SPECIFICKÉ METODY DETEKCE ANOMÁLIÍ V BEZDRÁTOVÝCH KOMUNIKAČNÍCH SÍTÍCH

SPECIFIC ANOMALY DETECTION METHOD IN WIRELESS COMMUNICATION NETWORKS

Bc. Eva Holasová
Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Technická 12, 616 00 Brno, Česká republika
Kontakt: xkucha24@vutbr.cz

Bc. Karel Kuchař
Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Technická 12, 616 00 Brno, Česká republika
Kontakt: xholas08@vutbr.cz

Ing. Radek Fujdiak, Ph.D.
Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Technická 12, 616 00 Brno, Česká republika
Kontakt: fujdiak@vutbr.cz

ABSTRAKT
Bezdrátové sítě, zejména pak technologie rodiny standardů IEEE 802.11, jsou jednou z klíčových součástí dnešní komunikace. Řešit kybernetickou bezpečnost těchto sítí je tak stěžejní, a to i vzhledem ke stále se zvyšujícímu počtu útoků a nově objevených zranitelností. Z tohoto důvodu se článek zabývá zranitelností bezpečnostních protokolů užitých v rámci IEEE 802.11 a to z pohledu metod detekce průniku i detekce obecných bezpečnostních incidentů. Prezentované výsledky najdou využitelnost mj. v systémech detekce a prevence.
Klíčová slova: 802.11, Wi-Fi, Kybernetická bezpečnost, Bezpečnostní incidenty.

ABSTRACT
Wireless networks, especially the technologies of the IEEE 802.11 family of standards, are one of the key components of today's communication. Addressing cyber security in these networks is thus crucial, also in view of the ever-increasing number of attacks and newly discovered vulnerabilities. For this reason, the article deals with the vulnerability of security protocols used in IEEE 802.11 in terms of intrusion detection methods and detection of general security incidents. The presented results will find usability, among other things, in detection and prevention systems.
Keywords: 802.11, Wi-Fi, Cybersecurity, Security incidents.

1 Úvod

Oblast bezdrátových sítí je v současné době značně využívána [1], což dokládá i neustálý vývoj standardů IEEE 802.11 (známo též jako Wi-Fi), viz kapitola 2. Lidé stále více používají Wi-Fi ve školách, v práci, v kavárnách a kdekoliv, kde je přístup k bezdrátové síti. Pomocí bezdrátových sítí komunikují nově i domácnosti [2], může být využívána internetem věcí [3, 4] nebo třeba v průmyslových bezdrátových senzorových sítích [5]. 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 [6].

V kapitole 3 je popsáno z čeho se skládá bezdrátová síť a jaké existují vektory útoky v těchto sítích. Tato kapitola také obsahuje tabulku s návrhy metod k simulaci jednotlivých útoků a zranitelností, pomocí jakých nástrojů je realizovat a detekovat. V kapitole 4 je popsána experimentální síť. Kapitola 5 představuje experimentální testování a výsledky, kterých bylo docíleno.

2 Aktuální stav

Bezdrátové sítě pracují v bezlicenčních pásmech ISM. Jedná se o 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 záleží, zda jde o vnitřní prostory budov (5,15-5,35 GHz), anebo o prostor mimo budovy (5,47–5,725 GHz). Další rozsah v pásmu 5 GHz je již omezen nízkým vysílacím výkonem [7]. K nejznámějším standardům IEEE 802.11 patří standardy IEEE 802.11a/b/g/n/ac nebo nejnovější ax. Nicméně standardů existuje mnohem více. Například standard IEEE 802.11e přišel s kvalitou služeb [8], standard IEEE 802.11i přinesl zabezpečení WPA (Wi-Fi Protected Access) [9]. Standard IEEE 802.11p se používá pro zajištění bezdrátového přístupu ve vozidlech [10]. Tabulka 1 představuje přehled nejznámějších standardů IEEE 802.11 z pohledu používajícího pásma, maximální přenosové rychlosti, technologie fyzické vrstvy, šířky kanálu a roku vytvoření (data převzata z [11, 12, 13, 14]).

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

Tabulka 1 Přehled vybraných standardů IEEE 802.11.

Tyto standardy jsou zpětně kompatibilní, což může představovat bezpečnostní riziko. Bezpečnost bezdrátové sítě je závislá na vybraném šifrovacím standardu. S postupným vývojem standardů IEEE 802.11 dochází i k vývoji bezpečnostních protokolů. Novější standardy poskytují vyšší úroveň zabezpečení, ale i u nich byly nalezeny zranitelnosti.

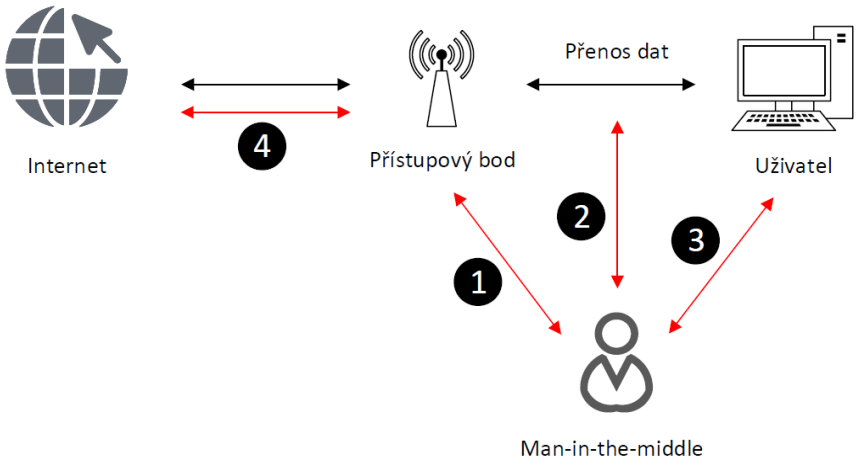
Tabulka 2 nabízí přehled bezpečnostních protokolů používaných u standardů IEEE 802.11. Porovnává protokol WEP (Wired Equivalent Privacy), WPA, WPA2 a WPA3 z pohledu šifrování, autentizace, integrity dat a správy klíčů. Tabulka obsahuje roky zahájení používání protokolů a s jakými standardy se začali používat. Dále tabulka obsahuje standardy, na kterých jsou protokoly dostupné dnes a kdy byla nalezena první zranitelnost těchto protokolů (data převzata z [6, 13, 15]).

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

Tabulka 2 Přehled bezpečnostních protokolů u standardů IEEE 802.11.

3 Návrh metod

Bezdrátové sítě jsou složeny z přístupového bodu, ke kterému se připojují uživatelské stanice. Tyto stanice využívají ke komunikaci vybraný standard, který definuje možné způsoby zabezpečení. Na obrázku 1 jsou zobrazeny jednotlivé vektory útoku na části bezdrátové sítě. Vektor útoku na přístupový bod (1), vektor útoku na přenos dat (2), vektor útoku na uživatele a uživatelskou stanici (3) a vektor útoku z internetu (4). V tomto článku je pracováno s vektory 1 a 3.



Obrázek 1 Identifikované vektory útoku v bezdrátových sítích.

Tabulka 3 představuje přehled simulovaných útoků nebo zranitelností zpracovaných v tomto článku. Na které bezpečnostní protokoly je cíleno a jakými nástroji jsou útoky nebo zranitelnosti realizovány. Jaké jsou jednotlivé detekce simulovaných útoků nebo zranitelností.

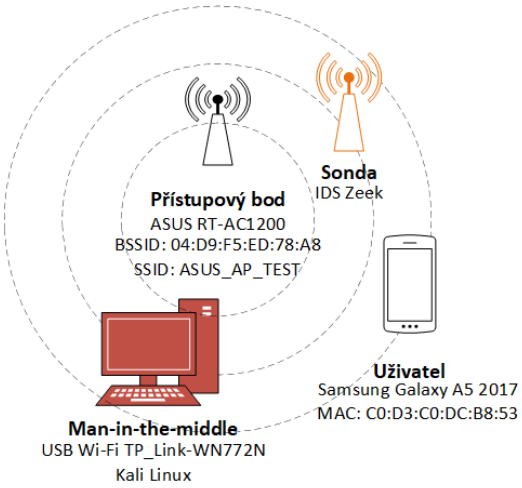
Slovníkový útok využívá předdefinovaného seznamu nejpoužívanějších hesel pro lámání hesel. Aircrack-ng je nejznámější a nejoblíbenější nástroj na lámání hesel [16]. Používá se k lámání hesel WEP a WPA-PSK (Pre-Shared Key). Nejprve zachytává pakety a pak je analyzuje. Aircrack-ng je soubor několika nástrojů, například: *aircrack-ng* na prolomení WEP a WPA/WPA2 klíčů, *airmon-ng* pro přepnutí síťového adaptéru do promiskuitního režimu nebo *airplay-ng*, který umožňuje zasílání deautentizačních paketů. KRACK (Key Reinstallation attack) je zranitelnost 4-way handshake bezpečnostního protokolu WPA2-Personal [17]. K simulaci KRACK je využit vytvořený skript na testování, zda je zařízení náchylné na tuto zranitelnost [18]. Útok DoS (Denial of Service) je realizován pomocí nástroje hping3. Hping3 je generátor a analyzátor paketů TCP/IP, který je schopný simulovat několik různých DoS útoků [19]. Pro detekci DoS útoku je použit IDS systém Zeek.

Vektor	Útok/Zranitelnost	Bez. Protokol	Nástroj	Detekce
1, 3	Slovníkový útok	WEP, WPA-PSK	Aircrack-ng	–
1, 3	KRACK	WPA2 – Personal	Skript	Sonda
1, 3	DoS	–	hping3	Zeek
1, 3	Deautentizace	–	Airplay-ng, sonda	Sonda

Tabulka 3 Přehled simulovaných útoků a zranitelností.

4 Experimentální prostředí

K provedení experimentálního testování je sestavena experimentální síť zobrazena na obrázku 2. Síť je složena z přístupového bodu, uživatelské stanice, stanice v režimu Man-in-the-middle (MITM) a sondy. K simulaci bezpečnostních incidentů je využita stanice s virtualizovaným operačním systémem Kali Linux [20]. Tato stanice je dále vybavena USB Wi-Fi adaptérem pracujícím v monitorovacím režimu. Aby bylo možné zachytávat veškerý síťový provoz, bylo využito příkazu *airmon-ng start wlan0*, který uvede bezdrátové rozhraní do monitorovacího režimu.



Obrázek 2 Experimentální síť.

5 Experimentální výsledky

5.1 Slovníkový útok

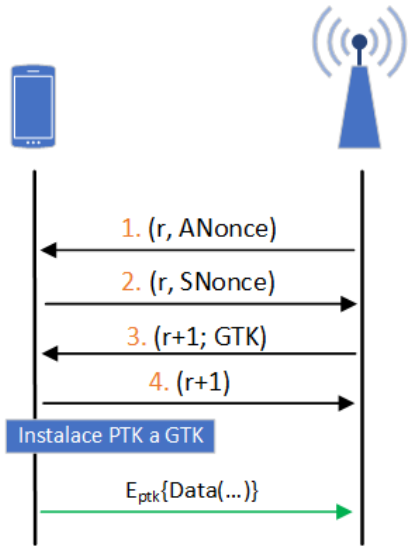
Experimentální testování je nejprve zaměřeno na slovníkový útok na bezpečnostní protokol WEP. Jelikož WEP není příliš podporován, je nutné využít standard IEEE 802.11g, a ten nastavit na přístupovém bodě. K prolomení hesla WEP je nutné zachytit síťovou komunikaci šifrovanou pomocí WEP. K tomu je třeba získat číslo kanálu a BSSID (Basic Service Set Identifiers) přístupového bodu. Jako klíč WEP byla nastavena kombinace 41831.

Pro výpis těchto informací je využit příkaz *airodump-ng wlan0mon*. Následné zachytávání provozu je provedeno pomocí příkazu *airodump-ng -c [kanál] -bssid [mac] -w [soubor] wlan0mon*. K fake autentizaci je využit příkaz *aireplay-ng -1 0 -a [mac] wlan0mon*, kde je následně generován provoz pomocí ARP (Address Resolution Protocol) request/replay zpráv příkazem *aireplay -3 -b [mac] wlan0mon*. Po dosažení přenesení určitého množství zpráv (minimálně 10000 vektorů) lze prolomit klíč pomocí příkazu *aircrack-ng -0 '[soubor]'*. Klíč k WEP byl prolomen po 10 sekundách a otestováno bylo 40418 klíčů.

Experimentální testování bylo provedeno obdobně pro bezpečnostní protokol WPA. Heslo k WPA je nastaveno na Anonymous. Postup je totožný, až na poslední příkaz. V případě WPA je nutné použít slovník, pomocí kterého bude přístupová fráze prolomena. Lze využít toho, že OS Kali Linux již obsahuje slovník "Rockyou" [21]. Poslední příkaz bude mít podobu *aircrack-ng -b [mac] -w /usr/share/wordlist/rockyou.txt [soubor]*. Prolomení hesla trvalo 17 minut.

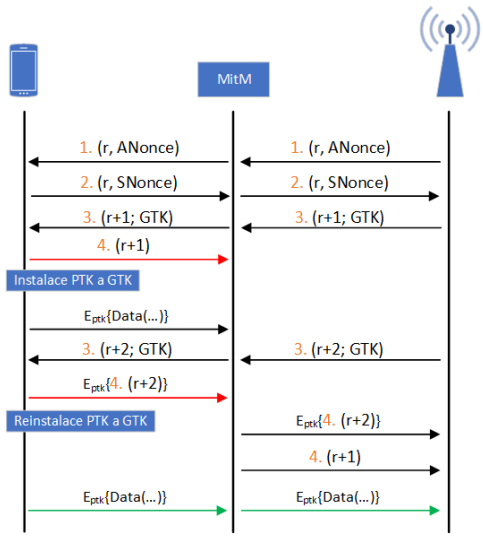
5.2 Simulace útoku KRACK

Současně používané bezdrátové standardy IEEE 802.11 pracují s protokolem WPA2. Protokol využívá k autentizaci mechanizmus 4-way handshake, viz obrázek 3. Tento protokol je ale zranitelný na útok KRACK. Útočník není schopen získat heslo k bezdrátové síti, ani získat šifrovací klíč, který byl dohodnut během 4-way handshaku. Je ale schopen dešifrovat komunikaci mezi klientem a přístupovým bodem. Poté je možné nejen komunikaci odposlouchávat, ale i vytvářet a injektovat provoz.



Obrázek 3 Autentizační mechanizmus WPA2 4-way handshake.

Na obrázku 4 je znázorněn postup útoku KRACK na 4-way handshake. Útok využívá ustanovení MITM, který přeposílá první tři zprávy 4-way handshaku. Čtvrtou zprávu od klienta však nepřepošle na legitimní AP. Klient v domnění, že 4-way handshake proběhl úspěšně, instaluje klíč relace PTK a začne posílat šifrovanou komunikaci směrem k AP přes MITM, který tuto zprávu opět nepřeposílá dále. Po vypršení časovače přijetí 4. zprávy legitimního AP, dochází k opětovnému zaslání zprávy 3 s inkrementovanou hodnotou replay counter (r). V reakci na tento stav dochází na klientské stanici k reinstalaci PTK klíče a odeslání zašifrované 4. zprávy. Tato zpráva je předána legitimnímu AP k dokončení 4-way handshaku. MITM nyní provede XOR operaci mezi původní 4. zprávou a šifrovanou 4. zprávou (červeně vyznačené) k získání keystreamu. Získaný keystream je využit k šifrování a dešifrování následujících zpráv (zeleně vyznačené).



Obrázek 4 Popis jednotlivých proměnných při útoku KRACK.

K demonstraci detekce pokusu o KRACK útok bylo využito toho, že je nutné, aby legitimní AP zopakoval 3. zprávu 4-way handshaku dvakrát a tím klient po druhé vygeneroval zprávu 4. Toto chování lze na síti detekovat pomocí síťového rozhraní v monitorovacím režimu. K detekci tohoto chování byl vytvořen skript v programovacím jazyce Python. Skript využívá nástroje Scapy, který umožňuje zachytávání a následnou práci se síťovým provozem v režimu sondy síťového provozu. Pravidlo s filtrací EAPOL (Extensible Authentication Protocol over LAN) rámců, viz výpis 1. Po zachycení EAPOL rámce dojde k zaznamenání počtu pokusů komunikace mezi AP a klientem, viz výpis 2.

```
sniff(filter="wlan proto 0x888e", prn=detection)
```

Výpis 1 Filtrační pravidlo, EAPOL rámec.

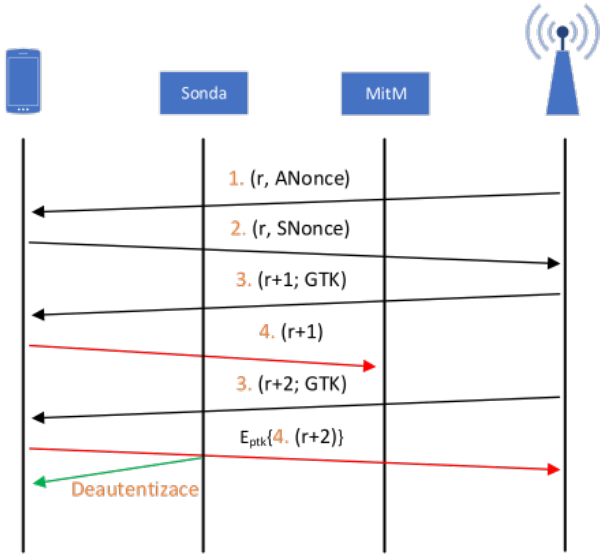
```
root@kali:~/PycharmProjects/detection# python3.7 eapol.py
Zdrojova adresa:  C0:D3:C0:DC:B8:53
Cilova adresa:  04:D9:F5:ED:7B:A8
ID:  14849
Typ:  2
BSSID:  04:D9:F5:ED:7B:A8
Komunikace zachycena: 1 x
```

Výpis 2 Výpis vytvořeného skriptu, výpis zachycení EAPOL rámce.

Tento skript lze dále rozšířit o následnou deautentizaci, pseudokód viz výpis 3, a přimět tak obě legitimní strany opětovně provést 4-way handshake pro ustanovení nového klíče relace, viz obrázek 3. V síti bude akceptován pouze 4-way handshake, který proběhl úspěšně na první pokus. Aby nevznikla přílišná zátěž sítě, lze dále využít skript pro detekci zranitelnosti na KRACK útok a provádět vyžadování 4-way handshaku na první pokus pouze pro zařízení s potenciální zranitelností.

```
if hanshakeDetection:
        create pair IP->number of message 3
        for every pair do:
                if message 3 > 1:
                        send deauthentication packet
```

Výpis 3 Pseudokód detekce podruhé zaslané zprávy 3 s deautentizací.

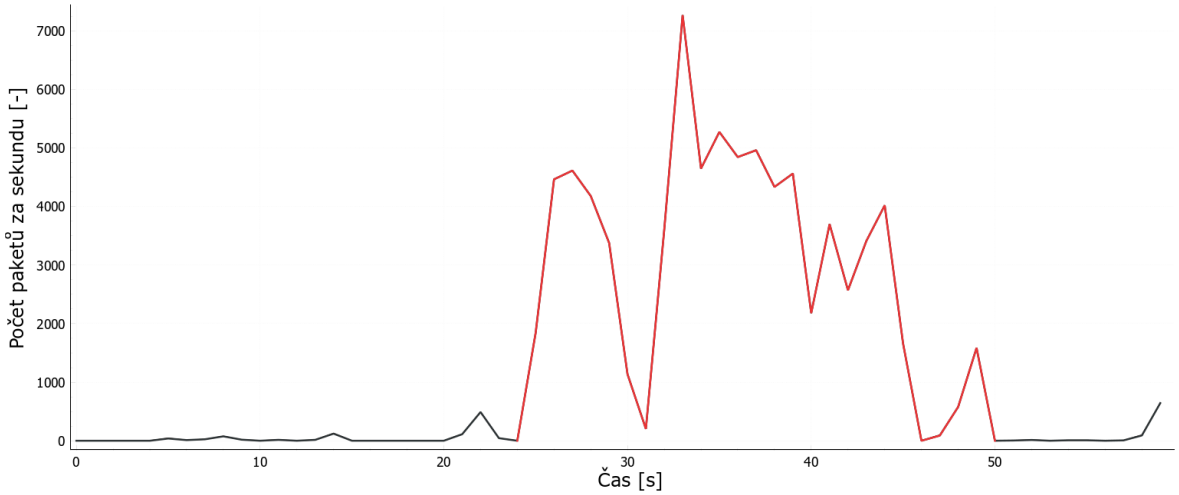


Obrázek 5 Princip proměnných detekující podruhé zaslanou čtvrtou zprávu 4-way handshaku.

5.3 Simulace útoku DoS

Dále byla v rámci experimentálního testování provedena detekce útoku DoS zaměřeného na uživatelskou stanici s OS Kali Linux. Ke generování útoku byla využita stanice Man-in-the-middle s OS Kali Linux, kde byl využit nástroj *hping3*. Aby bylo možné vytvořit metody, které budou schopny provádět detekci tohoto útoku, byl tento útok zaznamenán pomocí nástroje Wireshark [22] v rámci uživatelské stanice.

Pro vyvolání útoku DoS je použit příkaz *hping3 192.168.1.238 –flood*. Parametr *–flood* zajistí co nejrychlejší posílání paketů na cíl. Záznam provozu, viz obrázek 6, černě vynesený provoz odpovídá běžnému provozu na síti, červeně zvýrazněný odpovídá zatížení stanice způsobené zpracováním přijatých paketů při útoku DoS.



Obrázek 6 Úspěšně zaznamenaný provoz se zachyceným DoS útokem.

Ze záznamu provozu byla navržena metoda, která pracuje s průměrnou délkou navázaného spojení. Ta vychází z toho, že útok DoS využívá TCP spojení, která jsou velmi krátká a také z pohledu délky jejich trvání velice podobná. Rovnice 1 definuje výpočet průměrné délky spojení. Využívá se zde sumy dob jednotlivých spojení δ vždy pro jednotlivou IP adresu, s využitím jejich počtu n. Následně je vytvořeno pole ω, kde jsou uloženy procentuální rozdíly jednotlivých dob spojení.

$$\tau = \frac{\sum_1^n \delta}{n} [s]. \tag{1}$$

Rovnice 2 definuje výpočet průměrného procentuálního rozdílu jednotlivých procentuálních rozdílů jednotlivých dob spojení. Získaná hodnota definuje, v jakém průměrném poměru jsou jednotlivé TCP relace.

$$\lambda = \frac{\sum_1^m \omega}{m} [\%]. \tag{2}$$

K rozhodnutí, zda se jedná o útok, byla vytvořena rovnice 3, která porovnává momentální procentuální rozdíl λ s předchozím procentuálním rozdílem. Předchozí procentuální rozdíl je možné dále upravit pomocí parametru *k*.

$$\lambda_{r-1} * (1-k) \leq \lambda_r \leq \lambda_{r-1} * (1+k). \tag{3}$$

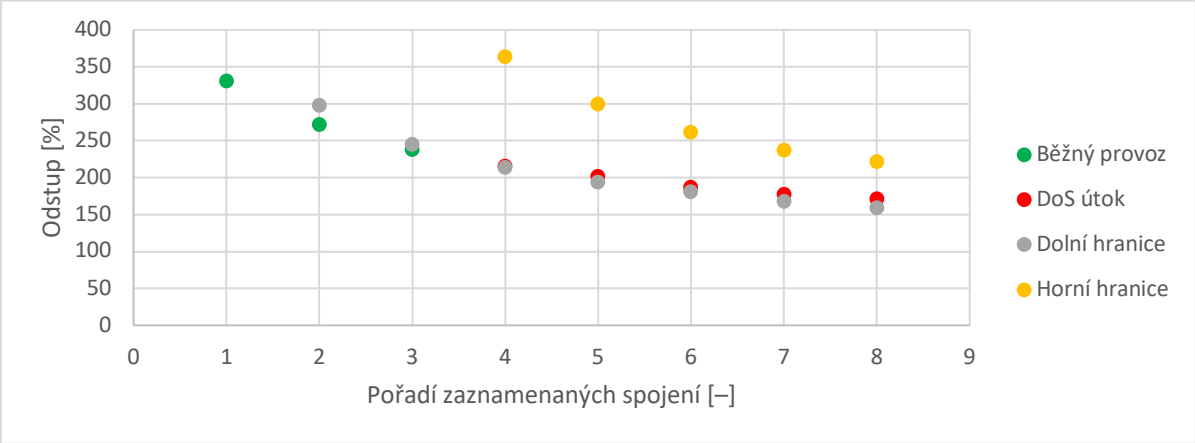
Navržené rovnice byly implementovány v IDS systému ZEEK. V tomto systému bylo využito skriptu *main.zeek* v rámci adresáře *conn*, který pracuje s jednotlivými spojeními. Po implementaci jednotlivých rovnic bylo provedeno experimentální testování s DoS útokem.

To znamená, že systém Zeek si v reálném čase zaznamenává, kolik spojení bylo vytvořeno z konkrétní IP adresy a vypočítává průměrnou délku všech spojení z této adresy. Vypočítává procentuální rozdíl délky trvání spojení od předchozího spojení a z těchto hodnot je vypočítán průměrný procentuální rozdíl. Takže pokud je zaznamenáno nové spojení z dané adresy, délka tohoto spojení je připočítána k sumě předchozích spojení a je přepočítán průměr délky spojení z dané adresy. Následně pokud je splněna podmínka v rovnici 3, je vyhlášen poplach.

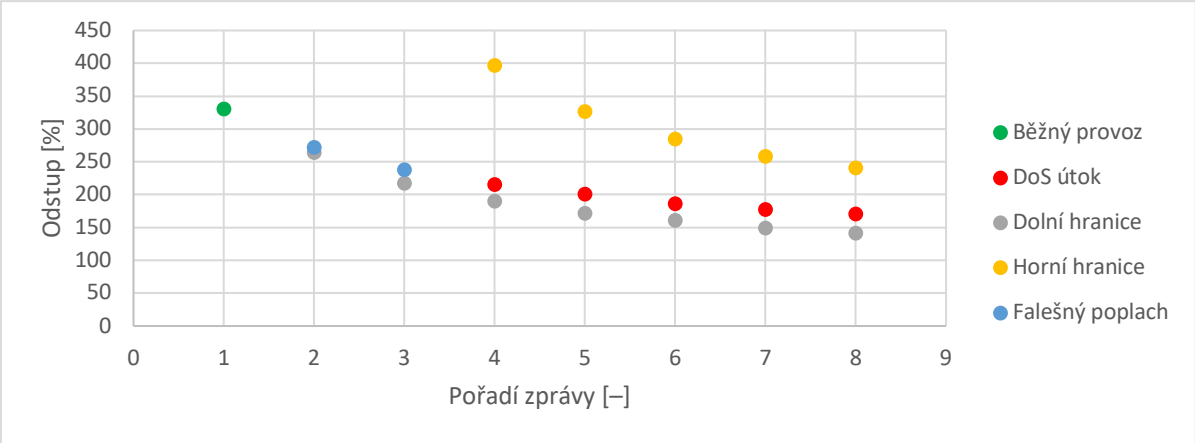
Výpis 4 zobrazuje vygenerovaný log v systému Zeek pomocí skriptu main.zeek s implementovanými rovnicemi, který upozorňuje na probíhající DoS útok. V rámci experimentálního testování byl parametr *k* z rovnice 3 nastaven na hodnotu 10 %. Obrázek 7 představuje znázornění běžného provozu a útoku DoS. Zároveň jsou v grafu vyneseny horní ($\lambda_{r-1} * (1+k)$) a dolní ($\lambda_{r-1} * (1-k)$) hranice, které odpovídají rovnici 3 s nastaveným parametrem k na hodnotu 0,1 (10 %). Jelikož se mění délka jednotlivých spojení, mění se i hodnoty hranic (rovnice 3), které vytvářejí odstup, ve kterém může být detekován a vyhlášen poplach. Parametr k=0,1 se nejvíce blíží vyneseným bodům a je stále schopen detekovat útok. 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 obrázek 8.

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

Výpis 4 Vygenerovaný log, detekce DoS útoku v IDS systému Zeek.



Obrázek 7 Parametr k nastaven na 10 %.



Obrázek 8: Parametr k nastaven na 20 %.

5.4 Detekce deautentizace

Velkou část útoků zahajuje proces deautentizace, proto byl využit skript [23], který umožňuje detekovat deautentizační rámce, které se vyskytly v síti. Skript vyžaduje nástroj Scapy pro práci se síťovým provozem a nastavení Wi-Fi adaptéru do monitorovacího režimu. Výpis 5 zobrazuje výstup skriptu při zachycení deautentizačního rámce s cílem odpojit zařízení s MAC adresou *c0:d3:c0:dc:b8:53* od bezdrátové sítě.

```
[#] Deauthentication Packet : c0:d3:c0:dc:b8:53 <---> 04:d9:f5:ed:7b:a8 | Packets : 1
[#] Deauthentication Packet : 04:d9:f5:ed:7b:a8 <---> c0:d3:c0:dc:b8:53 | Packets : 4
```

Výpis 5: Zachycení deautentizačních paketů.

6 Diskuze

Vytvořená metoda k detekci KRACK útoku v síti s následnou deautentizací se zaměřuje na průvodní jevy útoku. Tento jev (podruhé zaslaná třetí zpráva 4-way handshake) může nastat i v případě, kdy došlo v síti k chybě a je nutné přenášené zprávy zopakovat. Vytvořený skript zareaguje i v tomto případě a dochází tak k deautentizaci validního uživatele. Navržená metoda řeší pouze aktuální situaci a může tak docházet k deautentizacím opakovaně. V případě opakovaného pokusu o útok KRACK nebo vznikajícím chybám v síti, vyžadující opakování zprávy 3, může dojít k chvilkovému výpadku služby.

Různé typy DoS útoků představují vážnou hrozbu pro společnost, jelikož je těžké tyto útoky predikovat a bránit se jim. Vzhledem k nepředvídatelnému chování útočníka je obtížné odlišit legitimní síťový provoz od škodlivého provozu. Článek [24] popisuje důležitost vysoké úrovně přesnosti a účinnosti vytvořených detekčních metod. V článku je navržen pro detekci DoS útoků v síti pomocí několika modelů strojového učení, kdy výsledky těchto modelů se pohybují s úspěšností 99,7 % a zbylých 0,3 % tvoří falešné poplachy.

Metoda na detekci DoS útoku na uživatelskou stanici v bezdrátové síti implementovanou pomocí IDS Zeek nevyžaduje předcházející fázi učení a ani model strojového učení a umožňuje detekci útoku v reálném čase. Je však nutné vhodně zvolit korekční parametr k, který definuje oblast detekce, aby nedocházelo k falešným poplachům nebo nedetekování bezpečnostního incidentu.

7 Závěr

Bezdrátové sítě jsou stále více používány a je nutné udržovat jejich zabezpečení na co nejvyšší úrovni. Práce se nejprve zaměřuje na prolomení bezpečnosti WEP a WPA pomocí nástroje Aircrack-ng. U protokolu WPA2 byla využita zranitelnost KRACK v 4-way handshaku. Proti tomuto útoku lze síť chránit například pomocí detekce opětovného zaslání zprávy 3 a 4 4-way handshaku, které je představeno v tomto článku. Pro zvýšení bezpečnosti bezdrátových sítí lze také využít zachytávání deautentizačních rámců.

Navržené rovnice pro detekci DoS útoku se jeví jako efektivní, jsou schopné zachytit probíhající DoS útok na uživatelskou stanici. Jejich výhoda je v tom, že není nutné provádět žádnou fázi „učení“, ale je možné jejich okamžité nasazení. IDS systém ZEEK lze jednoduše upravit a rovnice tak implementovat. K detekci DoS útoku bylo využito jejich specifickému charakteru, který se postupně opakuje, tedy jednotlivé relace si jsou časově velice podobné. Tento způsob se v rámci experimentálního testování prokázal jako účinný. K provádění

detekce anomálií nejen v bezdrátových sítích je vhodné nasazovat a využívat IDS systémy, které jsou schopné získat velké množství parametrů síťového provozu, na jejich základě je vhodné vytvářet další mechanismy k detekci bezpečnostních incidentů.

Velkou výhodou a zároveň nevýhodou bezdrátových sítí je jejich volné šíření prostorem. Pro adekvátní zabezpečení je nutné dbát jak na uživatelskou část zabezpečení, tedy definovat určité požadavky na vytvořené heslo, tak i na zabezpečení poskytnuté samotným standardem. Pro zabezpečenou síť je vhodné nastavit nejsilnější úroveň zabezpečení, zvolit silnou přístupovou frázi a umístit do sítě IDS/IPS (Intrusion Detection System/Intrusion Prevention System) systém, nebo bezdrátový IDS/IPS systém, k zaznamenání nedovoleného chování v síti. Popřípadě používání dalších skriptů ke kontrole vybraných parametrů. Mimo IDS/IPS systémů je vhodné implementovat mechanismy využívající strojového učení, které jsou schopny provádět detekci anomálií vyskytujících se v síťovém provozu.

Poděkování

Tento článek byl vytvořen za podpory Národního programu udržitelnosti v rámci grantu LO1401 a Technologické agentury České republiky (TAČR) v rámci projektu č. TJ02000332. Pro výzkum byla využita infrastruktura vědecko-výzkumného centra SIX.

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] 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.

[7] MYKHALEVSKIY, Dmytro V. Investigation of Wireless Channels of 802.11 Standard in the 5ghz Frequency Band. *Latvian Journal of Physics and Technical Sciences* [online]. 2019, **56**(1), 41-52 [cit. 2020-05-27]. DOI: 10.2478/lpts-2019-0004. ISSN 0868-8257

[8] MANGOLD, S., SUNGHYUN CHOI, G.R. HIERTZ, O. KLEIN a B. WALKE. Analysis of IEEE 802.11e for QoS support in wireless LANs. *IEEE Wireless Communications* [online]. 2003, **10**(6), 40-50 [cit. 2020-05-27]. DOI: 10.1109/MWC.2003.1265851. ISSN 1536-1284.

[9] 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: Amendment 6: Medium Access Control (MAC) Security Enhancements," in IEEE Std 802.11i-2004 , vol., no., pp.1-190, 24 July 2004

[10] JIANG, Daniel a Luca DELGROSSI. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. *VTC Spring 2008 - IEEE Vehicular Technology Conference* [online]. IEEE, 2008, 2008, , 2036-2040 [cit. 2020-05-27]. DOI: 10.1109/VETECS.2008.458. ISBN 978-1-4244-1644-8. ISSN 1550-2252.

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

[12] *IEEE Communications Magazine* [online]. 2008, **46**(7) [cit. 2020-05-27]. ISSN 0163-6804.

[13] 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

[14] QU, Qiao, Bo LI, Mao YANG, Zhongjiang YAN, Annan YANG, Der-Jiunn DENG a Kwang-Cheng CHEN. Survey and Performance Evaluation of the Upcoming Next Generation WLANs Standard - IEEE 802.11ax. *Mobile Networks and Applications* [online]. 2019, **24**(5), 1461-1474 [cit. 2020-05-27]. DOI: 10.1007/s11036-019-01277-9. ISSN 1383-469X.

[15] 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. 2020-05-27]. DOI: 10.1109/ICCSIT.2009.5234856. ISBN 978-1-4244-4519-6.

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

[17] 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.

[18] VANHOEFM, Krackattacks-scripts. GitHub [online]. Dostupné z: https://github.com/vanhoefm/krackattacks-scripts

[19] Alexis. Hping3 – SYN Flooding, ICMP Flooding & Land Attacks. HACKERSPOIT [online]. Dostupné z: https://hsploit.com/hping3-syn-flooding-icmp-flooding-land-attacks/

[20] Kali Linux, Kali:Docs. Dostupné z: https://www.kali.org/docs/

[21] Common Password List (rockyou.txt): Built-in Kali wordlist rockyou.txt[on-line]. Dostupné z: https://www.kaggle.com/wjburns/common-password-list-rockyoutxt

[22] Wireshark[online]. Dostupné z: https://www.wireshark.org

[23] Wireless_scripts: deauthentication_detector.py [online]. Dostupné z: https://github.com/surajsinghbisht054/wireless_scripts/blob/master/deauthentication_detector.py

[24] AIT TCHAKOUCHT, Taha a Mostafa EZZIYYANI. Building A Fast Intrusion Detection System For High-Speed-Networks: Probe and DoS Attacks Detection. *Procedia Computer Science* [online]. 2018, **127**, 521-530 [cit. 2020-05-27]. DOI: 10.1016/j.procs.2018.01.151. ISSN 18770509.