VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Průzkum a ověření možností proaktivního vyhledávání bezdrátových sítí

Wireless Network and Proactive Scanning - Survey and Verification

2014 Jakub Jelínek

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Jakub Jelínek**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: Průzkum a ověření možností proaktivního vyhledávání bezdrátových sítí
Wireless Network and Proactive Scanning - Survey and Verification

Zásady pro vypracování:

Cílem práce je průzkum a ověření možností konfigurace a vyhledávání bezdrátových sítí s pomocí nástroje *iw* v prostředí GNU/Linux. Práce se zaměří především na proaktivní vyhledávání sítí na pozadí probíhající bezdrátové komunikace a využití získaného výsledku pro rychlou reasociaci v případě ztráty spojení s aktuálním přístupovým bodem. Pro účely demonstrace vznikne aplikace, která na základě proaktivního skenování vyvolá rychlou reasociaci.

1. Seznamte se s problematikou komunikace v prostředí bezdrátových sítí standardu 802.11 a nástrojem *iw* ve vhodné distribuci GNU/Linux.
2. Navrhněte a sestavte vhodné prostředí pro provádění proaktivního vyhledávání. Vyberte vhodný software a navrhněte metodiku pro prokázání vlivu vyhledávání sítí na probíhající komunikaci.
3. Navrhněte a implementujte aplikaci, která při ztrátě spojení využije výsledků vyhledávání sítí na pozadí k jeho rychlé obnově.
4. Zhodnotě dosažené výsledky.

Seznam doporučené odborné literatury:

GAST, Matthew. 802.11 wireless networks: the definitive guide. 2, illustrated. USA : O Reilly Media, Inc.,, 2005. 630 s. ISBN 9780596100520.
GORANSSON, Paul; GREENLAW, Raymond. Secure roaming in 802.11 networks. illustrated. USA : Newnes, 2007. 343 s. ISBN 9780750682114.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Martin Milata**

Datum zadání: 18.11.2011
Datum odevzdání: 07.05.2014

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Čestne prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením Ing. Martina Milatu. Uviedol som všetky literárne zdroje a publikácie, z ktorých som čerpal.

V Ostrave dňa 10. 4. 2014

.....

Jakub Jelínek

Poďakovanie

Ďakujem svojmu konzultantovi Ing. Martinovi Milatovi za cenné rady a pripomienky k bakalárskej práci.

Abstrakt

Práca sa zaoberá prieskumom a overením možností proaktívneho vyhľadávania sietí na pozadí prebiehajúcej bezdrôtovej komunikácie a využitím získaného výsledku pre rýchlu reasociáciu pri strate signálu s aktuálnym prístupovým bodom. V práci sa zoznámime so štandardom 802.11 pre bezdrôtové siete, problematikou vplyvu vyhľadávania bezdrôtových sietí na prebiehajúcu komunikáciu a nástrojom iw pre GNU/Linux. Zostavíme vhodné prostredie pre prevádzanie proaktívneho vyhľadávania, navrhneme metodiku pre preukázanie vplyvu vyhľadávania sietí na prebiehajúcu komunikáciu a implementujeme aplikáciu, ktorá pri strate spojenia využije výsledky vyhľadávania na pozadí k naviazaniu spojenia s najvhodnejším prístupovým bodom.

Kľúčové slová: Proaktívne vyhľadávanie; Bezdrôtové siete; Wi-Fi; iw Linux; Reasociácia

Abstract

This bachelors thesis deals with possibilities of proactive scanning in the background of ongoing wireless communication and utilizing obtained results for fast reassociation in case of lost signal with actual access point. In this thesis we will get familiar with 802.11 standard for wireless networks, impact of scanning on ongoing wireless communication and iw tool for GNU/Linux. We will set up an environment suitable for proactive scanning, suggest a method to demonstrate the impact of network scan on ongoing wireless communication and implement an application, which in case of lost connection will utilize obtained results for establishing connection with best available access point.

Keywords: Proactive scanning; Wireless networks; Wi-Fi; iw Linux; Reassociation

Zoznam použitých skratiek a symbolov

AP	–	Access Point
BSA	–	Basic Service Area
BSS	–	Basic Service Set
CLI	–	Command Line Interface
GNU	–	GNU's Not Unix
IBSS	–	Independent Basic Service Set
ICMP	–	Internet Control Message Protocol
IDE	–	Integrated Development Environment
IEEE	–	Institute of Electronics and Electical Engineers
LTS	–	Long Term Support
MAC	–	Media Access Control
OSI Model	–	Open Systems Interconnection Model
SSID	–	Service Set Identifier
TCP/IP	–	Transmission Control Protocol/Internet Protocol
USB	–	Universal Serial Bus
WEP	–	Wired Equivalent Privacy
Wlan	–	Wireless Local Area Network

Obsah

Seznam tabulek

Seznam obrázků

Zoznam výpisov zdrojového kódu

1 Úvod

Internet sa dnes stáva takmer nevyhnutným pre využitie všetkých funkcií prenosných zariadení. Zariadenia ako napríklad notebooky, tablety a mobilné telefóny sú dnes bežne vybavené bezdrôtovou sieťovou kartou. Naviac, s nástupom nových mobilných zariadení a ich podporou rozličných služieb sa zvyšujú nároky na kvalitu bezdrôtového pripojenia.

Podstatou riešeného problému je, že rýchlosť a odozva siete sa mení polohou k aktuálne pripojenému prístupovému bodu. Rozhodnutie, kedy sa prepojiť na vhodnejší prístupový bod záleží od použitého hardvéru a softvéru. Tieto riešenia sú často proprietárne[1] a v závislosti na kvalite implementácie niektoré fungujú lepšie, iné horšie. V mnohých prípadoch nastáva nadviazanie spojenia s vhodnejším prístupovým bodom až pri úplnej strate signálu.

Cieľom práce je overiť možnosti vyhľadávania dostupných bezdrôtových sietí na pozadí pomocou nástroja `iw` vo vhodnej distribúcii GNU/Linux. Ďalej zistiť, aký vplyv bude mať vyhľadávanie na pozadí pre prebiehajúcu komunikáciu a implementovať aplikáciu, ktorá pri strate spojenia využije výsledky vyhľadávania na pozadí pre jeho rýchlu obnovu.

V tejto práci chcem preskúmať, navrhnúť a otestovať riešenia proaktívneho vyhľadávania na pozadí, ktoré bude mať minimálny, alebo najlepšie žiadny negatívny vplyv na aktuálne prebiehajúcu komunikáciu a umožní rýchle prepojenie na vhodnejší prístupový bod. Za účelom demonštrácie a využitia navrhnutých riešení v praxi chcem implementovať aplikáciu, ktorá bude monitorovať bezdrôtové sieťové rozhranie a na základe získaných informácií rozhodne, kedy nastane prepojenie na iný prístupový bod.

[1] Proprietárny softvér alebo tiež softvér s uzavretým kódom.

2 Teoretická časť

V tejto časti si vysvetlíme, čo znamená pojem proaktívne vyhľadávanie, oboznámime sa so sieťovým štandardom IEEE 802.11 a problémom vyhľadávania dostupných sietí na pozadí už prebiehajúcej komunikácie.

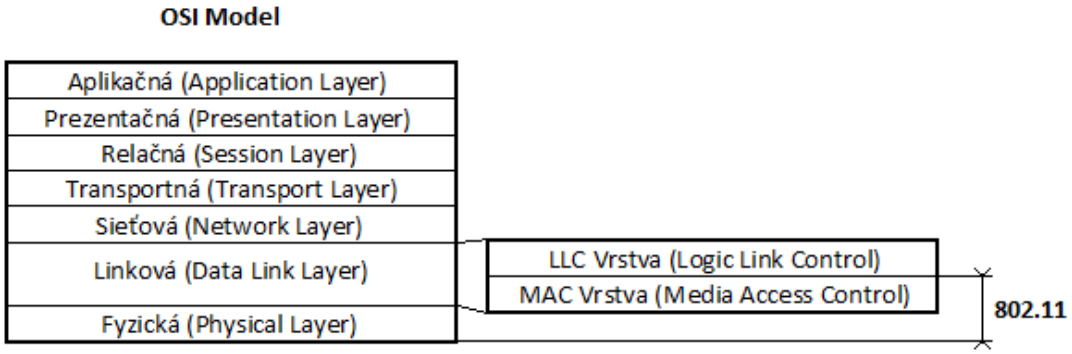
2.1 Proaktívne vyhľadávanie

Proaktivita - Reagovať dopredu, preventívne. Reagovať ešte predtým, ako sa niečo stane. [4]

Proaktívne vyhľadávanie v našom prípade znamená, že budeme dopredu, teda preventívne, skenovať dostupné siete, aby sme sa uistili, že aktuálny prístupový bod je najvhodnejší, alebo mohli v prípade prudkého zhoršenia signálu, či jeho úplnej straty okamžite reagovať.

2.2 Bezdrôtové siete IEEE 802.11

IEEE 802.11 je štandard bezdrôtových lokálnych sietí (wlan) s ďalšími doplnkami vyvíjaný skupinou Institute of Electrical and Electronic Engineers (IEEE). Tento štandard definuje špecifikácie pre fyzickú vrstvu a MAC podvrstvu linkovej vrstvy OSI Modelu. Pre lepšie pochopenie vzťahu 802.11 a OSI Modelu pozri obrázok 1. Štandard 802.11 zahŕňa niekoľko druhov modulácie, ktorých prehlaď nájdete v tabuľke 1.[6]



Obrázek 1: 802.11 a OSI Model [6]

2.3 Hlavné komponenty bezdrôtových sietí

IEEE 802.11 je súbor štandardov pre bezdrôtové lokálne siete. Tieto siete sa môžu skladať zo štyroch komponentov:

- **Stanice** - Siete sa stavajú kvôli dátovému prenosu medzi stanicami. Stanice sú výpočtové zariadenia s bezdrôtovým sieťovým rozhraním. Typicky sú tieto zariadenia

napájané batériou ako napríklad notebook alebo tablet. Neexistuje ale žiaden dôvod, pre ktorý by museli byť tieto stanice prenosné. V niektorých podmienkach sa používajú stolné počítače vybavené bezdrôtovou sieťovou kartou, aby sa predišlo nutnosti zavádzať novú kabeláž. [1]

Štandard	Rok uvedenia	Pásmo [GHz]	Maximálna teoretická rýchlosť [Mbit/s]
IEEE 802.11	1997	2,4	2
IEEE 802.11a	1999	5	54
IEEE 802.11b	1999	2,4	11
IEEE 802.11g	2003	2,4	54
IEEE 802.11n	2009	2,4 alebo 5	600
IEEE 802.11ac	2013	5	1000

Tabulka 1: Prehľad štandardov IEEE 802.11

- **Prístupové body** - Rámce siete 802.11 sa musia prekonvertovať na iný typ rámcov pre prenos do zvyšku sveta. Zariadenia nazývané prístupové body vykonávajú túto funkciu konvertovaním (premosťovaním) signálu. Prístupové body vykonávajú aj iné funkcie, ale premosťovanie je jednou z najdôležitejších. Prístupový bod sa obvykle pripája k sieti typu ethernet, čo umožňuje prenášať dáta medzi bezdrôtovými a drôtovými zariadeniami. Dôležitá úloha je aj zabezpečenie komunikácie medzi jednotlivými klientmi rovnakého prístupového bodu, pri ktorej ku konverzií signálu nedochádza. [1]

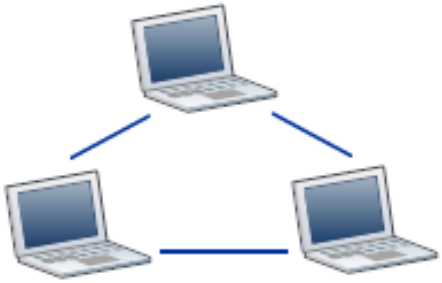
Obrázek 2: Hlavné komponenty siete 802.11 [1]

- **Bezdrôtové médium** - Štandard 802.11 používa na prenos rámcov medzi zariadeniami elektromagnetické vlnenie (umožňuje aj prenos pomocou infračerveného spektra, ale bezdrôtová komunikácia pomocou elektromagnetického vlnenia sa presadila oveľa viac). [1]
- **Distribučný systém** - Vo väčšine komerčných produktov je distribučný systém implementovaný ako kombinácia premosťovacieho systému a distribučného média. Takúto sieť, ktorá prepája prístupové body, voláme `backbone network` a väčšinou býva zrealizovaná technológiou ethernet. [1]

2.4 Typy bezdrôtových sietí podľa operačného módu

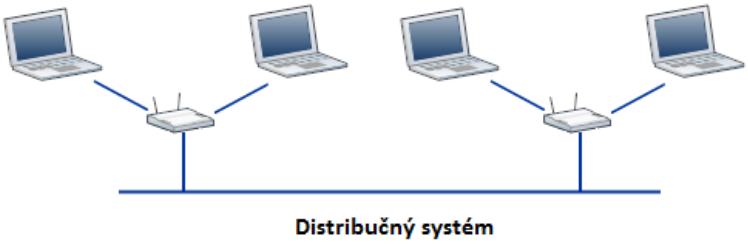
Bezdrôtová sieť môže byť podľa potrieb užívateľov alebo požadovaných funkcií vybudovaná rôznymi spôsobmi. Základný stavebný blok bezdrôtových sietí je BSS (Basic Service Set). Jedná sa o množinu staníc, ktoré spolu komunikujú v určitej oblasti, ktorá sa nazýva BSA (Basic Service Area). Veľkosť tejto oblasti je závislá na dosahu signálu jednotlivých členov BSS. Podľa toho, ako prebieha komunikácia medzi jednotlivými stanicami BSS, rozlišujeme dve rôzne topológie sietí: [1]

- **Independent BSS** - Independent BSS (IBSS) alebo tiež Ad-hoc sieť pozostáva z jednotlivých staníc, prepojených medzi sebou priamo. Na takejto bezdrôtovej sieti nie je k dispozícii žiadny prístupový bod, ktorý by sieť riadil, čo znamená, že všetky stanice pripojené k takejto sieti sú si rovné. Najmenšiu takúto sieť môžeme vytvoriť, ak máme k dispozícii aspoň dve stanice s bezdrôtovou sieťovou kartou. Siete typu Ad hoc majú využitie hlavne vtedy, ak chceme vytvoriť dočasnú sieť a po splnení účelu býva spojenie ukončené. [1]



Obrázek 3: Independent BSS [1]

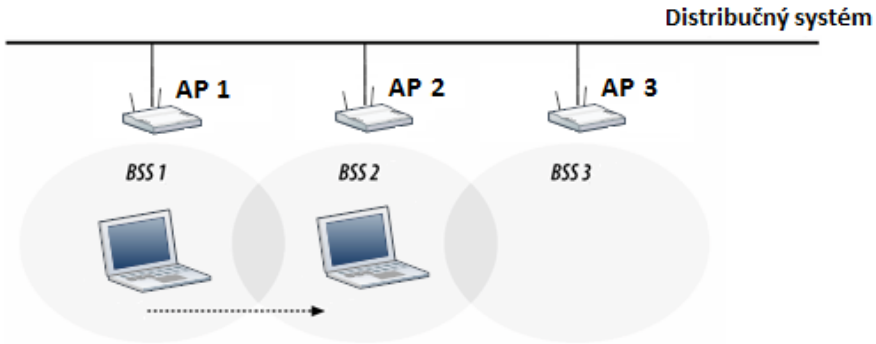
- **Infrastructure BSS** - Pre vytvorenie Infrastructure BSS siete potrebujeme prístupový bod (AP), cez ktorý prebieha všetka komunikácia, vrátane komunikácie medzi jednotlivými stanicami v rovnakej servisnej oblasti (BSA). To znamená, že ak chcú stanice v takejto oblasti spolu komunikovať, komunikácia prebieha v dvoch krokoch. Stanica najprv pošle rámec prístupovému bodu, ten potom prepošle tento rámec stanici, ktorej bol rámec adresovaný. Aj keď je takáto komunikácia náročnejšia na prenosovú kapacitu, prináša viacero výhod. Dosah takejto siete je definovaný dosahom prístupového bodu, vďaka čomu je možné komunikovať na väčšie vzdialenosti, pretože stanice, ktoré spolu komunikujú, nemusia byť medzi sebou v dosahu. [1]



Obrázek 4: Infrastructure BSS [1]

2.5 Roaming

Jedná sa o plynulé prechádzanie medzi prístupovými bodmi. Aby bol takýto prechod možný, prístupové body musia byť v rovnakej sieti. Rozhodnutie, kedy sa asociovať s iným prístupovým bodom, závisí čisto na klientovi. Štandard 802.11 nešpecifikuje, kedy alebo ku ktorému prístupovému bodu by sa mal klient pripojiť. Algoritmy roamingu sa preto líšia sieťovou kartou, firmvérom alebo použitým softvérom. [5]



Obrázek 5: Roaming [1]

2.5.1 Rámce v 802.11

V bezdrôtových sieťach 802.11 odvysielané rámce spadajú do troch kategórií:

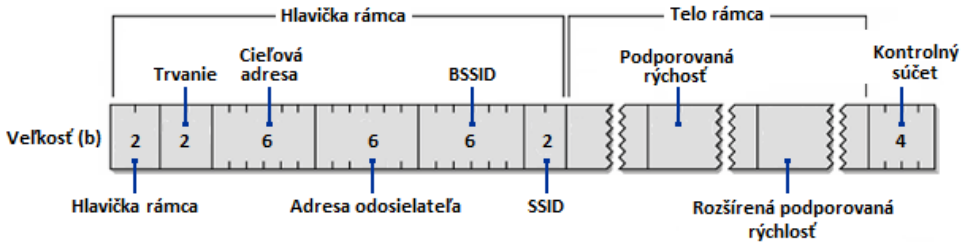
Control Frames - Asistujú pri doručovaní dátových rámcov medzi stanicami a zabraňujú kolíziám.

Data Frames - Väčšina dátových rámcov prenáša dáta do iných vrstiev OSI modelu, no sú aj výnimky, keď `Data Frames` rámce neobsahujú takéto dáta a majú iný účel.

Managemen Frames - Management rámce nás v tejto práci zaujímajú najviac, lebo infor-

mujú o dostupných sieťach a slúžia na asociáciu či autentifikáciu. Z management rámcov sú pre nás najzaujímavejšie tieto:

- **Beacon Frames** - Beacon rámce oznamujú existenciu prístupového bodu a zohrávajú dôležitú úlohu vo viacerých službách údržby. Sú vysielané v pravidelných intervaloch, aby stanice podľa nich mohli nájsť a identifikovať prístupové body pre pripojenie do siete. Obsahujú informácie o sieťach ako BSSID, SSID a podporované prenosové rýchlosti. [5]
- **Probe Request** - Tento typ rámcov používajú mobilné stanice na aktívny sken. Obsahuje dve dôležité časti: SSID a podporované prenosové rýchlosti. Ak probe request obsahuje špecifické SSID, na túto požiadavku odpovedajú iba prístupové body s takýmto SSID. Ak klient pošle probe request, ktorý obsahuje nulové SSID, na túto požiadavku odpovedajú všetky prístupové body, ktoré ju obdržia. [5]
- **Probe Response** - Ak Probe Request zachytí sieť s kompatibilnými parametrami, odpovie naň rámcom typu Probe Response. Probe Response rámce majú podobnú štruktúru ako beacon rámce. [5]



Obrázek 6: Štruktúra Probe Request rámca [1]

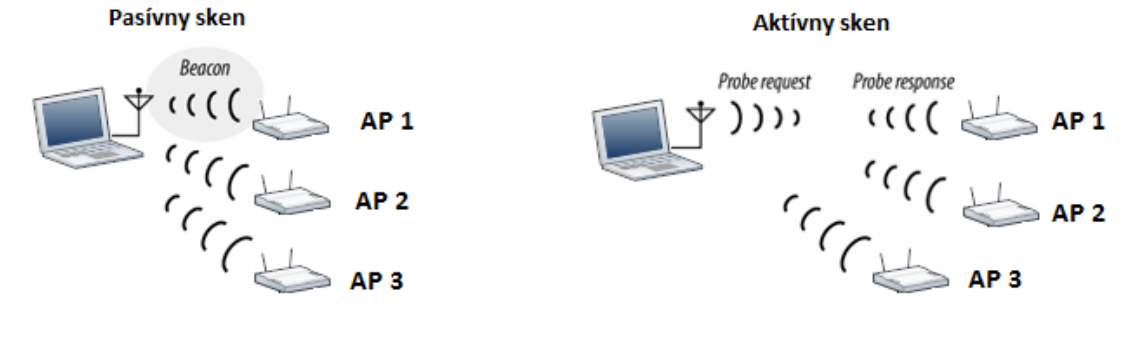
2.6 Skenovanie wlan sietí

Klienti bezdrôtových sietí sa o dostupných prístupových bodoch môžu dozvedieť skenovaním príslušných kanálov. Sken môže byt aktívny alebo pasívny.

Počas skenovania klient nemôže odosielať ani prijímať iné dáta. Je viacero prístupov, ktorými sa dá tento vplyv skenovania na klientské dáta minimalizovať. Jeden zo spôsobov je naskenovať iba jeden alternatívny kanál v jednom čase a obnoviť predošlú komunikáciu (skenovanie jedného kanálu spôsobí iba minimálne prerušenie komunikácie) a takto postupne prejsť všetky dostupné frekvencie. Ďalšia možnosť je skenovať dostupné siete v čase, keď sa aktívne neprenášajú žiadne dáta. Posledná možnosť je skenovať dostupné siete iba ak je to nevyhnutné (napríklad pri strate signálu). [5]

2.6.1 Pasívny sken

Klient sa prepne na skenovaný kanál a čaká na periodické beacon rámce odvysielané prístupovými bodmi na danom kanáli. Prístupové body posielajú periodické beacon rámce približne každých 100 milisekúnd, čo je celkom dlhá doba. Ak by sme chceli preskenovať viac kanálov naraz, zaberie to dlhú dobu, počas ktorej klient musí prerušiť príjem/odosielanie iných dát. Keď zase skrátime dobu skenovania jednotných kanálov, môže sa stať, že beacon rámce niektorých prístupových bodov vôbec nezachytíme. [5]



Obrázek 7: Pasívny a aktívny sken [1]

2.6.2 Aktívny sken

Klient sa prepne na skenovaný kanál, odvysiela probe request a počká na odpoveď prístupových bodov (alebo na beacon rámce), ktoré sú na skenovanom kanáli. Štandard 802.11 nešpecifikuje ako dlho by mal klient čakať, ale 10 milisekúnd by malo vo väčšine prípadov stačiť. [5]

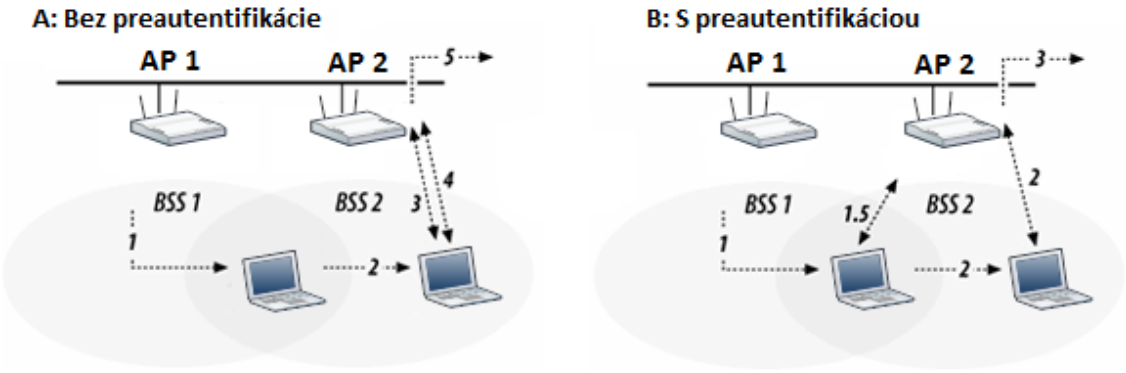
2.7 Naviazanie spojenia s wlan sieťou

Po naskenovaní bezdrôtových sietí sa stanica môže pokúsit'o pripojenie. Do ktorej siete sa pripojí, závisí na preferenciách stanice alebo rozhodnutí užívateľa. Pre získanie prístupu do siete je potrebná autentifikácia a asociácia.

- **Autentifikácia** - Pre naviazanie spojenia s bezdrôtovou sieťou sa klient musí najprv autentifikovať. Je to proces, pri ktorom klient pošle svoju identitu prístupovému bodu. Takáto prvotná (nízkoúrovňová) autentifikácia ešte neznamená žiadne zabezpečenie a slúži iba k prvému kroku pripojenia k bezdrôtovej sieti. So správnou metódou EAP zabezpečenia môže byť autentifikácia k sieti veľmi silná, ale takáto rozšírená forma autentifikácie vyžaduje, aby najprv prebehla tá nízkoúrovňová. [1]
- **Preautentifikácia** - Preautentifikácia sa používa na urýchlenie asociácie s bezdrôtovou sieťou . Autentifikácia môže často spôsobit'dlhší výpadok spojenia pri prepájaní

medzi prístupovými bodmi. Stanice sa počas skenu môžu takto autentifikovať s viacerými prístupovými bodmi a v prípade potreby okamžite asociovať s novým prístupovým bodom.[1]

- **Asociácia** - Ak autentifikácia prebehla úspešne, stanica sa môže asociovať s daným prístupovým bodom na získanie plného prístupu k sieti. Po úspešnej asociácii prístupový bod zaregistruje pripojené zariadenie do siete. Klient môže byt v jednom čase asociovaný iba s jedným prístupovým bodom. [1]



Obrázek 8: Úspora času pri preautentifikácií [1]

Krok	Bez preautentifikácie	S preautentifikáciou
0	Stanica je asociovaná s AP1	Stanica je asociovaná s AP1
1	Stanica sa dostane do prieniku signálov AP1 a AP2	Stanica sa dostane do prieniku signálov AP1 a AP2 a detekuje prítomnosť AP2
1.5	-	Stanica sa preautentifikuje s AP2
2	AP2 má lepší signál, stanica sa rozhodne prepojiť k AP2	AP2 má lepší signál, stanica sa rozhodne prepojiť k AP2
3	Stanica sa autentifikuje s AP2	Stanica sa pripojí k sieti
4	Stanica sa asociuje s AP2	-
5	Stanica sa pripojí k sieti	-

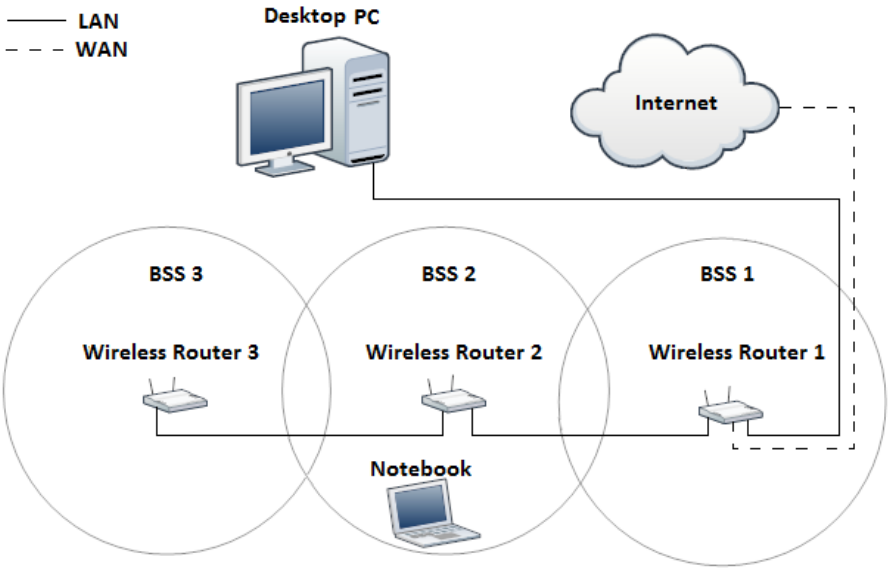
Tabulka 2: Vysvetlenie jednotlivých krokov k obrázku číslo 8. [1]

3 Experimentálna časť

Z teoretickej časti tejto práce (časť 2.6) vieme, že pri skenovaní bezdrôtových sietí musí klient prerušiť aktuálne odosielané aj prijímané dáta. V tejto časti práce navrhneme vhodné prostredie pre realizáciu proaktívneho vyhľadávania, oboznámime sa s nástrojom `iw` na prevádzanie vyhľadávania, navrhneme vhodnú metodiku na preukázanie vplyvu vyhľadávania na prebiehajúcu komunikáciu a zrealizujeme samotné testy.

3.1 Fyzická topológia testovacej siete

K praktickej časti tejto práce potrebujeme vytvoriť sieť vhodnú na prevádzanie proaktívneho vyhľadávania a otestovať vplyv samotného vyhľadávania na prebiehajúcu komunikáciu. Ďalej potrebujeme výsledky proaktívneho vyhľadávania využiť na rýchle obnovenie spojenia v prípade straty signálu s aktuálnym prístupovým bodom. Naša testovacia sieť by sa preto mala skladať minimálne z dvoch prístupových bodov, ktorých dosah (BSA) sa bude aspoň čiastočne prekrývať a dve stanice (jedna z nich musí byť vybavená bezdrôtovou sieťovou kartou), ktoré budú cez bezdrôtové spojenie medzi sebou komunikovať. Návrh zapojenia siete, ktorá spĺňa naše požiadavky, je na obrázku číslo 9.



Obrázek 9: Návrh fyzického zapojenia siete

3.2 Nastavenie zariadení testovacej siete

Po zapojení siete je potrebné nakonfigurovať pripojené zariadenia. `Wireless Router 1` bude slúžiť ako internetová brána, server DHCP a prvý bezdrôtový prístupový bod. Kedže máme nastavené pevné IP adresy, server DHCP nevyužijeme. Bude ale zapnutý v

prípade potreby pripojenia iného zariadenia do siete. Aby sme predišli konfliktom ako obsadenie IP adresy niektorého zo zariadení nastaveného na pevnú IP adresu, server DHCP bude prideľovať adresy v rozsahu 192.168.1.10 až 192.168.1.254. `Wireless Router 2` a `Wireless Router 3` budú slúžiť iba ako bezdrôtové prístupové body. Všetky zariadenia v sieti budú mať nastavenú pevnú IP adresu. Pre prehľadnejšiu konfiguráciu siete pozri tabuľku 3.

Zariadenie	IP Adresa	Subnet	DHCP Server	Wlan SSID	Internetová brána	Zabezpečenie
Wireless Router 1	192.168.1.1	255.255.255.0	áno	WiFi1	áno	WEP
Wireless Router 2	192.168.1.2	255.255.255.0	nie	WiFi2	nie	WEP
Wireless Router 3	192.168.1.3	255.255.255.0	nie	WiFi3	nie	WEP
Destkop PC	192.168.1.4	255.255.255.0	-	-	-	-
Notebook	192.168.1.5	255.255.255.0	-	-	-	-

Tabulka 3: Konfigurácia zariadení

3.3 Použité nástroje

3.3.1 Nástroje na meranie kvality bezdrôtového spoja

Na určenie kvality bezdrôtového spoja budeme merať jeho dva parametre: čas odozvy a rýchlosť prenosu dát . Na určenie odozvy siete použijeme nástroj `ping` a rýchlosť prenosu budeme merať nástrojom `iperf`.

3.3.1.1 ping Nástroj `ping` je základný diagnostický nástroj, ktorým môžeme otestovať funkčnosť a odozvu TCP/IP sietí. Spravidla býva súčasťou väčšiny operačných systémov a jeho funkcia je všade rovnaká. Nástroj ping vyšle ICMP požiadavku „echo request“ na špecifikovanú ip adresu a čaká, či mu dané zariadenie odpovie.

3.3.1.2 iperf `Iperf` je nástroj na meranie rýchlosti a kvality sieťového prepojenia. Tento nástroj sa dá veľmi ľahko nainštalovať na akýkoľvek UNIX/Linux alebo MS Windows operačný systém. Parametre pripojenia sa určujú medzi dvoma počítačmi, na ktorých máme spustený `iperf`. Na jednom počítači musí byť iperf spustený ako server a na druhom ako klient.

3.3.2 Wireshark - Monitorovanie sieťovej prevádzky

Nástroj `Wireshark` je protokolový analyzér a paketový sniffer. Medzi jeho najčastejšie využitie patrí analýza a ladenie problémov v počítačových sieťach, vývoj software, vývoj komunikačných protokolov a štúdium sieťovej komunikácie. Zachytené dáta sa dajú prechádzať v grafickom rozhraní, alebo ako výstup na terminál (TShark).

3.3.3 strace - Sledovanie systémových volaní a signálov

Nástroj `strace` pracuje na úrovni systémových volaní a s jeho pomocou sa dá zistiť, čo program požadoval od jadra systému. Jednotlivé zaznamenané operácie môžu byť napríklad pokusy o čítanie či zápis do súboru, alebo tiež pokus o otvorenie soketu. O každom volaní sa dozvieme, s akými argumentami bolo volané a tiež ako dopadlo.

3.4 Nástroj iw

Tento nástroj slúži na manipuláciu a konfiguráciu bezdrôtových sieťových rozhraní v prostredí GNU/Linux. Dokumentácia a zdrojový kód nástroja `iw` sú dostupné na webovej stránke `http://wireless.kernel.org/en/users/Documentation/iw`. Inštalácia tohto nástroja prebieha cez správu balíkov príkazom „`apt-get install iw`“.

3.4.1 Vybrané funkcie nástroja iw a ich výstup

V tejto časti práce sú popísané funkcie nástroja `iw`, ktoré v práci využijeme, alebo sú pre prácu zaujímavé. V ďalšej časti práce sa pokúsime na nástroj `iw` nahliadnuť hlbšie a zistiť, ako to na jeho pozadí funguje.

3.4.1.1 scan

Príkazom `scan` naskenujeme okolité siete:

iw dev wlan0 scan

```
BSS 00:22:b0:5f:c1:60 (on wlan0)
    freq: 2412
    beacon interval: 100
    signal: -32.00 dBm
    Information elements from Probe Response frame:
    SSID: WiFi1
    Supported rates: 1.0* 2.0* 5.5* 11.0*
    DS Parameter set: channel 1
BSS 00:02:72:63:7c:16 (on wlan0)
    freq: 2437
    beacon interval: 100
    signal: -64.00 dBm
    Information elements from Probe Response frame:
    SSID: Wifi2
    Supported rates: 1.0* 2.0* 5.5* 11.0* 6.0 9.0 12.0 18.0
    DS Parameter set: channel 6
```

Výpis 1: Výpis programu iw pre príkaz scan

Vo výpise číslo 1 môžeme vidieť, že máme v dosahu dve bezdrôtové siete. Ďalej ich silu signálu, BSS, SSID a niektoré ďalšie parametre.

3.4.1.2 connect

Príkazom `connect` sa môžeme pokúsiť pripojiť na bezdrôtovú sieť:

iw wlan0 connect Wifi1 - Pokúsi sa pripojiť k sieti, ktorej SSID je Wifi1

iw wlan0 connect Wifi1 2412 - Pokúsi sa pripojiť k sieti, ktorej SSID je Wifi1 na frekvencií 2412 (Užitočné, ak máme viacero sietí s rovnakým SSID)

iw wlan0 connect Wifi1 keys 0:12345 - Pokúsi sa pripojiť k sieti, ktorej SSID je Wifi1 so zabezpečením WEP s heslom 12345

Príkaz `connect` nemá žiadny výpis na konzolu. Či sa pripojenie podarilo môžeme overiť príkazom `link`.

3.4.1.3 link

Príkazom `link` zistíme, či sme pripojení k bezdrôtovej sieti:

iw dev wlan0 link

```
SSID: WiFi1
freq: 2412
RX: 10802 bytes (218 packets)
TX: 117 bytes (3 packets)
signal: −32 dBm
tx bitrate: 48.0 MBit/s
```

Výpis 2: Výpis programu iw pre príkaz link pri aktívnom spojení

iw dev wlan0 link

```
Not connected.
```

Výpis 3: Výpis programu iw pre príkaz link pri neaktívnom spojení

Vo výpise 2 vidíme aktuálne pripojenú sieť a jej parametre. Ak nie sme pripojení k žiadnej sieti, nastane výpis 3.

3.4.1.4 interface add

Príkazom `interface add` je možné pridávať rozhrania pre rôzne režimy.

iw dev wlan0 interface add mon0 type monitor - Vytvorí rozhranie typu monitor pre zariadenie wlan0.

3.4.1.5 set channel

Príkaz `set channel` slúži na prepnutie sieťovej karty na požadovaný kanál.

iw dev wlan0 set channel 1 - Prepne sieťovú kartu na kanál 1

3.4.1.6 disconnect

Príkazom `disconnect` sa odpojíme od aktuálne pripojenej bezdrôtovej siete:

iw dev wlan0 disconnect

Príkaz `disconnect` nemá žiadny výpis na konzolu.

3.4.2 Systémové volania iw scan

Zaujíma nás, čo sa deje na úrovni jadra pri vyvolanom skene nástrojom `iw` a kedy vlastne samotný sken prebieha. Na sledovanie použijeme nástroj `strace`.

Na test použijem notebook so systémom Ubuntu, ktorý bude mať v dosahu minimálne dva bezdrôtové prístupové body testovacej siete.

Najprv skúsime sken sledovať pri neaktívnom bezdrôtovom spojení s právami roota príkazom `strace iw dev wlan0 scan`. Následný výpis nástroja `strace` bol pomerne dlhý, preto som z neho vybral iba časti, ktoré som považoval za zaujímavé (výpis 4).

strace iw dev wlan0 scan

```
execve("/sbin/iw", ["iw", "dev", "wlan0", "scan"], [/* 23 vars */]) = 0
.
.
setsockopt(3, 0x10e /* SOL_?? */, 1, [6], 4) = 0
socket(PF_FILE, SOCK_DGRAM|SOCK_CLOEXEC, 0) = 4
 ioctl (4, SIOCGIFINDEX, {ifr_name="wlan0", ifr_index=3}) = 0
close(4)                                = 0
.
.
<vypis naskenovanych sieti>
.
.
exit_group(0)                   = ?
```

Výpis 4: Časť výpisu strace - neaktívne spojenie

Vo vybraných častiach môžeme vidieť, že na začiatku vzniká nový proces `iw` a volanie `execve` preberá tri parametre: plnú cestu k programu, pole jeho argumentov a pole premenných prostredia. Nasledovalo množstvo správ, v ktorých som nič zaujímavé nenašiel. Ďalej prišlo k nastaveniu (setsockopt) a otvoreniu soketu (socket). Nasledovalo systémové volanie `ioctl` s parametrom názvu a indexu sieťového volania. Táto sekvencia sa vo výpise opakuje niekoľkokrát. Potom nastáva výpis naskenovaných sietí a ukenčenie všetkých vlákien procesu.

Z výpisu nebolo jasné, či samotný sken prebieha pri každom otvorení soketu, tak som sledovanie tentokrát zopakoval s parametrom pre zobrazenie dĺžky trvania jednotlivých volaní.

strace -r iw dev wlan0 scan

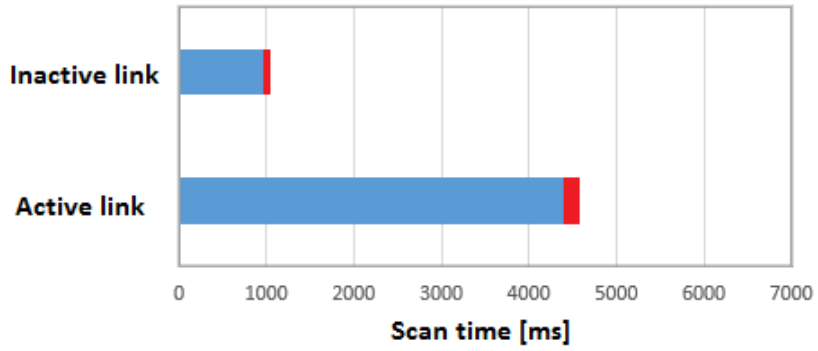
```
0.000228 setsockopt(3, 0x10e /* SOL_?? */, 1, [6],  4)  = 0
4.583556 socket(PF_FILE, SOCK_DGRAM|SOCK_CLOEXEC, 0) = 4
0.000202 ioctl(4,  SIOCGIFINDEX, {ifr_name="wlan0", ifr_index=3}) = 0
0.000308 close(4)                       = 0
```

Výpis 5: Časť výpisu strace - aktívne spojenie

Pri zobrazení časových známok bolo vidieť, že iba jedno otvorenie soketu trvalo podstatne dlhšie. Predpokladám, že samotný sken sietí prebieha práve tu.

V ďalšom teste skúsime sken sledovať pri aktívnom bezdrôtovom spojení s `Wireless Router 1` a právami roota. Výpis nástroja `strace` bol veľmi podobný. Hlavný rozdiel bol, že otvorenie soketu trvalo podstatne dlhšie (výpis 5).

Test pri aktívnom aj neaktívnom spojení som desaťkrát zopakoval. Rozdiel týchto dĺžok je vidieť na grafe obrázku č. 10. Červenou farbou je znázornená odchýlka pri jednotlivých meraniach. Predpokladám, že dĺžka skenu závisí aj od použitého hardvéru a prostredia, v ktorom sa sken vykonáva. Meranie ale dokázalo, že proces skenovania pri aktívnom spojení trvá podstatne dlhšie.



Obrázek 10: Priemerný čas trvania scanu pri aktívnom a neaktívnom spojení

Pri pokuse vyvolať sken nástrojom `iw` bez práv roota nastane chyba "Operation not permitted (-1)" a proces sa ukončí.

3.4.3 Nástroj iw na úrovni sieťových rámcov

Z teoretickej časti tejto práce vieme, že rámec je dátová jednotka linkovej vrstvy OSI modelu. My sa tieto rámce pokúsime zachytiť nástrojom Wireshark a analyzovať, čo sa odohráva pri vyvolaní skenu nástrojom `iw`.

3.4.3.1 Prostredie pre zachytávanie rámcov

Zachytávanie rámcov bude prebiehať v prostredí navrhnutej testovacej siete. Jednotlivé prístupové body sú rozmiestnené v rodinnom dome, kde predpokladám minimálne rušenie prístupovými bodmi, ktoré nie sú súčasťou testovacej siete. Každý prístupový bod má nastavený kanál, na ktorom bude vysielať:

`Wireless Router 1` - kanál 1.
`Wireless Router 2` - kanál 6.
`Wireless Router 3` - kanál 13.

Najbližšie k mobilnej stanici, na ktorej bude zachytávanie rámcov prebiehať, je umiestnený `Wireless Router 1`. O niečo ďalej je umiestnený `Wireless Router 2` a `Wireless Router 3` je umiestnený v najväčšej vzdialenosti od mobilnej stanice.

Mobilná stanica (wlan klient), na ktorej budeme zachytávať rámce bude notebook s operačným systémom Ubuntu 12.4 LTS, čo je linuxová distribúcia založená na jadre Debian GNU/Linux. V Ubuntu vypneme službu sieťového manažéra príkazom " `service network-manager stop`" a nastavíme pevnú IP adresu podľa tabuľky konfigurácie zariadení č. 3.

Na to, aby sme mohli zachytávať všetky rámce protokolu 802.11, ktoré sú odvysielané v dosahu sieťovej karty notebooku na nastavenej frekvencii, musíme najprv prepnúť kartu do módu monitor. Prepnúť kartu do módu monitor sa dá viacerými spôsobmi. V našom prípade sme monitor rozhranie pre sieťovú kartu vytvorili nástrojom `iw`. Či sa nám monitor rozhranie podarilo vytvoriť, môžeme overiť príkazom `iwconfig`.

iw dev wlan0 interface add mon0 type monitor
iwconfig

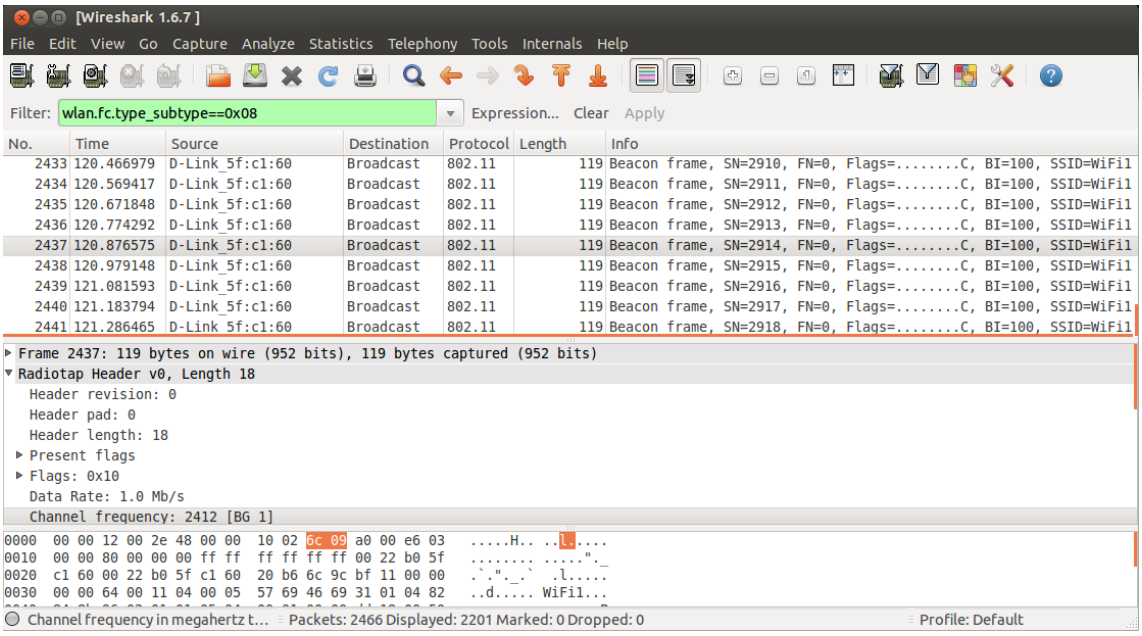
```
root@jakub:/home/jakub# iw dev wlan0 interface add mon0 type monitor
root@jakub:/home/jakub# iwconfig
wlan0     IEEE 802.11bg ESSID:off/any
          Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
          Retry long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

mon0      IEEE 802.11bg Mode:Monitor Tx-Power=20 dBm
          Retry long limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
```

Výpis 6: Vytvorenie a zobrazenie monitor rozhrania

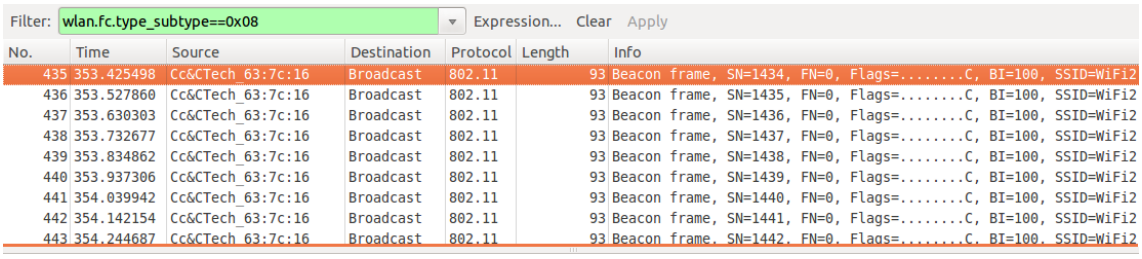
3.4.3.2 Zachytávanie 802.11 rámcov nástrojom Wireshark

Po vytvorení vhodného prostredia pre zachytávanie 802.11 rámcov sme spustili program Wireshark a vybrali vytvorené monitor rozhranie. Zachytávanie bezdrôtovej komunikácie cez Wireshark fungovalo bez problémov. Pre lepší prehľad zachytených rámcov som nastavil filter v nástroji Wireshark tak, aby zobrazoval iba zachytené beacon rámce. V zachytených beacon rámcoch boli vidieť rámce odvysielané routerom `Wireless Router 1`, čo znamenalo, že je sieťová karta na kanáli 1. V tom nás utvrdila aj informácia z Radiotap Haderu zachyteného beacon rámca (obrázok č. 11).



Obrázek 11: Wireshark - Zachytené beacon rámce kanál 1

Pomocou nástroja `iw` môžeme tiež zmeniť kanál, na ktorom sieťová karta načúva. Príkazom iw dev wlan0 set channel 6 sme prepli kartu na 6. kanál a znovu zachytili beacon rámce. Tentokrát sme zachytili beacon rámce vysielané routerom `Wireless Router 2` (obrázok č. 12).

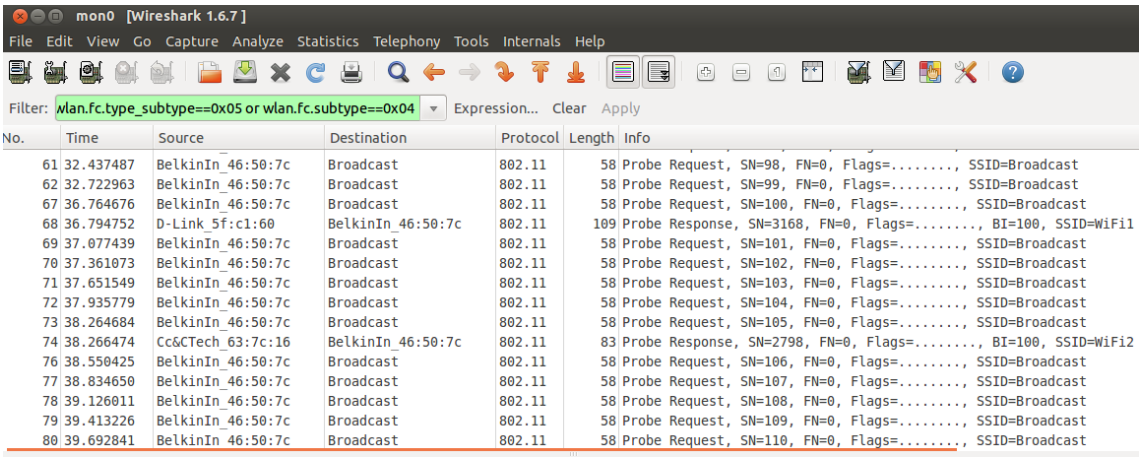


Obrázek 12: Wireshark - Zachytené beacon rámce kanál 6

Po prepnutí na kanál č. 13 sa nám beacon rámce routera, ktorý bol umiestnený najďalej, zachytiť vôbec nepodarilo. Zachytávanie beacon rámcov vo všetkých prípadoch prebiehalo pri neaktívnom bezdrôtovom spojení. Skúsil som podobný test aj pri aktívnom spojení, kde sme zistili, že zachytávanie beacon rámcov na rôznych kanáloch manuálnym prepínaním na iné kanály funguje iba vtedy, ak nemáme aktívne bezdrôtové spojenie. Ak sme pripojený na nejakú bezdrôtovú sieť, pri pokuse prepnúť kanál nastane chyba "Device or resource busy". To znamená, že rámce 802.11 môžeme zachytávať iba na kanáli, na ktorom komunikuje sieťová karta s pripojeným prístupovým bodom.

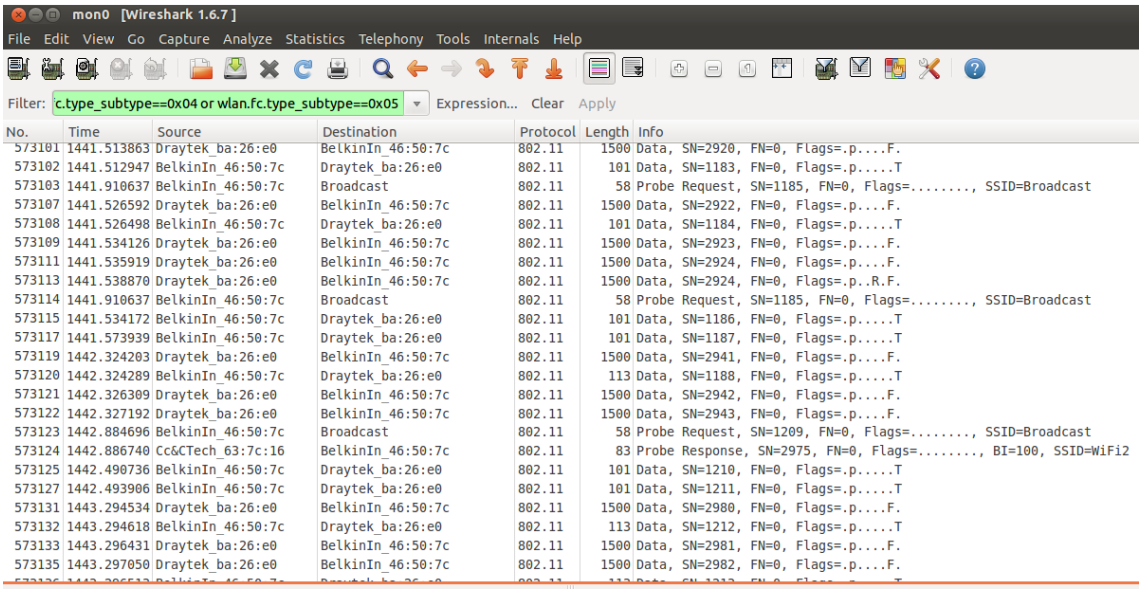
3.4.3.3 iw scan - analýza nástrojom Wireshark

V rovnakých podmienkach sme sa snažili zachytiť, čo sa odohráva na pozadí vyvolaného skenu pomocou nástroja `iw`. Najprv som skúsil vykonať sken pri neaktívnom bezdrôtovom spojení a nechal som zobraziť iba `probe request` a `probe response` rámce. Zo zachytených rámcov je zrejmé, že sken pomocou nástroja `iw` je aktívny. Po vyvolaní skenu sieťová karta postupne prechádza jednotlivé kanály, na ktorých vyšle `probe request` rámec a počká na prípadnú odpoveď. Wiresharkom zachytené rámce sú na obrázku č. 13.



Obrázek 13: Wireshark - iw scan

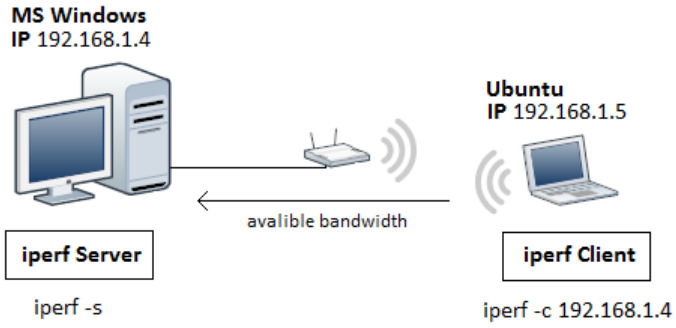
Druhý test prebiehal pri aktívnom bezdrôtovom spojení s routerom `Wireless Router 2`. Po tomto bezdrôtovom spojení sme dali kopírovať súbor, aby sme docielili tok dátových rámcov. Následne sme vykonali sken nástrojom `iw` a pre väčší prehľad filtrom vo Wiresharku odstránili všetky rámce typu `Control Frames`. Zachytené rámce sú na obrázku 14). Po vyvolaní skenu, tak ako v predchádzajúcom prípade, sieťová karta postupne prechádza jednotlivé kanály, na ktorých vyšle `probe request` rámec a počká na prípadnú odpoveď. Zároveň však vidíme, že aj počas skenu sa sieťová karta prepne na pôvodný kanál a komunikuje s asociovaným prístupovým bodom, aby nedošlo k dlhšiemu prerušeniu dátového toku.



Obrázek 14: Wireshark - iw scan 2

3.4.4 iw scan - vplyv na prebiehajúcu komunikáciu

V tejto časti sa zameriame na vplyv skenu vyvolaného nástrojom `iw` na dva parametre bezdrôtového spoja: čas odozvy a rýchlosť prenosu dát. Testy budú prebiehať v rovnakom prostredí ako zachytávanie rámcov (časť 3.4.3.1). Každý test prebehol niekoľkokrát a ich výsledky boli medzi sebou porovnávané. Z týchto testov som vždy vybral jeden, ktorý podľa môjho názoru najlepšie reprezentoval skutočnosť.



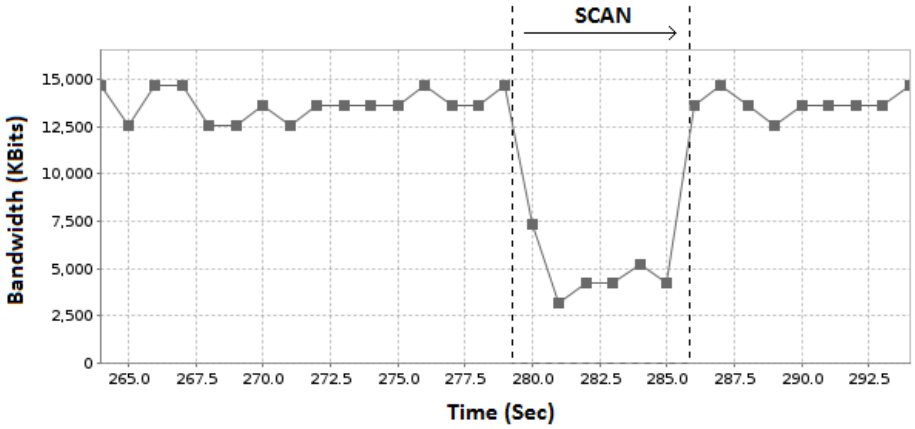
Obrázek 15: Konfigurácia iperf

3.4.4.1 Vplyv vyhľadávania na rýchlosť prenosu dát

Test rýchlosti prenosu dát prebiehal na bezdrôtovom spoji medzi notebookom a rou-

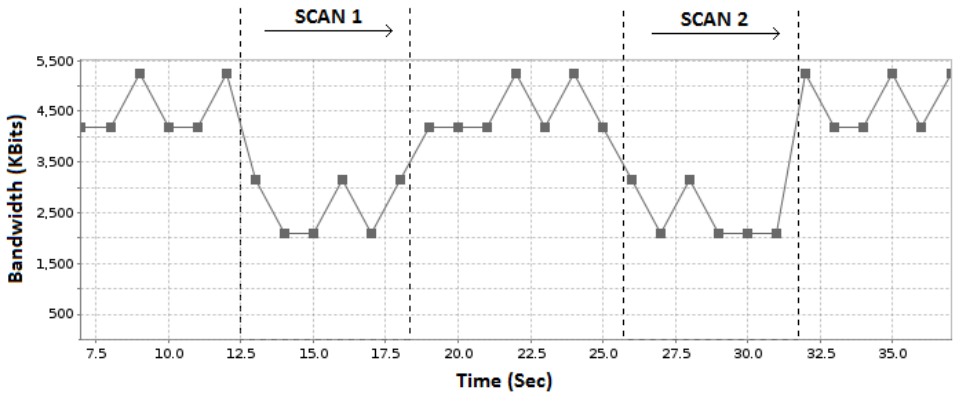
terom `Wireless Router 1`.

Prvý test rýchlosti prenosu prebiehal pri najlepšej dosiahnutej úrovni signálu z asiciovaného bezdrôtového prístupového bodu. Stanica bola umiestnená v jeho tesnej blízkosti a nástrojom `iperf` sme merali maximálnu rýchlosť prenosu dát počas vyvolaného skenu nástrojom `iw`. Pre nastavenie iperf pozri obrázok 15. Na grafe obrázku číslo 16 môžeme pozorovať prudký pokles rýchlosti prenosu počas priebehu skenu. Test sme zopakovali



Obrázek 16: Pokles rýchlosti prenosu dát pri vysokej úrovni signálu

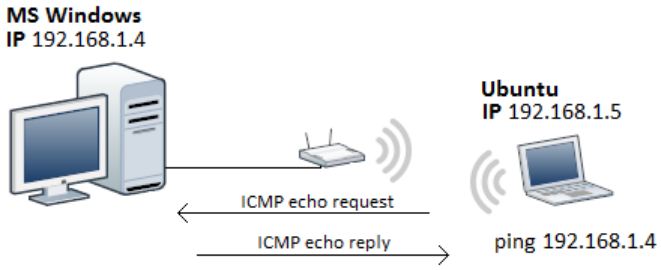
po vzdialení sa od asociovaného bezdrôtového bodu pred hranicu, kedy by už prichádzalo k výpadkom spojenia. Vtedy bol dopad skenovania na rýchlosť prenosu dát podstatne nižší. Pozri obrázok 17.



Obrázek 17: Pokles rýchlosti prenosu dát pri nízkej úrovni signálu

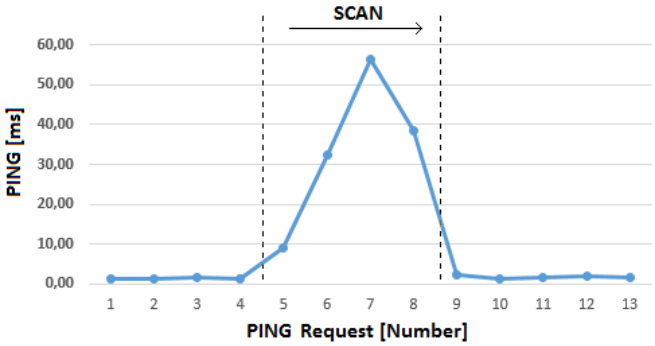
3.4.4.2 Vplyv vyhľadávania na odozvu siete

Test vplyvu skenu vyvolaného nástrojom `iw` na odozvu prebiehal na bezdrôtovom spoji medzi notebookom a routerom `Wireless Router 1` nami vytvorenej testovacej siete. Zvýšenie odozvy siete sa počas skenovania prejavilo hlavne pri dobrej úrovni signálu.



Obrázek 18: Test odozvy sieťového spoja

Ako sa signál vzďaľovaním od prístupového bodu zhoršoval, rástla aj odozva siete. Po určitej hranici sa už odozva siete skenovaním podstatne nezhoršovala.



Obrázek 19: Zvýšenie odozvy siete pri najlepšej úrovni signálu

3.4.5 Zhodnotenie

Zistené skutočnosti a testy sa zhodujú s predpokladmi z teoretickej časti práce. Skenovanie sietí spôsobom, akým ho vyvolá nástroj `iw`, má negatívny vplyv na prebiehajúcu bezdrôtovú komunikáciu. Tento negatívny vplyv sa stáva ťažšie pozorovateľný pri zhoršení parametrov bezdrôtového spoja (časť 3.4.4). Pri vyvolaní skenu nástrojom `iw` bezdrôtová sieťová karta striedavo prerušuje aktuálne prebiehajúcu komunikáciu, aby mohla postupne naskenovať okolité bezdrôtové siete. Tento záver potvrdzuje okrem zhoršenia parametrov ako rýchlosť prenášaných dát a odozvy siete aj rozdiel dĺžky skenu (časť 3.4.2) a prenášané dátové rámce pri aktívnom a neaktívnom bezdrôtovom spojení (časť 3.4.3).

4 Implementácia aplikácie

4.1 Špecifikácia aplikácie

Aplikácia bola implementovaná pre testovanie a demonštráciu možností proaktívneho vyhľadávania bezdrôtových sietí.

Funkciou aplikácie je vykonávať vyhľadávanie na pozadí prebiehajúcej komunikácie a v prípade straty signálu s aktuálnym prístupovým bodom tieto výsledky využiť na rýchle obnovenie spojenia.

Pri tvorbe aplikácie sú využité poznatky z teoretickej aj experimentálnej časti tejto práce.

4.2 Vývojové prostredie a požiadavky aplikácie

Aplikácia na bezdrôtové vyhľadávanie sietí je implementovaná v programovacom jazyku Java a jej vývoj prebiehal v prostredí NetBeans IDE.

Jedna z hlavných výhod aplikácií implementovaných v jazyku Java je, že nie sú závislé na konkrétnej platforme a dajú sa spustiť všade, kde je nainštalovaný JRE. Aplikácia ale pracuje s nástrojmi operačného systému GNU/Linux cez rozhranie príkazového riadku (CLI), preto bude správne fungovať iba v distribúciách operačného systému Linux.

Požiadavky pre správne fungovanie aplikácie:

- Operačný systém založený na platforme GNU/Linux
- Java Standard Edition JRE 1.7
- Nástroje `iw`, `tshark` a `grep`
- Administrátorské práva
- Vypnutý GNU/Linux sieťový manažér
- Sieťová karta v móde monitor
- Nastavený rovnaký kanál na bezdrôtových prístupových bodoch

4.3 Shell skript a nástroje GNU/Linux

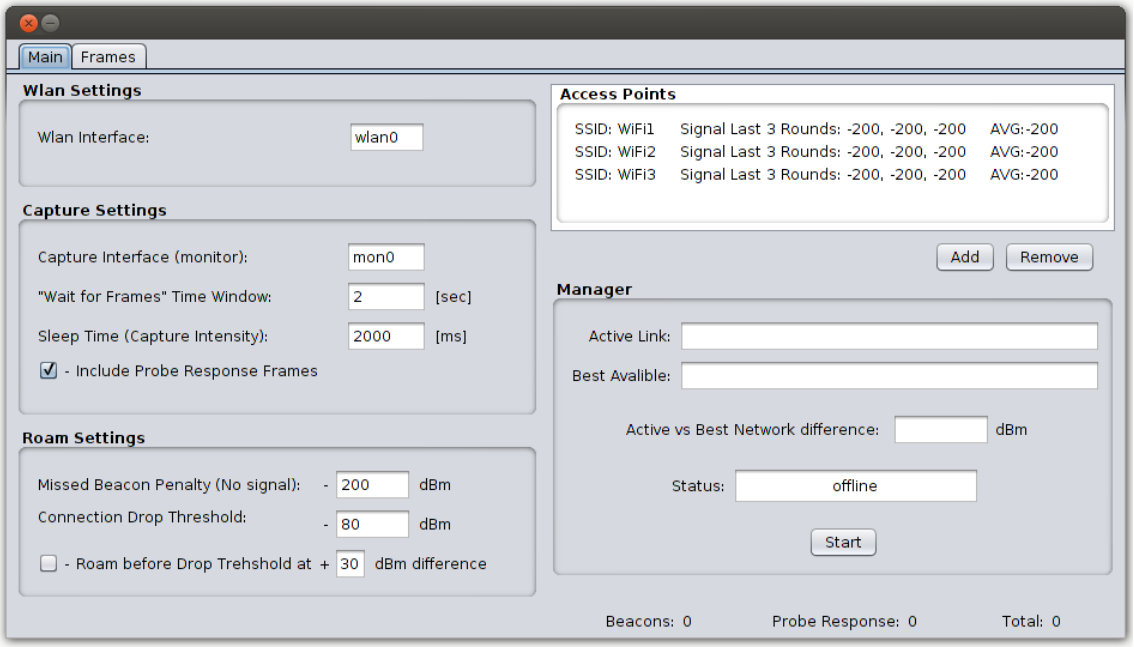
GNU/Linux shell je špeciálny interaktívny nástroj, ktorý užívateľom poskytuje spôsob, akým môžu spúšťať programy, spravovať súbory na súborovom systéme a riadiť procesy bežiace na systéme Linux. Okrem sady interných príkazov môžeme cez shell spúšťať aj iné programy a nástroje.[3]

Aplikácia je postavená na komunikácii s nástrojmi Linuxu, ktoré sú spúšťané cez shell. Nižšie si popíšeme všetky nástroje, s ktorými aplikácia pracuje a ich využitie.

- **iw** - Nástroj iw aplikácia používa na nadviazanie a ukončenie spojenia s bezdrôtovým prístupovým bodom.
- **tshark** - Nástroj Tshark je obdoba Wiresharku s textovým výstupom. Tsharkom budeme zachytávať 802.11 rámce na monitor rozhraní bezdrôtovej sieťovej karty.
- **grep** - Grep je nástroj na vyhľadávanie regulárnych výrazov v texte. V aplikácii tento nástroj používame na filtrovanie výstupu z Tsharku.

4.4 Grafickéhé rozhranie implementovanej aplikácie

V tejto časti práce si vysvetlíme princíp fungovania implementovanej aplikácie. Grafické rozhranie aplikácie je rozdelené do niekoľkých častí, ktorých rozloženie môžeme vidieť na obrázku grafického rozhrania aplikácie (obrázok 20). Funkciu každej časti si nižšie popíšeme a vysvetlíme podrobnejšie.



Obrázek 20: Grafické rozhranie implementovanej aplikácie

4.4.1 Wlan Settings

V tejto časti programu je jedno vstupné pole `Wlan Interface`, ktoré slúži na určenie bezdrôtového sieťového rozhrania, cez ktoré bude aplikácia nadväzovať a monitorovať spojenie s prístupovými bodmi.

4.4.2 Capture Settings

Časť `Capture Settings` slúži pre nastavenie možností zachytávania rámcov.

Nastavenie `Capture Monitor` definuje rozhranie, na ktorom budeme zachytávať 802.11 rámce.

Nastavenie `Wait for Frames Time Window` určuje dĺžku, počas ktorej budeme na monitor rozhraní zachytávať `beacon` rámce pred spracovaním.

`Sleep Time` určuje, koľko má aplikácia čakať medzi jednotlivými zachytávaniami rámcov.

Poslednou možnosťou v tejto časti `Include Probe Response Frames` môžeme nastaviť, či má aplikácia spracovávať aj zachytené `probe response` rámce.

4.4.3 Roam Settings

Nastavenia v `Roam Settings` určujú, za akých podmienok nastane ukončenie spojenia s aktuálne pripojeným a nadviazanie spojenia s vhodnejším prístupovým bodom.

Hodnotu `Missed Beacon Penalty` aplikácia nastaví pre sieť, ktorej `beacon` rámce resp. `probe response` rámce v danom kole nezachytí. `Connection Drop Threshold` určuje hodnotu signálu, pri ktorej nastane ukončenie spojenia s aktuálne pripojenou bezdrôtovou sieťou v prípade, že je dostupná sieť s lepším signálom.

Pri vybratí možnosti `Roam before Drop Threshold` sa program pokúsi o nadviazanie spojenia s novým prístupovým bodom aj v prípade, keď má nový dostupný prístupový bod lepší signál o užívateľom definovanú hodnotu ako aktuálne pripojený, pričom signál aktuálne pripojenej siete nemusí klesnúť pod hodnotu signálu zadanú v `Connection Drop Treshold`.

4.4.4 Access Points

Aplikácia ďalej obsahuje časť s názvom `Access Points`. Tá slúži pre správu údajov o prístupových bodoch, s ktorými má aplikácia pracovať. Tieto údaje sú potrebné pre pripojenie k daným bodom (BSS, SSID, prístupové heslo). Prístupové body, ktoré nie sú v tomto zozname, budú aplikáciou ignorované. Užívateľ má možnosť prístupový bod pridať alebo odobrať podľa potreby. Údaje o prístupových bodoch sa pri ukončení aplikácie uložia na disk do súboru v priečinku, z ktorého bola aplikácia spustená. Pri spustení aplikácie sa údaje z tohto súboru načítajú do programu.

V tejto časti aplikácie sa taktiež počas monitorovania zobrazujú informácie pre každý z monitorovaných prístupových bodov o troch posledných nameraných hodnotách signálov a ich priemer.

4.4.5 Manager

Časť `Manager` slúži na spustenie monitorovania prístupových bodov v okolí. Po spustení bude aplikácia v tejto časti zobrazovať informácie o najlepšom (najlepší priemerný signál z posledných troch zachytávaní rámcov) dostupnom prístupovom bode, o aktuálne pripojenom prístupovom bode a rozdiele signálu medzi nimi v dBm.

Ďalej obsahuje stavový riadok, ktorý zobrazuje, či aplikácia inicializuje takzvaný roam na iný prístupový bod.

4.5 Spôsob vyhodnocovania údajov

4.5.1 Určenie signálu prístupového bodu z rámocv

Určenie signálu prístupových bodov v okolí funguje na zachytávaní `beacon` a `probe response` rámcov nástrojom `tshark`. Každý takýto rámec obsahuje informácie ako BSS, SSID a typ rámca. Rámce tiež obsahujú `Radiotap Header`, ktorý obsahuje rozširujúce informácie, z ktorých vieme určiť okrem iného aj intenzitu signálu zachyteného rámca.

Aplikácia porovnáva zachytené rámce a určuje, či patria niektorému s nami monitorovaných prístupových bodov. Z rámcov, v ktorých je zhoda s monitorovanou sieťou, aplikácia spriemeruje signál a priradí ho k danému prístupovému bodu ako signál za dané kolo.

4.5.2 Výber najlepšieho prístupového bodu

Najlepší prístupový bod je vybraný na základe posledných troch zachytávaní rámcov. Prístupový bod s najlepším priemerom signálu aplikácia vyberie ako najlepší.

4.5.3 Algoritmus rozhodovania manžéra

```
while(startThread != null)                                    // 1
{
    if (IsConnectedApBest() == false)                         // 2
    {
        if (ConnectedApSignal() <= threshold)                 // 3
        {
            ActionField.setText("Roaming! (low signal)");
            ConnectToBestAp();
        }
        else if (differenceChecked == true)                   // 4
        {
            if (SignalDifference() >= difference)             // 5
            {
                ActionField.setText("Roaming! (difference)");
                ConnectToBestAp();
            }
            else ActionField.setText("Idle");
        }
        else ActionField.setText("Idle");
    }
    else ActionField.setText("Idle");
}
```

Výpis 7: Algoritmus rozhodovania manažéra

1 – Hlavný cyklus, ktorý beží ak je manažér zapnutý.

2 – Podmienka, ktorou manažér zisťuje, či je pripojený prístupový bod najlepší. V prípade, že pripojený prístupový bod je najlepší, ostáva manažér daný cyklus nečinný.

3 – Podmienka, ktorá nastáva v prípade, že máme dostupný lepší prístupový bod. Touto podmienkou manažér zisťuje, či je úroveň signálu z aktuálne pripojeného bodu rovnaká alebo menšia, než pri ktorom má nastať naviazanie spojenia s lepším prístupovým bodom. Pri splnení tejto podmienky nastáva prepojenie s lepším prístupovým bodom. Pri nesplnení sa kontroluje podmienka 4.

4 – Touto podmienkou manažér kontroluje, či užívateľ vybral možnosť prepojenia na lepší prístupový bod aj v prípade ním definovaného rozdielu signálu medzi aktuálne pripojeným a najlepším dostupným prístupovým bodom. Pri nesplnení ostáva manažér daný cyklus nečinný. Pri splnení tejto podmienky sa kontroluje podmienka 5.

5 – Táto podmienka kontroluje, či je rozdiel signálu medzi aktuálne pripojeným a najlepším dostupným prístupovým bodom väčší, ako definoval užívateľ v `Roam before Drop Threshold`. Pri splnení tejto podmienky nastáva prepojenie s lepším prístupovým bodom. Inak ostáva manažér daný cyklus nečinný.

4.6 Test implementovanej aplikácie

Test implementovanej aplikácie prebiehal v prostredí navrhnutej testovacej siete z experimentálnej časti. Pre fyzickú topológiu siete pozri obrázok číslo 9 a pre konfiguráciu zariadení tabuľku číslo 3. Pre tento test sme nastavili všetky prístupové body na 1. kanál a umiestnili ich čo najďalej od seba.

Aplikáciu budeme testovať spôsobom, že nástrojom `iperf` budeme merať rýchlosť prenášaných dát po bezdrôtovom spoji medzi notebookom a desktopom, pričom sa s notebookom budeme pohybovať medzi jednotlivými prístupovými bodmi siete. Pre nastavenie `iperf` pozri obrázok 15.

Aplikácia by mala pri strate alebo zhoršení signálu s aktuálne pripojeným prístupovým bodom vyvolať rýchlu reasociáciu na základe proaktívneho vyhľadávania.

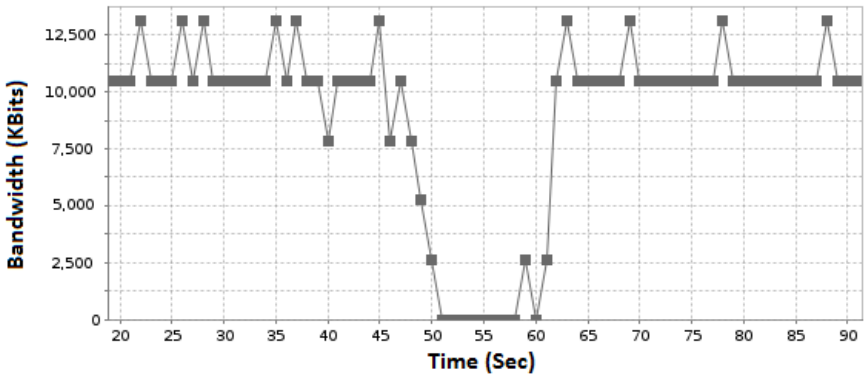
Východzie nastavenia aplikácie sú na obrázku číslo 20.

4.6.1 Test číslo 1

Pri tomto teste sme notebook presúvali od prístupového bodu `Wireless Router 1` k prístupovému bodu `Wireless Router 2`. Aplikácia mala nastavené na východzie hodnoty okrem `Connection Drop Threshold`, ktorá bola pre tento test nastavená na -70

dBm.

Na grafe obrázku č. 21 môžeme vidieť ako pri klesnutí signálu pod -70 dBm z `Wireless Router 1` nastalo prepojenie na `Wireless Router 2`.

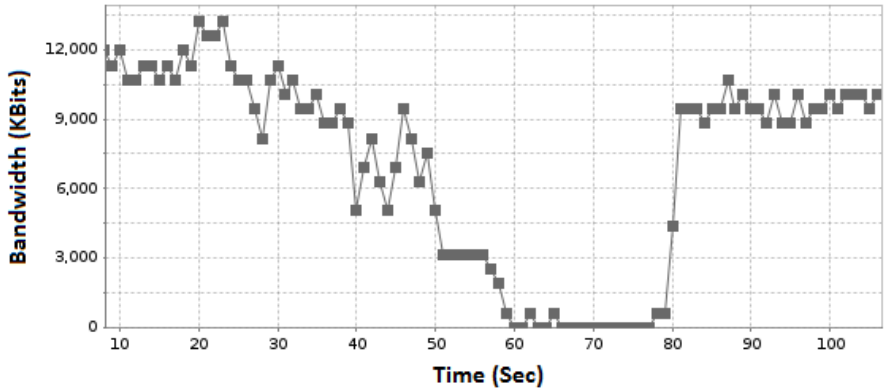


Obrázek 21: Test aplikácie č. 1

4.6.2 Test č. 2

Pri tomto teste sme notebook presúvali od prístupového bodu `Wireless Router 1` k prístupovému bodu `Wireless Router 3`. Prístupový bod `Wireless Router 2` bol vypnutý a aplikácia mala nastavené východzie hodnoty.

Na grafe obrázku č. 22 môžeme vidieť, ako pri klesnutí signálu z prístupového bodu `Wireless Router 1` pod - 80 dBm nastalo obnovenie spojenia s prístupovým bodom `Wireless Router 3`.

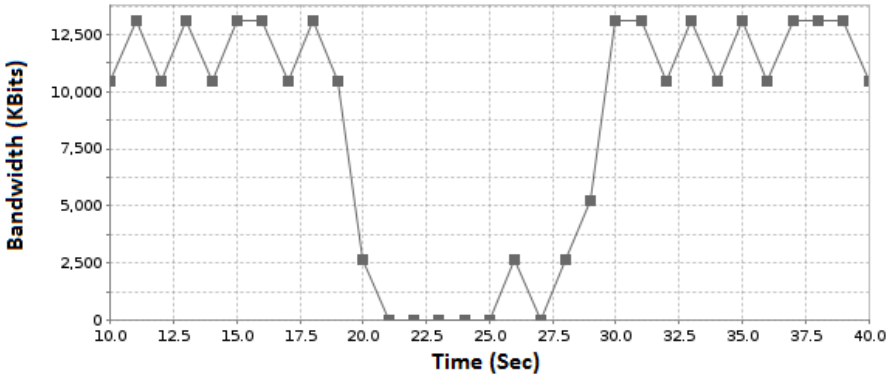


Obrázek 22: Test aplikácie č. 2

4.6.3 Test č. 3

Pri teste číslo 3 sme umiestnili `Wireless Router 1` a `Wireless Router 2` do tesnej blízkosti notebooku a aplikácia mala nastavené na východzie hodnoty. Notebook bol pripojený k `Wireless Router 1`, ktorý sme počas merania rýchlosti spojenia odpojili od elektrickej siete.

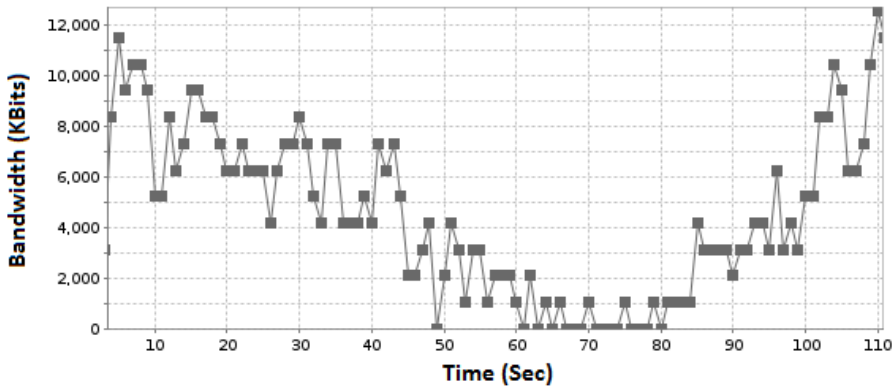
Na grafe obrázku 23 môžeme vidieť, ako pri výpadku prístupového bodu `Wireless Router 1` nastalo obnovenie spojenia s prístupovým bodom `Wireless Router 2`.



Obrázek 23: Test aplikácie č. 3

4.6.4 Test č. 4

Pri tomto teste bol zapnutý iba `Wireless Router 1`. S notebookom sme sa od neho postupne vzďaľovali , až kým nezačalo dochádzať k výpadkom spojenia. Po opätovnom priblížení k prístupovému bodu sa spojenie obnovilo (obrázok 24).



Obrázek 24: Test aplikácie č. 4

5 Záver

V práci sme sa zaoberali možnosťami proaktívneho vyhľadávania dostupných bezdrôtových sietí na pozadí prebiehajúcej komunikácie. Vyhľadávanie pri aktívnom bezdrôtovom spojení môže výrazne zhoršiť parametre spojenia, čo má negatívny vplyv na prebiehajúcu komunikáciu. Zistili sme, že pri nízkej úrovni signálu je vplyv vyhľadávania na bezdrôtovú komunikáciu podstatne menší, ako keď sa nachádzame v bezprostrednej blízkosti prístupového bodu.

Pri strate spojenia výsledky proaktívneho vyhľadávania zohrávajú dôležitú úlohu v rýchlosti obnovenia spojenia s novým prístupovým bodom. Bez výsledkov proaktívneho vyhľadávania systém najprv musí naskenovať okolité prístupové body a až potom môže obnoviť spojenie.

Hlavným problémom proaktívneho vyhľadávania na pozadí bolo navrhnúť riešenie, ktoré by čo najmenej obmedzovalo prebiehajúcu bezdrôtovú komunikáciu a zároveň by pri strate signálu boli výsledky proaktívneho vyhľadávania aktuálne.

Výsledkom tejto práce je aplikácia, ktorá pri strate signálu využije výsledky proaktívneho vyhľadávania na rýchle obnovenie spojenia s najvhodnejším prístupovým bodom. Aplikácia je navrhnutá tak, aby neobmedzovala prebiehajúcu bezdrôtovú komunikáciu. Implementácia aplikácie je použiteľná v reálnom prostredí a vo veľa prípadoch zrýchli proces obnovenia spojenia. Jej hlavnou nevýhodou je, že všetky prístupové body s ktorými má pracovať, musia byť nastavené na rovnaký kanál.

Ďalší vývoj aplikácie by mohol spočívať v podpore viacerých sieťových rozhraní, kde by jedno sieťové rozhranie bolo vyhradené iba na zachytávanie rámcov. Takýmto riešením by sa odstránil problém nutnosti nastaviť prístupové body na jeden kanál, ale vzrástli by požiadavky na hardvér.

6 Reference

[1] GAST, Matthew. *802.11 Wireless Networks: The definitive guide*. Sebastopol: O'Reilly, 2005, xxi, 630 s. ISBN 978-0-596-10052-0.

[2] GORANSSON, Paul a Raymond GREENLAW. *Secure roaming in 802.11 networks*. Boston: Newnes/Elsevier, c2007, xxiv, 343 p. ISBN 07-506-8211-6.

[3] BLUM, Richard. *Linux command line and shell scripting bible*. Indianapolis, IN: Wiley Pub., c2008, xxx, 809 p. ISBN 04-702-5128-X.

[4] STEVENSON, Angus. *Oxford dictionary of English*. New York, NY: Oxford University Press, 2010, xxii, 2069 p. ISBN 978-019-9571-123.

[5] CISCO SYSTEMS, Inc. *Voice over Wireless LAN 4.1 Design Guide* [online]. [cit. 2014-03-16]. Dostupné z: `http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book.pdf`

[6] MICROSOFT CORPORATION. *How 802.11 Wireless Works* [online]. [cit. 2014-04-15]. Dostupné z: `http://technet.microsoft.com/cs-cz/library/cc757419.aspx`

A Príloha na CD

Obsah CD
Priložené CD obsahuje implementáciu aplikácie na proaktívne vyhľadávanie bezdrôtových sietí.