typu logů je možnost dalšího zpracování.

Podporované typy rámců:

Data Frame - Většina datových rámců 802.11 obsahuje skutečná data, která jsou předávána z protokolů vyšší vrstvy. Užitečné zatížení vrstvy (payload) 3 - 7 MSDU je obvykle šifrováno z důvodu ochrany osobních údajů. Některé datové rámce 802.11 nenesou žádné užitečné zatížení MSDU, ale mají zvláštní účel řízení MAC v BSS. Jednoduchý datový rámec obsahuje informace o horní vrstvě MSDU zapouzdřené v těle rámce. Integrační služba, která sídlí v přístupových bodech a kontrolerech WLAN, vezme užitečnou zátěž MSDU jednoduchého datového rámce a převede MSDU do 802,3 ethernetových rámců. Klientské stanice někdy používají nulové funkční rámce k informování AP o změnách stavu úspory energie.

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). Informační pole jsou pole pevné délky v těle řídícího rámce. Informační prvky mají různou délku.

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 Other. Jednotlivý popis podtypu rámce a jeho význam je popsán v části analýzy.

Kromě typu rámce nástroj může specifikovat protokol. Program rozlišuje tři protokoly: TCP, UDP, ICMP. Pokud rámec obsahuje jiný protokol tak bude přidán do skupiny „Other“, pokud se nedá zjistit jeho protokol, rámec se zapíše do skupiny „Unknown“. Na konci programu se zobrazí uživatelovi výsledná statistika počtu jednotlivých rámců, jak číselně tak i procentně. Taky se zobrazí informace o počtu úspěšně nactencych rámců, celkový počet rámců a čas zpracování.

Vývoj

Nástroj je napsán v programovacím jazyce Python 3 a je postaven nad knihovnou Scapy. Scapy je výkonný interaktivní program pro manipulace s pakety. Je schopen falšovat nebo dekódovat pakety širokého počtu protokolů, posílat je na drát, zachytávat je, odpovídat požadavkům a odpovědím a mnohem více. Scapy snadno zvládne většinu klasických úkolů, jako je skenování, sledování, testování, testování jednotek, 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 v5. 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.

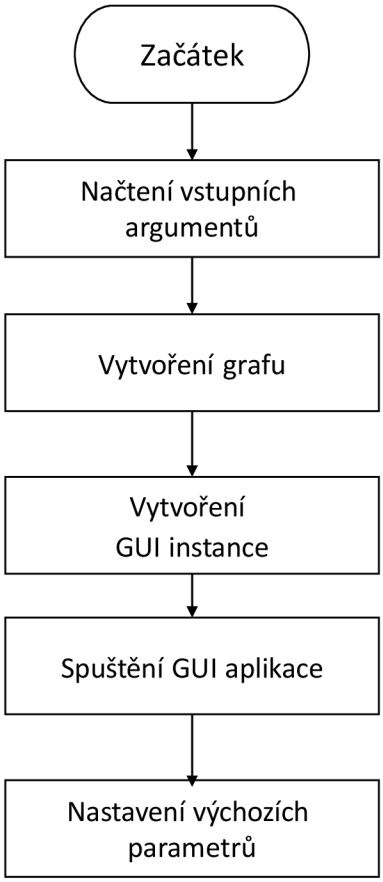
PyQt5 může být také zabudován do aplikací založených na C ++, aby umožnil uživatelům těchto aplikací konfigurovat nebo vylepšit funkčnost těchto aplikací.

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), navržený k blízce se podobat tomu to 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.

Proces spuštění programu



Obr. 3.1: Vývojový diagram procesů naběhnutí 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 a je to název bezdrátové síťové karty, pokud takový parametr není specifikován, program se ukončí s chybovým hlášením.

Dále se spustí process vytvoření instance grafu. Pro každý typ grafu je určena kontretni instance třídy `Figure`, z balíčku `matplotlib`. Po vytvoření instance, do objektu grafu se vkladaij takové výchozí nastavení a hodnoty jako: velikost plochy grafu, typ grafu, název grafu, jeho hodnoty a další. Pak každá instance grafu se ukládá do paměti.

Dalším krokem je vytvoření GUI instance. Když objekt je 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 logovacich souborů, důležité proměnné apod.)

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. Její hlavním úkolem je šustění procesu naběhnutí programu, tento proces je popsán v předchozí kapitole.

GUI - jak napovídá název, obsahuje v sobě fuknce pro práce 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.

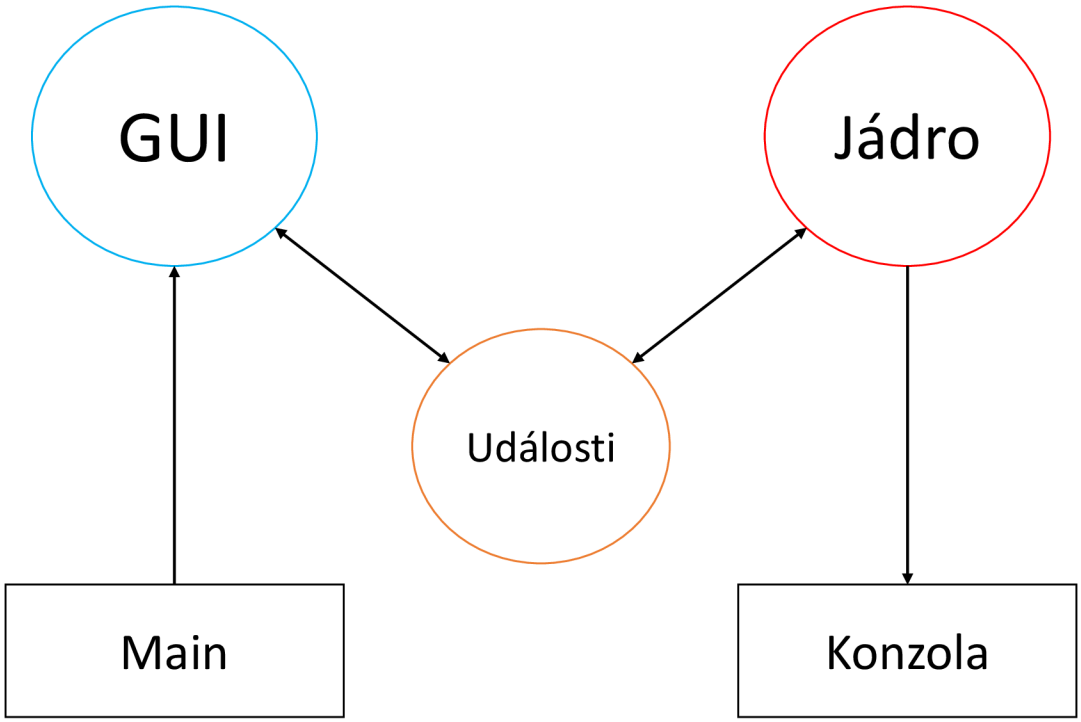
Události - jsou to propojení mezi grafickým rozhraním a jádrem programu. Zodpovědné za volání určitých funkcí podle hodnoty příchozí událostí.

Jádro programu - obsahuje v sobě byznys logiku aplikace. Vykonává určité funkce dle událostí (aktualizace grafu, parsovani zachyceného rámce a jeho analýza a další).

Konzola - simulování příkazového řádku, přijímá text od jádra programu a následně zobrazuje ho.

Funkční bloky

Hlavním funkčním blokem celého nástroje je funkce `realTime`. Tato fuknce řídí celý proces zachytávání rámců a běží v zvláštním vlákně. Hned na začátku funkce se snaží detekovat bazdratove zařízení které bylo předáno uživatelem jako vstupní parametr.



Obr. 3.2: Struktura programu.

Pokud takové zařízení nenajde nebo nebude možné spustit zachytávání, program skončí. V případě úspěchu, začne samotný proces zachytávání. Funkce dostane do proměnné objekt typu `packet` z knihovny Scapy 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 apData. apData je třída vytvořená za účelem uchování informace o provozu určitého přístupového bodu do paměti.

Pokud detekovány přístupový bod již nachází v seznamu nalezených, bude načten jeho apData a následně tento rámec bude analyzován. Informace kterou se dá zjistit z rámce, bude zapsána do objektu apData příslušného přístupového bodu. Pak na konci se zavolá aktualizace dat.

Dalším, jedním z důležitých funkčních bloků je `updatePlotData`. 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 `apData`, 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 funkce překreslování grafu.

Použití

Pro použití programu uživatel musí nainstalivat Python 3 na svůj počítač. Vzhledem k tomu že Python balíčky se dá nainsalovat na Linux operační systémy, nástroj může být spouštěn i na OpenWrt routeru přes SSH připojení.

Dále je potřeba zapnout monitorovací režim na WiFi kartě. Dá se to udělat 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 něho ale v „monitorovacim“ režimu on naposloucha veškerý provoz kolem sebe což umožňuje načítání rámců do lokální paměti a jejich následující analýzu.

Dále můžeme spustit nástroj pomocí příkazu:

```
analyzer.py wlan0mon
```

Nástroj vyžaduje jako vstupní parameter název WiFi zařízení v monitorovacím režimu.

Po naběhnutí se zobrazí hlavní okno programu. Detalni 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 jemu informace o AP v sekci datailu. Kromě toho se bude zobraovat statistika, včetně grafů, jen pro provoz zvoleného AP. Pokud uživatel zvolí All access points, bude se spočítat statistika pro všechny nalezené přístupové body.

Types of graphs - Seznam typů grafů. Grafy se aktualizují každých 50 ms.

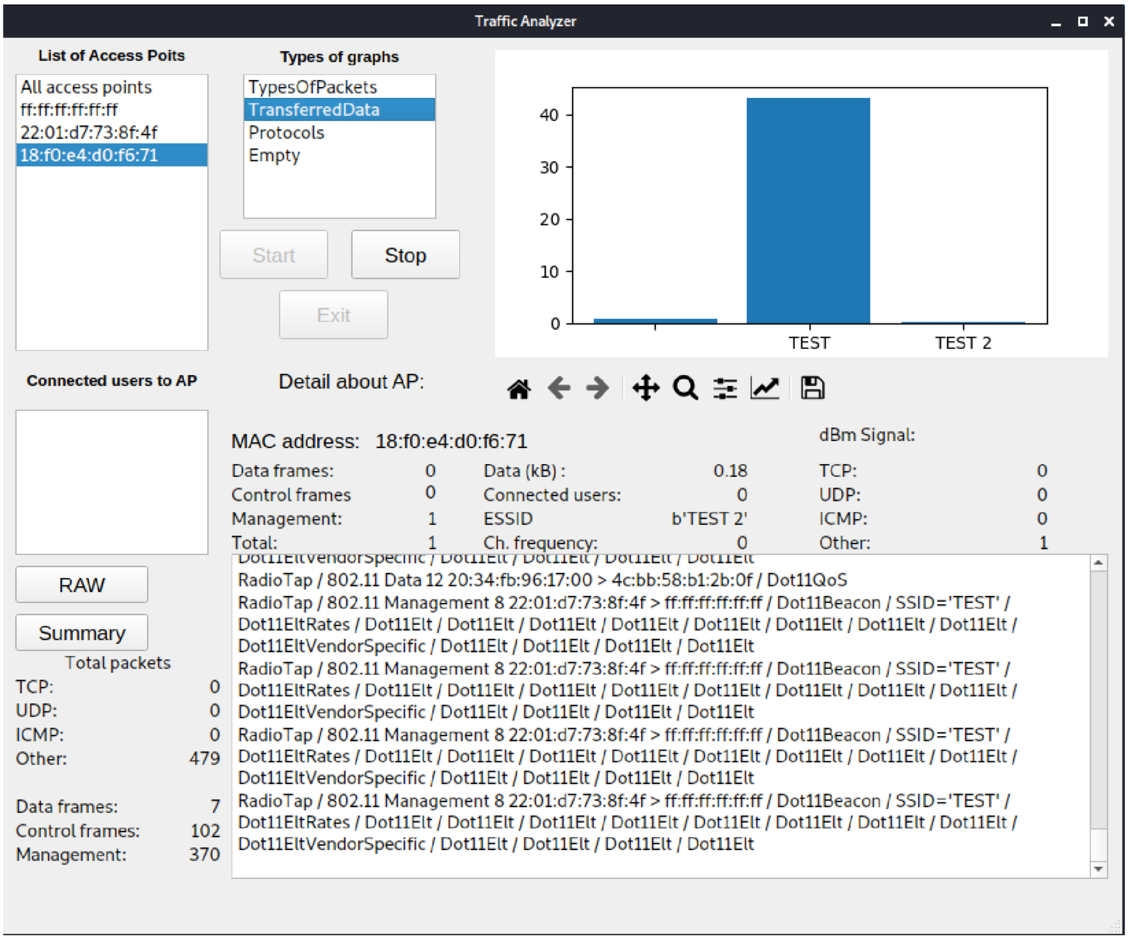
TypesOfPackets - znázorňuje počet různých typů rámců v síti.

TransferedData - zobrazuje velikost přenesených v každé síti.

Protocols - zobrazuje počet rámců s určitým protokolem.

Connected users to AP - Sekce, kde se zobrazují MAC adresy uživatelů určitého přístupového bodu.

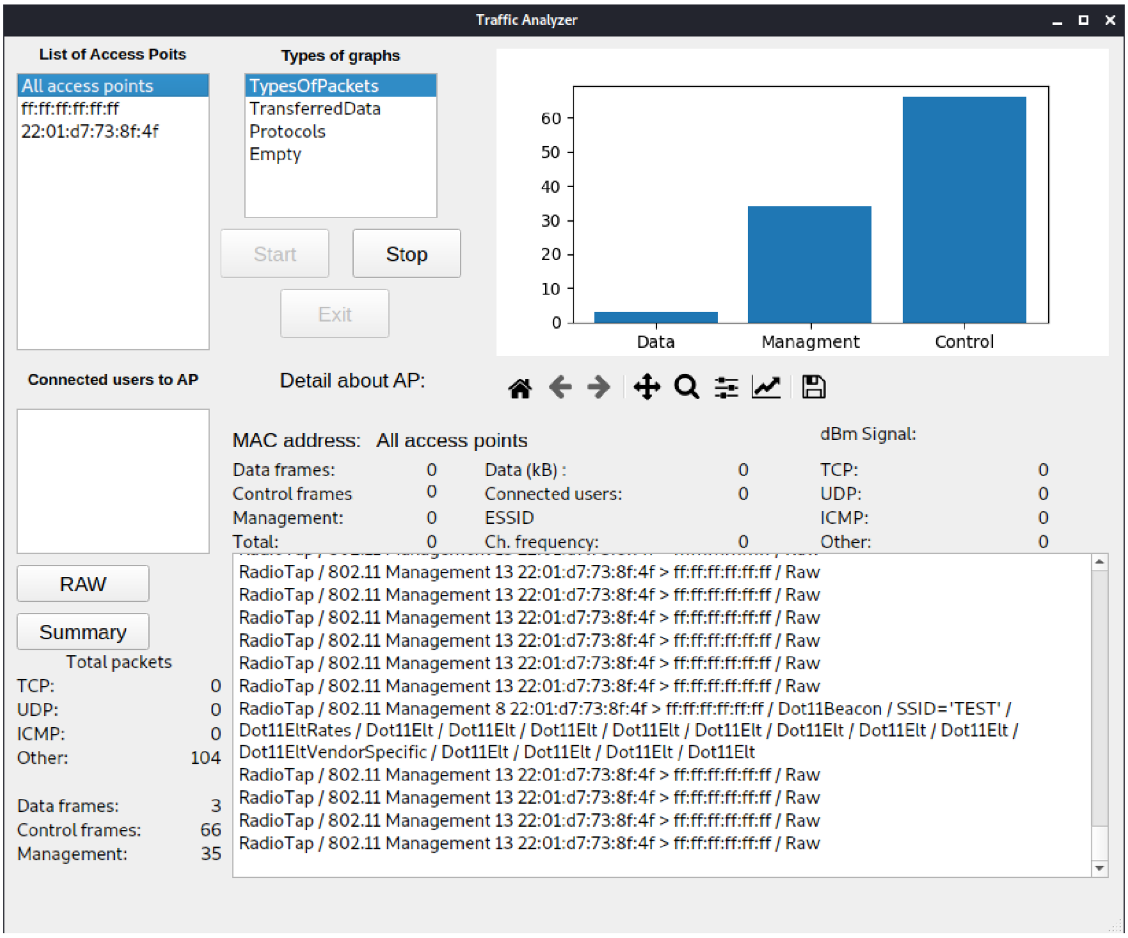
Detail - Sekce pro zobrazení podrobnější informace o přístupovém bodu. Jsou tady jak počty rámců rozdělených do typů a podtypů, tak i název sítí, frekvence, vysílací síla signálu, velikost přenesených dat.



Obr. 3.3: Příklad prostředí programu Traffic Analyzer

Konzola - Cast programů kde se zobrazují výpis informace o zachyceném rámci. Pomocí pomocných tlačítek uživatel může zvolit jaký výpis chce. Pokud zvolí režim RAW tak se do konzoly 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 vypisane informace záleží na typu rámce.

Logovani - Program nabízí uživatelovi 2 typy logovani. První je zápis výpisu konzoly do log souboru, výhodou takového logu je to že data do něho se 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 informace. Druhý typ je ukládání zachyceného provozu do pcap souboru. Výhodou tohoto typu logů je možnost dalšího zpracování.



Obr. 3.4: Příklad fungování programu Traffic Analyzer

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 konfigurace nastavení, například pracovní frekvence, je potřeba tyto nastavení měnit před spuštěním programu. Samotný proces záchytu rámců není závislý na typu modulace, tedy je možné zachytávat provoz různých Wi-Fi standartu `(a\b\g\n\ac\ad)` které používají různou modulace (OFDM , MIMO, DSSS).

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 instalace je potřeba spustit další příkazy v python knzole:

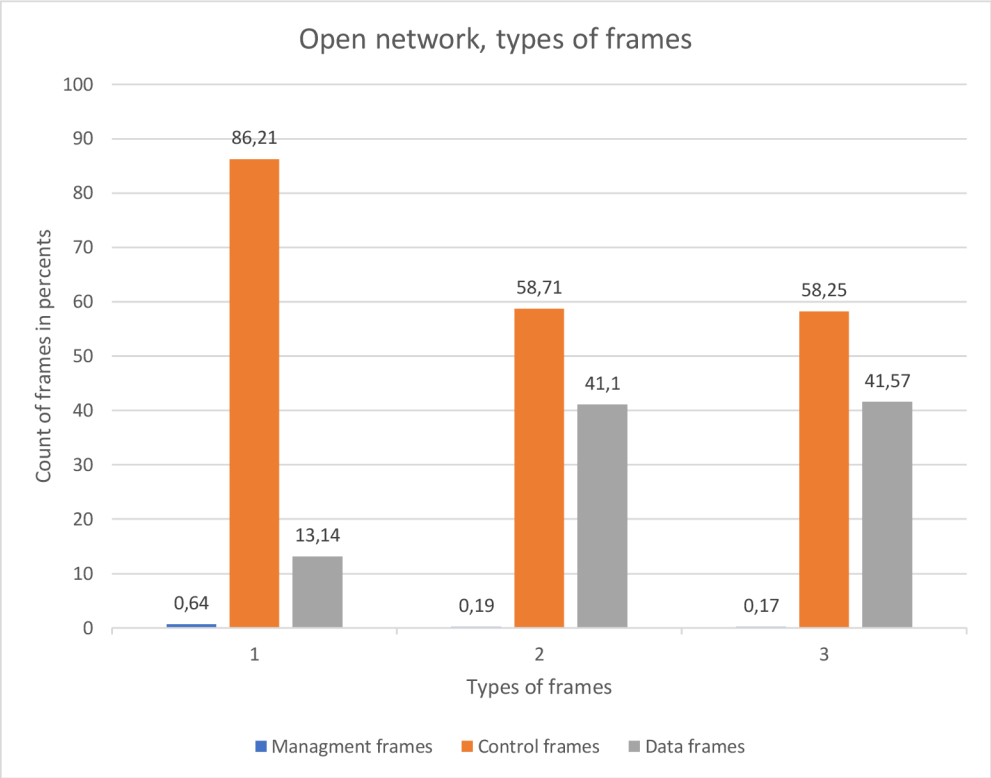
```
pip install -pre scapy[basic]
```

```
pip install matplotlib
```

Výhody Trafic Analyzer

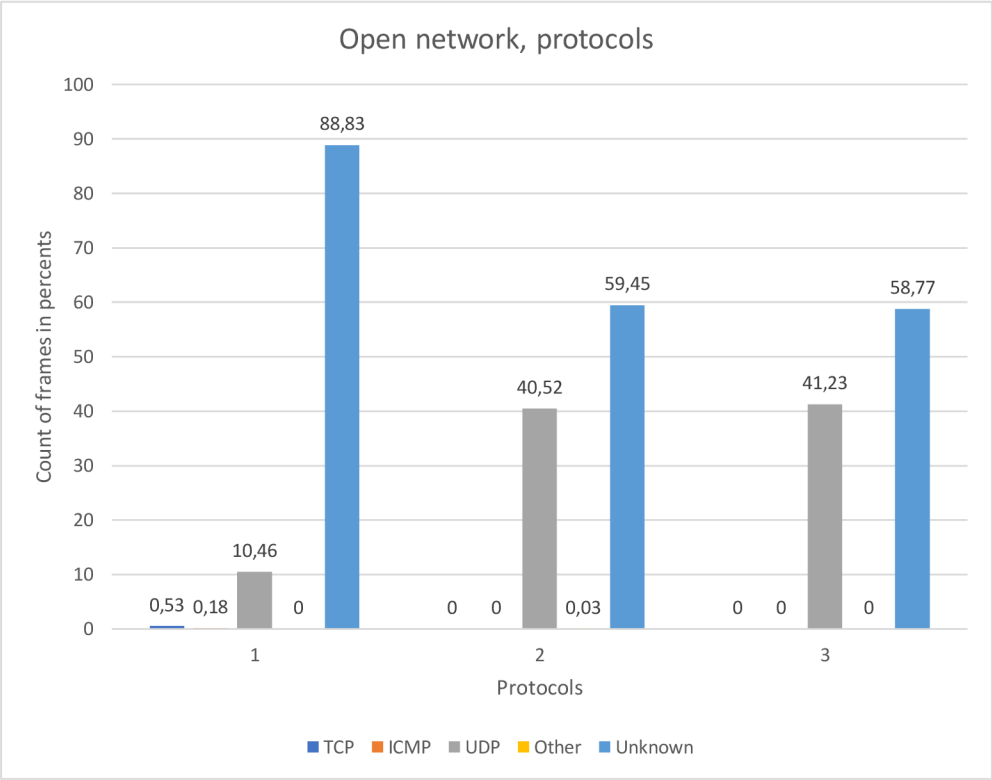
Vzhledem k tomu že program je napsán v programovací jazyce Python 3, dá se ho spustit skoro na jakým koliv zařízení, které podporuje GUI. Díky využití vice-vlaknoveho programování je program dost rychlý a navíc není moc náročný na HW zařízení. Oproti ostatním softwarům dá se program jednoduše modifikovat, vylepšovat a přidávat další části pro analýzu dat, např. další typy grafů apod.

3.1.3 Analýza zachycených dat



Obr. 3.5: Výsledky analýzy otevřené sítě, typy rámců.

Síťový provoz obsahuje mnoho různých informací. Například existují všechny pakety vysílání, které obsahují informace o bezdrátové síti, SSID atd. To je to,

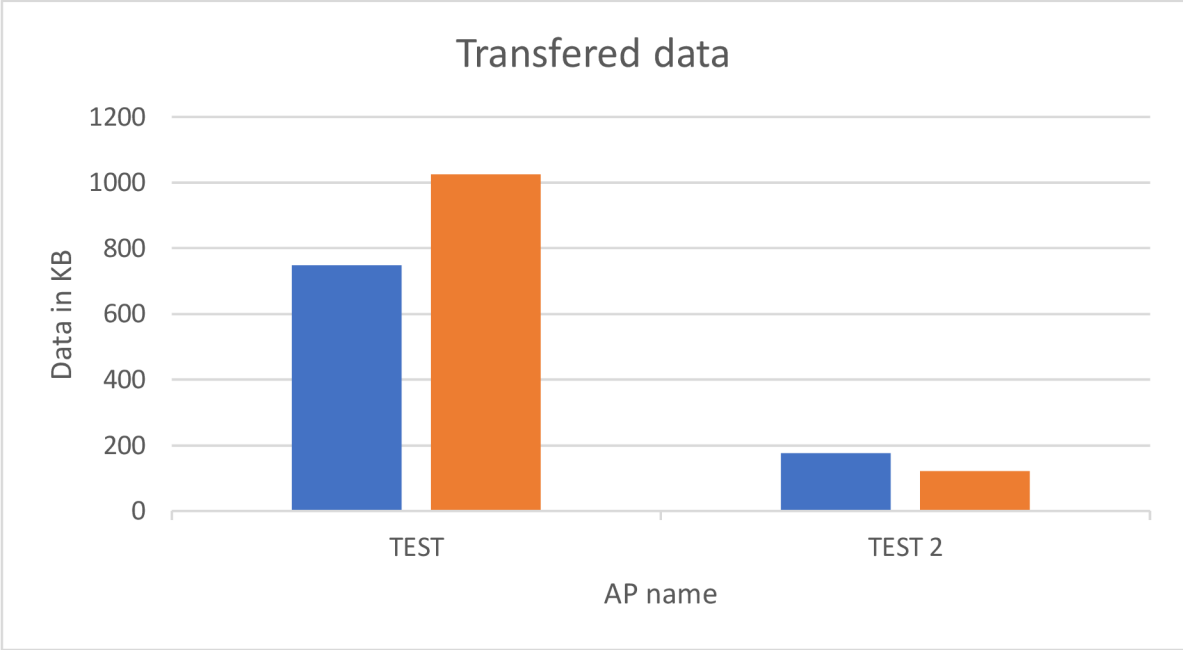


Obr. 3.6: Výsledky analýzy otevřené sítě, protokoly.

co vaše zařízení přijímá, když hledá dostupné sítě. Otázkou je, jak můžeme třídit všechny pakety a najít něco zajímavého.

Každá služba na internetu používá to, co se nazývá port, to je způsob, jak služba (jako webový server) a klient komunikovat. Webové servery používají port 80, e-mailové servery používají port 25 (a některé další), FTP používá port 21, SSH používá port 22 atd. Jeden server může spouštět více služeb (web, e-mail, FTP atd.), I když je IP adresa stejná, protože každá služba používá jiný port.

Nejprve začneme analýzou provozu nezabezpecene sítě protože takový provoz obsahuje poměrně velkou sadu informací. Spustil jsem Traffic Analyzer pro vytvoření třech vzorků zachyceneo provozu. HotSpot s názvem TEST vysílá přes protokol n. TEST 2 je typu b. Oba hot spoty vysílají na frekvenci 2,4 GHz. Vzhledem k tomu že nepodařilo se mi zprovoznit poskytnuty Wi-Fi adaptér, musel jsem provést měření pomocí vlastního zařízení. Kvůli omezené možnosti síťové karty, jsem neschopen otestovat zachytávání provozu přeneseného na jiných frekvencí a pomocí jiných pro-



Obr. 3.7: Výsledky analýzy velikosti přenesených dat.

tokolů.

První graf znázorňuje počet různých typů rámců v procentech. Na obrázku 3.5 lze vidět že v každém z třech měření největší počet mají control rámce. Je to logické protože řídící rámce pomáhají s dodáním datových rámců. To znamená že jejich počet bude stanovit většinu zachyceného provozu.

Další graf (obrázek 3.6) znázorňuje počet výskytů jednotlivých protokolů při každém měření. Vzhledem k tomu že většinu provozu saňoví řídící rámce které neobsahují hlavičku s definici protokolu, na tomto grafu většina rámců spadá do skupiny Unknown.

Nakonec třetí graf, na obrázku 3.7, znázorňuje množství přenesených dat v každé síti.

Dále spustil jsem Traffic Analyzer ale už pro AP zabezpečeného provozu. Jak lze vidět z grafu, situace je téměř stejná jen z jedním rozdílem. Ze zabezpečené sítě kvůli šifrovanému provozu se nedá vůbec zjistit použitý protokol, tedy všechny zachycené

rámce spadají do skupiny Unknown.

Data ve veřejné síti

Z zachyceného provozu nezabezpecene sítě se dá zjistit celkem hodně informací. Nástroj Traffic Analyzer spuštěný v RAW režimu vypíše do konzoly všechno co se dá zjistit. Příklad výpisu informace o jedním rámci:

802.11 hlavička rámce:

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

QoS, LLC, SNAP hlavičky rámce:

```
###[ 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
```

IP hlavička 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
    \options   \
```

Hlavička použitého protokolu:

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

DNS hlavička:

```
###[ 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
    \qd        \
    |###[ DNS Question Record ]###
    |  qname     = 'www.avast.com.'
    |  qtype     = A
    |  qclass    = IN
        an        = None
        ns        = None
        ar        = None
```

Takže je zřejmé že z výpisů můžeme zjistit 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 což v tomto případě www.avast.com. V některých rámcích se dá najít zařízení ze kterého byl připojen uživatel.

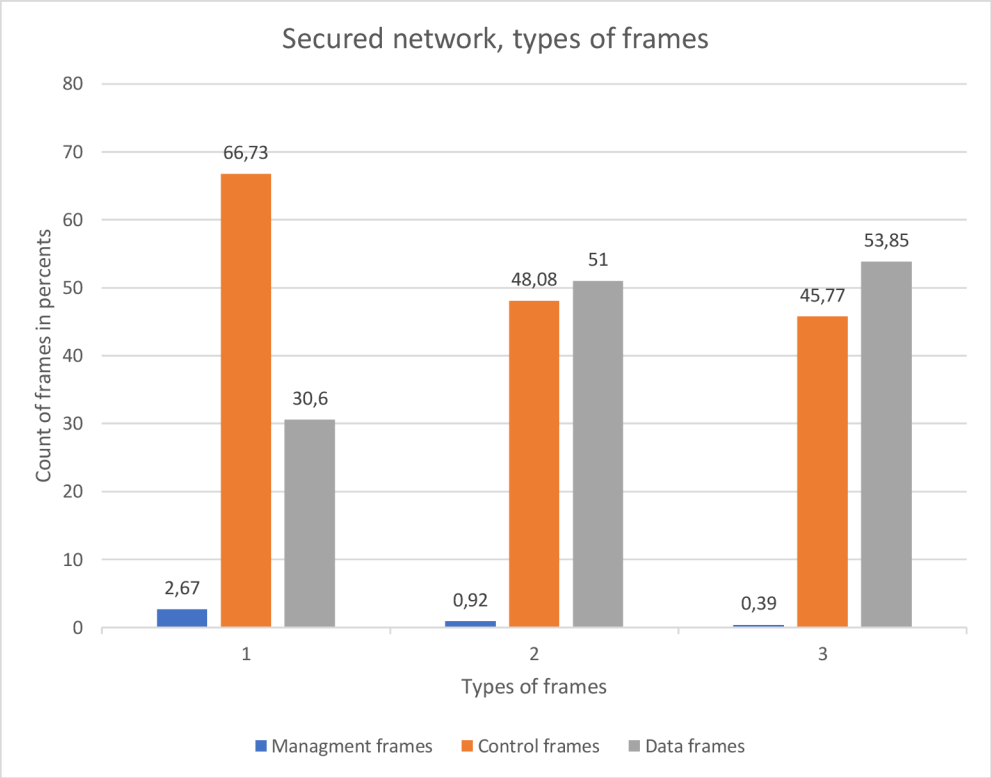
Data v zabezpečené síti

V zabezpečené sítě kvůli šifrování nezjistíme moc informace ale jen základní věci. Příklad výpisu informace datového rámce:

```
###[ 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...'
```

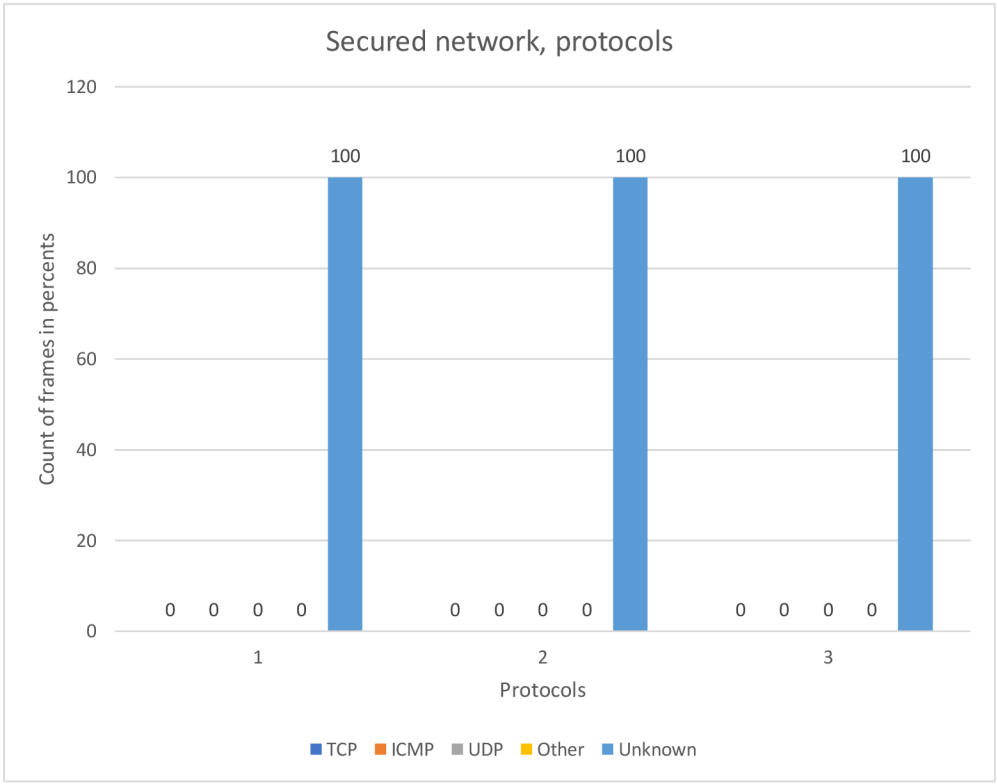
Jak vidíme z obrázku č. 3.8, lze zjistit počty typu přenesených rámce stejně jako u veřejné síti. Opačná situace je u statistiky použitých protokolů, podle obrázku č.

3.9 vidíme, že v zabezpečené síti se nedá vůbec detekovat použitý typ protokolu.



Obr. 3.8: Výsledky analýzy zabezpečené sítě, typy rámců.

Maximálně co se dá najít tak to zdrojové a cílové MAC adresy, informaci o QoS pokud jsou a TKIP packet který obsahuje šifrovaná data.



Obr. 3.9: Výsledky analýzy zabezpečené sítě, protokoly.

Závěr

V této semestrální práce jsem se zaměřil na standard IEEE 802.11 pro rodinu bezdrátových protokolů. V teoretické části probral jsem design sítí postavených na protokolu 802.11, jednotlivé vrstvy komunikace. Taky probral jsem různé standardy protokolů, jejich výhody, nevýhody následně se zaměřil na bezpečnost 802.11. V části věnované bezpečnosti popsal jsem bezpečnostní protokoly WEP, WPA, WPA2 a jejich odlišnosti. V neposlední řadě popsal jsem možnosti prolomení každého protokolu a možností pasivního odposlechů. V praktické části zaměřil jsem se na implementaci programu pro analýzu zachyceného provozu. Můj první návrh programu byl v programovacím jazyce JAVA ale vzhledem k tomu že se mi nepodařilo vyřešit chyby při použití specifických knihoven pro práce s zachyceným provozem, napsal jsem 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. Tak uživatel si 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 uživatel může si prohlídnout seznam MAC adres pripojinych uživatelů do určitého AP.

Program taky nabízí uživatelovi 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 konzole se zobrazuje výpis informací o zachyceném rámců. Pomocí pomocných tlačítek uživatel může zvolit jaký výpis chce. Pokud zvolí režim RAW tak se do konzoly 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 vypisane informace záleží na typu rámce.

Dále, v rámci analýzy, provedl jsem několik testovacích měření a na základě zjištěných dat, statistikych údajů a grafů, vygenerovaných pomocí nově vytvořeného programu, bylo prokázáno co všechno se dá zjistit ze provozu veřejné a zabezpečené síti.

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] 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.

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

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

[6] 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`

[7] 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`

[8] 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`

[9] 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`

[10] 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`