VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav inteligentních systémů

Ing. Matej Kačic

Analýza útokov na bezdrôtové siete

Tézy k dizertačnej práci

Školitel: doc. Dr. Ing. Petr Hanáček

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

Obsah

1 Úvod **5**
1.1 Ciele a prínosy práce 5

2 Návrh systému pre generovanie útokov **6**
2.1 Generovanie rámcov 7

3 Nové využitie zraniteľnosti GTK kľúča **8**
3.1 Transportná vrstva 8
3.2 Popis útoku 9
3.3 Realizácia navrhnutého útoku 10

4 Analýza útokov pomocou reputačného systému **11**
4.1 Architektúra navrhnutého systému 12
4.1.1 Získavanie vstupných dát 13
4.1.2 Identifikácia zariadenia 14
4.1.3 Mobilita entít 15
4.1.4 Vlastnosti komunikácie ovplyvňujúce dôveru 15
4.1.5 Detektory vyšších vrstiev 16
4.2 Výpočet dôvery a reputácie 17
4.3 Reputačné systémy 17
4.4 Základné pojmy 17
4.5 Požiadavky na reputačný systém 18
4.6 Návrh reputačného systému 19
4.7 Formálna definícia výpočtu reputácie 19

5 Experimentálne výsledky **23**
5.1 Výber vhodných metrík pre výpočet dôvery 23
5.2 Existujúce metriky 24
5.3 Vlastné metriky 27
5.4 Detektor vyšších vrstiev 28
5.5 Overenie reputačného systému ako celku 30

Literatúra **33**

Životopis **35**

Abstrakt **37**

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.

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.

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* [7]. 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 [20], 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.

1.1 Ciele a prínosy práce

Táto práca si dáva za cieľ zmapovať existujúce zraniteľnosti a útoky v prostredí bezdrôtových sietí založených na štandarde 802.11i [1] 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.

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.

2 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.

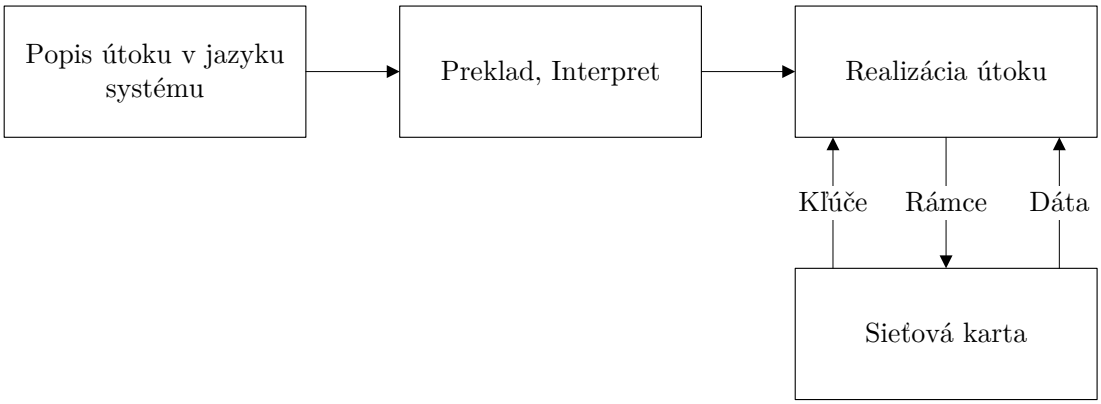
Na základe zistených nedostatkov existujúcich nástrojov bol vytvorený systém, ktorý pomocou pseudojazyka umožňuje jednoducho definovať rámce a celý priebeh rôznych typov útokov. Hlavným nedostatkom väčšiny menovaných nástrojov je absencia užívateľskej definície rámcov štandardu 802.11. Niektoré z nástrojov (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 1.



Obr. 1: Schéma fungovania systému pre generovanie útokov

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* [12].

K realizácii generátora boli využité nástroje YACC a LEX [5]. 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.

2.1 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.Vstupným parametrom funkcie je popis paketu pomocou jazyka Scapy, a musí obsahovať popis jednotlivých častí pomocou hlavičiek, ktoré môžu byť za sebou zreťazené.

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* [6], 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.

Pre šifrovanie dátových rámcov boli použité metódy (WEP, TKIP a CCMP) *Zabezpečenie bezdrôtových sietí*. Pre samotné šifrovanie boli do nástroja zaintegrované časti nástroja aircrack-ng a implementácia metódy CCMP z nasledujúceho zdroja [18].

Navrhuntý 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. 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.

3 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 [2]. Pre úspešnú injekciu je vyžívaná zraniteľnosť *Hole 196* popísaná na začiatku tejto kapitoly. Kompletný postup útoku sme publikovali na konferencii IDAACS 2013 v Berlíne [16].

3.1 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 [11].

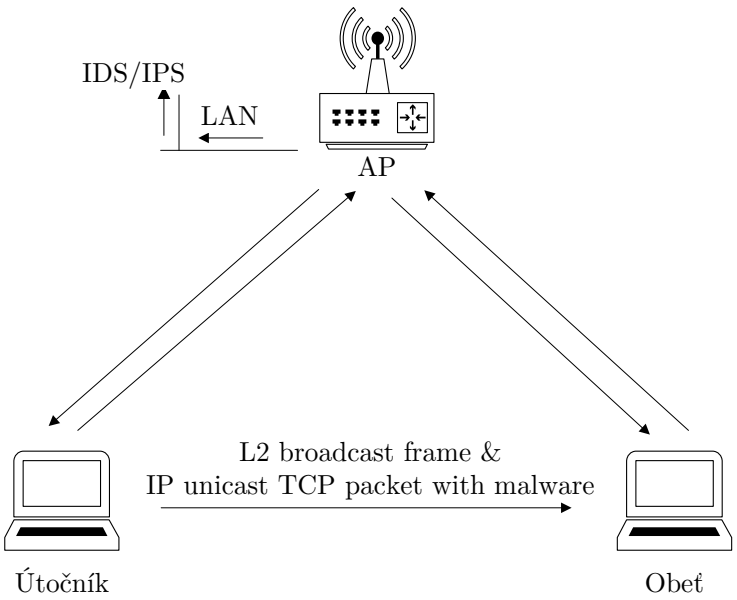
Na tejto vrstve existujú dva protokoly: UDP *(User Datagram Protocol)* a TCP *(Transmission Control Protocol)*. Hlavným účelom TCP protokolu je spoľahlivý prenos medzi dvoma bodmi. K zostaveniu spoľahlivého spojenia medzi dvoma procesmi je použitá technika *three-way handshake*. Najprv klient posiela 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.

3.2 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 2 ukazuje v detaile kroky, ktoré je nutné realizovať k injekcii malware v protokole TCP.



Obr. 2: 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 jednot-

livými 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,

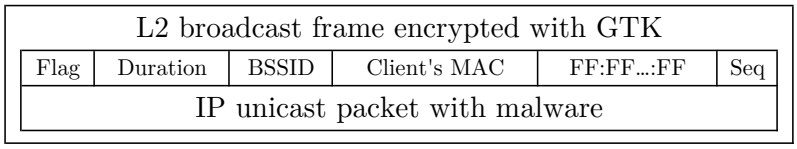
2. dátová časť rámca je definovaná ako unicast IP paket s cieľovou IP adresou obete,

3. IP paket obsahuje dátovú časť, ktorá obsahuje škodlivý kód.

Podarilo sa nám teda vytvoriť všesmerový rámec obsahujúci jednosmerový IP paket (viď obrázok 3). 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. 3: Zapuzdrenie jednosmerového paketu do všesmerového rámca

3.3 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.

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

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

Touto jednoduchou službou sme otestovali injekciu malware bez možnosti detekcie. Aby sme ukázali praktickejšie využitie tohoto princípu vybrali sme si z databáze *exploit-db* [3] 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 [4]. 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. S využitím tohoto princípu je útočníkov pokus úspešný a jeho aktivita nie je detekovaná žiadnym ochranným protiopatrením.

Autor zraniteľnosti [7] 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.

4 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

[1] odpoveď je doručená tradičnou cestou

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.

4.1 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 [15] v Medelíne v roku 2013. Schému navrhnutého systému zobrazuje obrázok 4, 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.

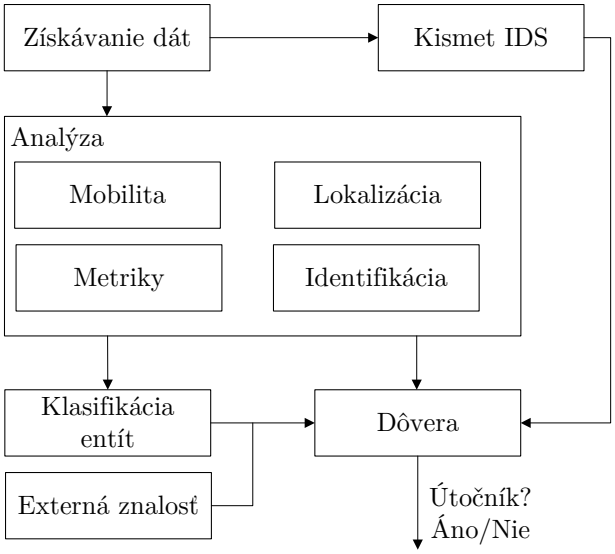
5. Klasifikácia entít – tento modul klasifikuje entity na základe ich správania a ich reputácie, pričom sa ich snaží rozdeliť do niektorých kategórií, ako napríklad administrátor, hosť, zamestnanec sekretárka, prístupový bod, útočník[2].

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.

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



Obr. 4: Architektúra detekčného systému

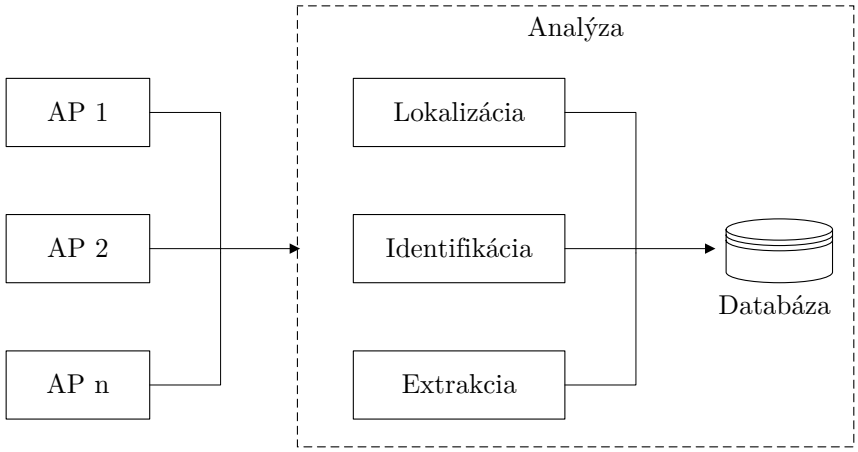
4.1.1 Získavanie vstupných dát

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 5 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. 5: Zobrazenie toku dát v detekčnom systéme

4.1.2 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* [21]:

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 [21].

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.

4.1.3 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 [13].

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:

$$m \in M, M = \{Stationary, Low, Medium, High, VeryHigh\} \tag{1}$$

4.1.4 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 štatistických metódach alebo jednoduchých funkciách. Zdrojom dát pre tieto metriky sú informácie obsiahnuté v každom rámci posielanom po bezdrôtovom médiu.

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

$$f = (id, len, src, dst, bssid, dssid, mac, data), \tag{2}$$

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

Definícia 4.1. Množinu všetkých rámcov f, ktoré vstupujú do systému budeme označovať ako M_f.

$$M_f = \{f_1, f_2, \ldots, f_n\} \tag{3}$$

Definícia 4.2. Definujme postupnosť rámcov R_f, ktorá je definovaná nad množinou rámcov M_f:

$$R_f = \{f_1, f_2, \ldots\}, f_i \in M_f, \tag{4}$$

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

Definícia 4.3. Metrika je teda funkcia ψ, ktorej vstupom je postupnosť rámcov R_f a výstupom je číselná hodnota m.

$$m = \psi(R_f) \tag{5}$$

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 5.1, v ktorej budú experimentálnou metódou vybrané vhodné metriky určené pre výpočet dôvery.

4.1.5 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 [8] *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.

4.2 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.

4.3 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 [22, 10].

4.4 Základné pojmy

Medzi základné pojmy v oblasti reputačných systémov a výpočtu dôvery patria [17, 14]:

- **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.

$$(Alice, Bob, authentication) \in T \tag{6}$$

  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 [19].

- **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.

4.5 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.

4.6 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 4.1.2 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 4.1.

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.

4.7 Formálna definícia výpočtu reputácie

Definícia 4.4. 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.

$$E = \{e_1, e_2, \ldots, e_n\} \tag{7}$$

Definícia 4.5. 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.

$$r_e = \langle 0, 1\rangle \subset \mathbb{R} \tag{8}$$

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.

$$r_e = \frac{1 - R_s}{2} \tag{9}$$

Definícia 4.6. 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.

$$d_p = \langle 0, 1\rangle \subset \mathbb{R} \tag{10}$$

Definícia 4.7. 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.

$$T = \langle 0, 1\rangle \subset \mathbb{R} \tag{11}$$

Definícia 4.8. 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.

$$S_e = a^{n_e} \tag{12}$$

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.

$$\lim_{n_e \to \infty} a^{n_e} = 0 \tag{13}$$

Definícia 4.9. 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.

$$T_{c_{1,n}} = f_i(S_1, \ldots, S_k), 1 \leq k \leq n-1 \tag{14}$$

$$T_{c_{k,n}} = f_n(S_{k-n+1}, \ldots, S_k), k > n \tag{15}$$

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.

$$T_{c_{k,n}} = \frac{\sum_{i=k-n+1}^{k} \beta^{n_i} r_{e_i}(1 - Se_i) d_p}{n}, k > n \tag{16}$$

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 :

$$N_t = \begin{cases} 0.01, & \text{keď } \omega < C_{untrust}; \\ 0.99, & \text{keď } \omega > C_{trust}; \\ 0.98\frac{C_{trust} - \omega}{C_{trust} - C_{untrust}} + 0.01, & \text{inak.} \end{cases} \tag{17}$$

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 [9], ktorý sa zaoberal normalizáciou a dynamikou výpočtu dôvery v reputačných systémoch.

Nová hodnota dôvery sa vypočíta podľa rovnice:

$$T_{new} = \alpha T_{old} + (1 - \alpha) N_t, \tag{18}$$

kde α symbolizuje koeficient zotrvačnosti pôvodnej dôvery voči novo vypočítanej.

Definície 4.4 až 4.9 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. 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.

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.

5 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.

5.1 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:

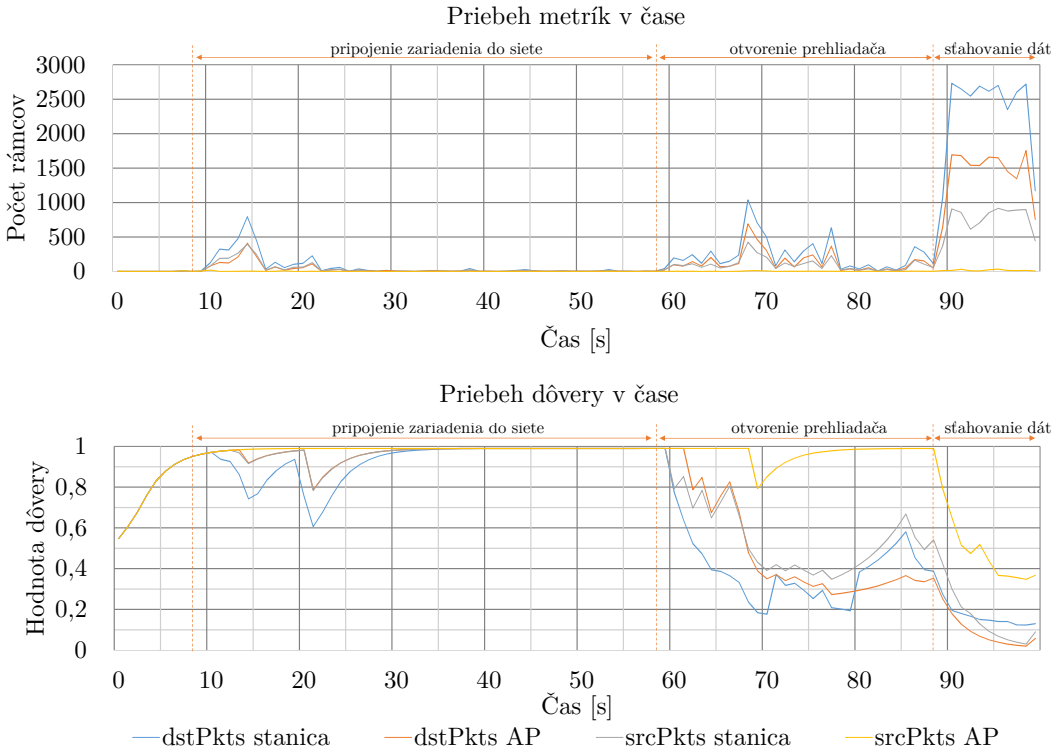
- metrika môže pri bežnej teda validnej komunikácii ovplyvniť hodnotu dôvery takým spôsobom, aby sa výkyvy v aktuálne hodnote dôvery príliš neodlišovali od dlhodobého priemeru týchto hodnôt,
- metrika musí mať istý potenciál pre detekciu útokov alebo výkyvov v správaní danej entity.

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.

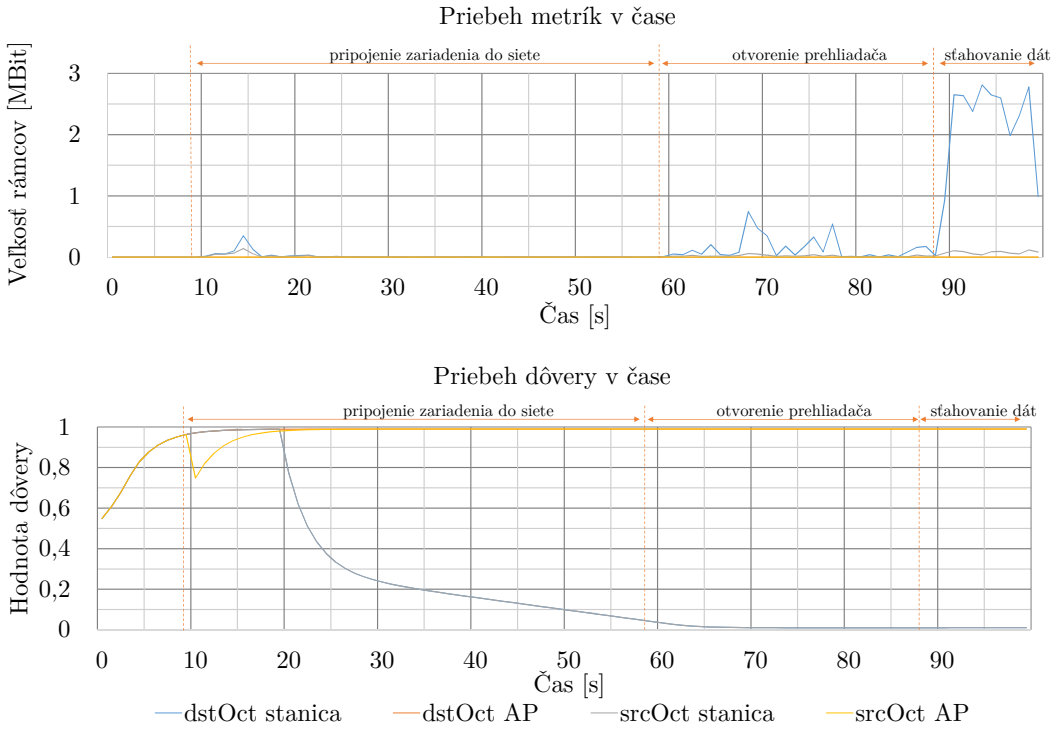
5.2 Existujúce metriky

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 6, 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.



Obr. 6: Vplyv skupiny metrík založených na počte rámcov na vývoj dôvery

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. Celý priebeh experimentu je zobrazený na grafe 7, 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.



Obr. 7: Vplyv skupiny metrík založených veľkosti prenesených dát na vývoj dôvery

Použitie metrík, ktorých vstupom je sila signálu prípadne úroveň rušenia signálu pre pripojené zariadenie v bezdrôtovej sieti ukazuje tabuľka 1,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.

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

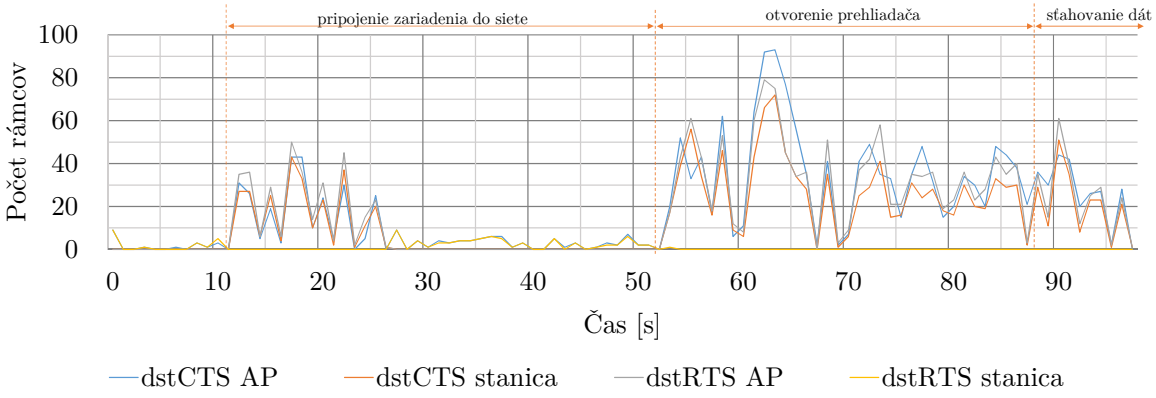
Tabuľka 1: Smerodajné odchýlky sily signálov nameraných v dBm

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 metrík 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 8, 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. 8: 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.

5.3 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.

$$AuthAnomaly(C_d, N_d) = \begin{cases} 1, & \text{keď } Mod(C_d) = N_d; \\ 0, & \text{inak.} \end{cases} \tag{19}$$

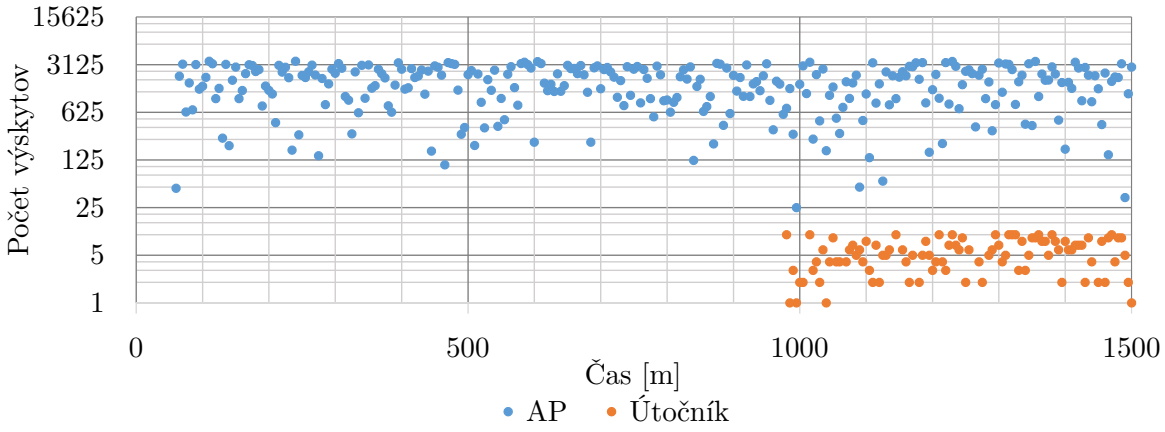
Navrhnutý systém je schopný detekovať zariadenie na základe odtlačku zariadenia. Za tohoto predpokladu je možné implementovať detektor, ktorý bude vracať hodnotu 1 v prípade, že došlo k zmene MAC adresy zariadenia, ktoré už v minulosti malo vytvorený odtlačok. Detektor reaguje i na rámce, ktoré mohli 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*. 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 9 ukazuje počet výskytov metriky *srcFromds* v čase v minútach počas testovania, ktoré bolo odlišné ako v predchádzajúcich prípadoch.

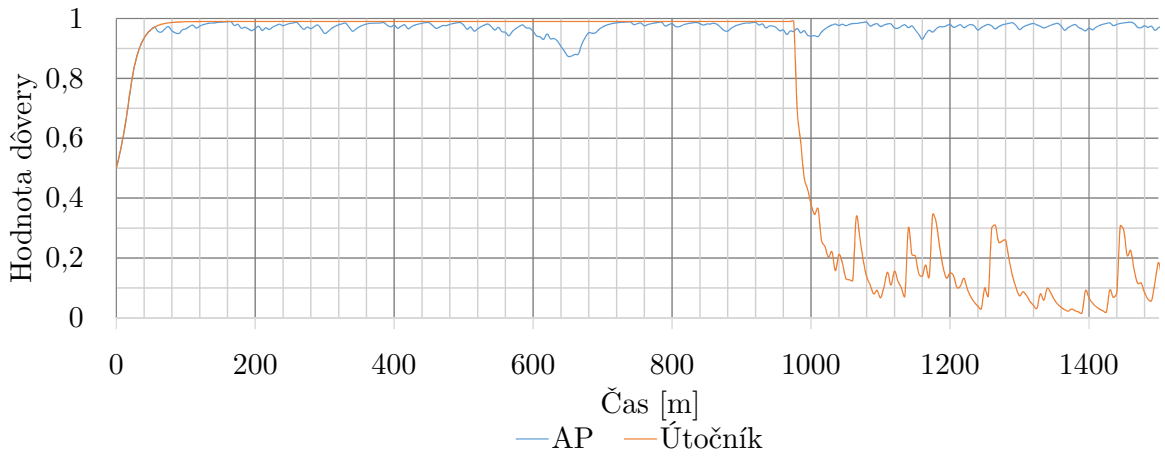
Z grafu môžeme vidieť bežnú prevádzku na WiFi sieti, pričom približne od tisícej minúty generátor zamiešal do validnej komunikácie rámce, ktoré boli súčasťou skrytého útoku na ARP tabuľku pomocou zraniteľnosti *Hole 196*. V tomto prípade sú rámce jasne separovateľné čo by v prípade reálneho prostredia 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 10. Z grafu vyplýva, že metrika reflektuje správne zmeny



Obr. 9: Graf počtu výskytov metriky *srcFromds* detekcie v čase

v správaní stanice pri generovaní rámcov potrebných pre skrytý ARP útok.



Obr. 10: Priebeh dôvery na základe metriky *srcFromds*

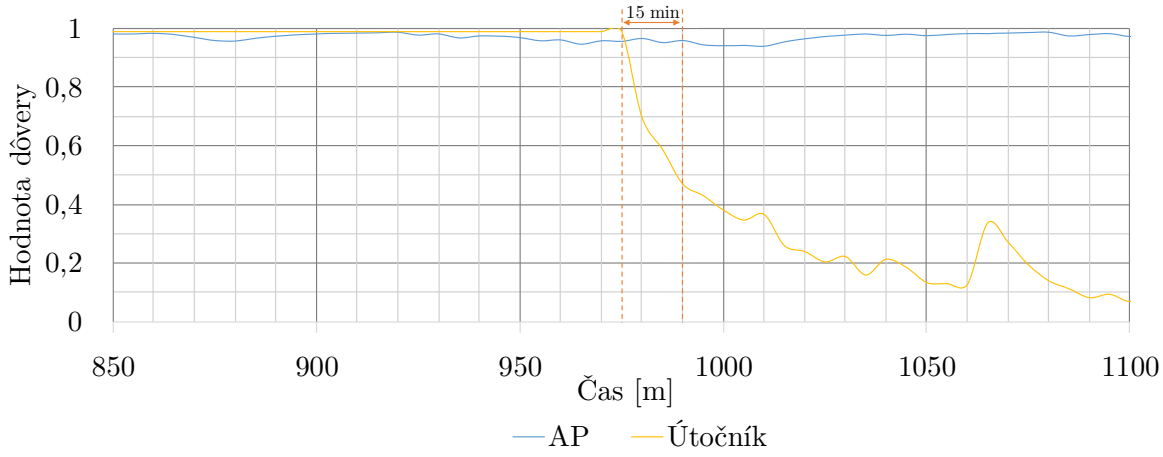
Detail priebehu dôvery metriky *srcFromds* je zobrazený na grafe 11, z ktorého je vidieť, že systém začne vyhodnocovať útočníka ako nedôveryhodného až po približne 15 minútach. Počas tejto doby by za reálnych podmienok ostal útočník nedetekovaný.

5.4 Detektor vyšších vrstiev

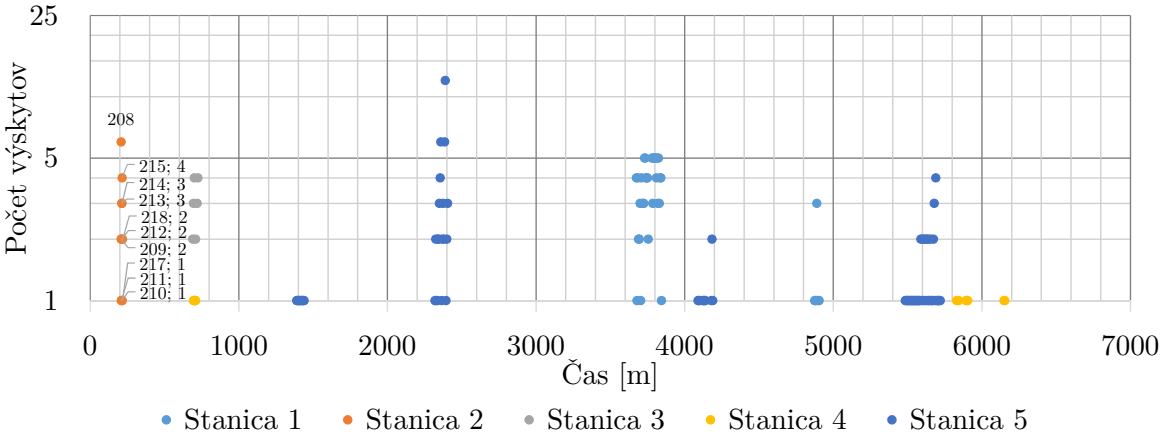
V rámci tejto práce bol implementovaný jednoduchý detektor *Data anomaly*, ktorého vstupom sú dáta z vyšších vrstiev. Detektor odhaľuje anomálny prenos dát jednej entity. Metóda agreguje všetku komunikáciu vedenú z jednej entity na základe cieľových IP adries a kontroluje prekročenie maximálnej povolenej hranice. V prípade dosiahnutia tejto hranice je udalosť poslaná do reputačného systému.

Graf na obrázku 12 zobrazuje počet výskytov tejto udalosti pre 5 rôznych staníc na časovej osi v minútach. Dĺžka vygenerovaných dát bola 5 dní.

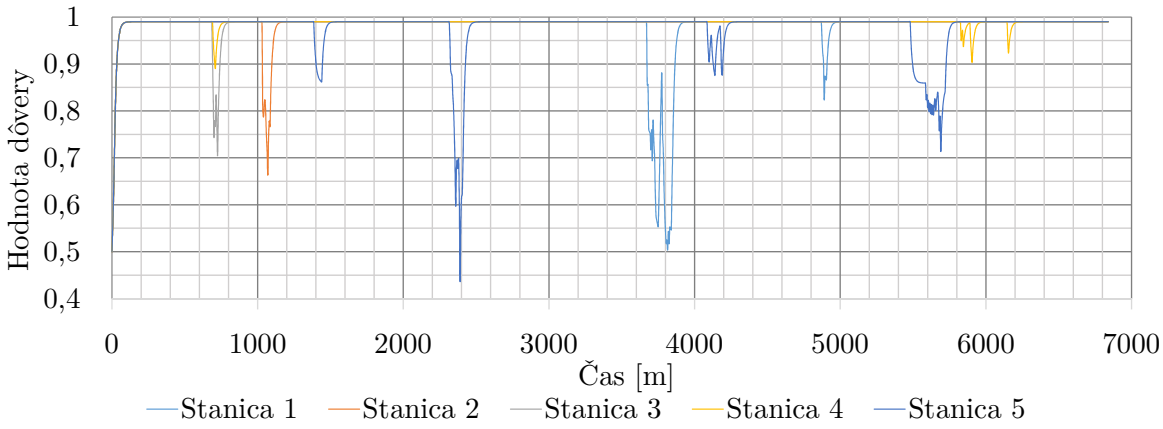
Graf na obrázku 13 zobrazuje priebeh dôvery na základe detektoru *Data anomaly*, kde môžeme vidieť jednotlivé výkyvy v hodnote dôvery. Hodnota dôvery klesala s odpovedajúcim počtom výskytov tejto udalosti, avšak i pri veľkom výskyte neklesla pod úroveň 0.5, teda pod úroveň nedôveryhodnosti.



Obr. 11: Detail priebehu dôvery na základe metriky *srcFromds*



Obr. 12: Graf počtu výskytov detektoru *Data anomaly* detekcie v čase



Obr. 13: Priebeh dôvery na základe detektoru *Data anomaly*

Nasledujúca tabuľka 2 sumarizuje vhodnosť použitia jednotlivých metrík pre výpočet dôvery zariadenia, pričom rozlišujeme metriky prebrané z existujúcich výskumov a metriky vytvorené počas tejto práce.

Táto časť experimentov sa venovala výberu vhodných metrík pre výpočet hodnoty

	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 2: Prehľad vhodnosti použitia metrík pre výpočet dôvery

dôvery. Nasledujúca časť bude venovaná overovaniu všetkých vhodných metrík ako celku pri výpočte hodnoty dôvery.

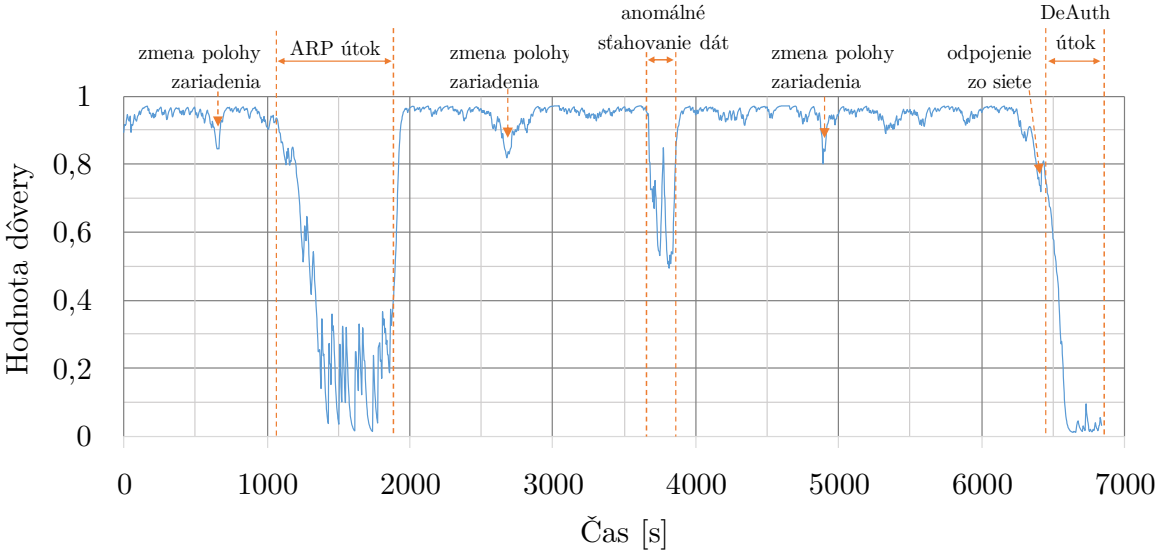
5.5 Overenie reputačného systému ako celku

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 **??** *Analýza útokov vydávajúcich sa za prístupový bod* ukážka **??**, kde sa jednalo o využitie zraniteľnosti GTK kľúča k ovplyvneniu záznamu v ARP tabuľke obete. Druhým útokom bol útok na dostupnosť popísaný v kapitole **??** *Analýza útokov s dopadom na dostupnosť* pomocou deautentizácie stanice.

Graf 14 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.

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



Obr. 14: Priebeh dôvery v čase pri použití viacerých metrík

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 odlišného 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 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.

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

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

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

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

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

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

[8] Barabas, M.; Homoliak, I.; Kacic, M.; aj.: Detection of network buffer overflow attacks: A case study. In *Security Technology (ICCST), 2013 47th International Carnahan Conference on*, IEEE, 2013, s. 1–4.

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

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

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

[12] 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.

[13] 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.

[14] 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.

[15] Kacic, M.; Hanacek, P.; Henzl, M.; aj.: A concept of behavioral reputation system in wireless networks. In *Security Technology (ICCST), 2013 47th International Carnahan Conference on*, IEEE, 2013, s. 1–5.

[16] Kacic, M.; Hanacek, P.; Henzl, M.; aj.: Malware injection in wireless networks. In *Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), 2013 IEEE 7th International Conference on*, ročník 1, IEEE, 2013, s. 483–487.

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

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

[19] 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.

[20] 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.

[21] 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.

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

Životopis

Osobné údaje

Meno:	Matej Kačic
Národnosť	slovenská
Dátum narodenia	3. marca 1986
E-mail:	ikacic@fit.vutbr.cz
Web:	www.fit.vutbr.cz/ ikacic

Vzdelanie

od 2010	Fakulta informačních technologií VUT v Brně, doktorský študijny program Výpočetní technika a informatika
2008 – 2010	Fakulta informačních technologií VUT v Brně, magisterský študijny program Informační technologie, DP: Systém řízení dopravy
2005 – 2008	Fakulta informačních technologií VUT v Brně, bakalársky študijny program Informační technologie, BP: Aplikace pro odhalování plagiátů u rozsáhlých projektů
2001 – 2005	Gymnázium Pierra de Coubertina, Piešťany, Slovensko

Kariéra

od 2016	Architekt bezpečnonsti, AEC a.s., návrh bezpečnostných opatrení v korpotátnom prostredí
2014 – 2016	Senior IT bezpečnostní konzultant, AEC spol. s r.o., Počítačová bezpečnost, audit operačních systémů, penetrační testování, pokročilé bezpečnostní technologie
2010 – 2014	Technický a výzkumný pracovník, Fakulta informačních technologií VUT v Brně

Publikácie

3 publikácie v DBLP
7 publikácií v Scopus
1 publikácie v recenzovanom neimpaktovanom priodiku (DSM 1211-8737)
9 publikácií na medzinárodnej konferencii
2 publikácie v medzinárodnom časopise
4 citácie

Projekty

Spolehlivost a bezpečnost v IT, VUT v Brně, FIT-S-14-2486, 2014-2016
Pokročilé bezpečné, spolehlivé a adaptivní IT, VUT v Brně, FIT-S-11-1, 2011-2013
Bezpečné a spolehlivé počítačové systémy, VUT v Brně, FIT-S-17-4014, FIT-S-17-4014, 2017-2019

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.