Slovenská technická univerzita v Bratislave
Fakulta informatiky a informačných technológií
Ilkovičova 3, 842 16 Bratislava 4

Praktické cvičenie č. 1

Roman Panenka

Študijný program: Počítačové komunikačné systémy a siete
Predmet: Bezdrôtové komunikačné systémy
Ročník: Ing. 1.
Akademický rok: 2010/2011

Obsah

1. Cieľ zadania

Prvé praktické cvičenie je zamerané na úvodné oboznámenie sa so základnými nástrojmi a technikami používanými na detekciu a analýzu bezdrôtovej siete na báze štandardu 802.11b pracujúcej v infraštruktúrnom režime.

Študent si prakticky osvojí používanie vybraných nástrojov, analyzuje existujúcu sieť a bude skúmať vplyv niektorých parametrov na intenzitu signálu bezdrôtovej siete.

2. Technické a programové prostriedky

Pre úspešné dosiahnutie cieľov zadania a na efektívny výskum parametrov intenzity signálu, potrebuje študent nasledujúce technické a programové prostriedky:

- Prístupový bod (AP) D-Link AirPlus 900AP+ pracujúci v pásme 2,4 GHz
- Notebook s OS Microsoft Windows, interná sieťová karta
- Softvérové vybavenie
  - Program WireShark[1]
  - Program Netstumbler[2]
  - Program Vistumbler[3]
  - Program Inssider[4]
  - Program OmniPeek[5]
  - Aircrack-ng (MS Windows / linux)[6]

3. Význam použitých skratiek

- SSID – Service set identifier – jedinečný identifikátor bezdrôtovej počítačovej siete
- MAC – Media Access control – jedinečný identifikátor sieťového zariadenia – fyzická
- dBm – decibels to milliwatt – jednotka intenzity signálu
- AP – Access point – zariadenie, ku ktorému sa pripájajú klienti bezdrôtovej siete
- RSSI - Received Signal Strength Indication – jednotka určujúca kvalitu signál pre bezdrôtové zariadenia
- 802.11 – súbor wifi štandardou

[1] http://media-2.cacetech.com/wireshark/win32/wireshark-win32-1.2.2.exe

[2] http://downloads.netstumbler.com/downloads/netstumblerinstaller_0_4_0.exe

[3] http://downloads.sourceforge.net/project/vistumbler/Vistumbler%20MDB/Vistumbler%20v9.7/Vistumbler_v9-7.exe?use_mirror=dfn

[4] http://www.metageek.net/files/webfm/Software/Inssider_Installer.msi

[5] http://www.brothersoft.com/d.php?soft_id=226397&url=http%3A%2F%2Ffiles3.brothersoft.com%2Futilities%2Fnetwork%2FOmniPeek60demo.exe

[6] http://download.aircrack-ng.org/aircrack-ng-1.1-win.zip

4. Postup cvičenia

Pokiaľ ešte nie sú vyššie uvedené programové prostriedky nainštalované, je potrebné ich nainštalovať na vybraný notebook. Jedná sa o voľne dostupné programy, ktoré netreba zakupovať. Úlohou je skúmať závislosť intenzity signálu bezdrôtovej siete v závislosti od vzdialenosti od prístupového bodu pri priamej viditeľnosti a v priestore s prekážkami. Pri vypracovávaní zadania sa zameriame na sieť, ktorej SSID je BKS.

Prvým programom je WireShark slúžiaci na odchytávanie rámcov v sieti. Pod OS Windows v kombinácii s niektorými sieťovými kartami však doposiaľ nie je možné odchytávať niektoré riadiace rámce štandardu 802.11, a preto budeme používať aj program OmniPeek, ktorý toto umožňuje.

Ďalším programom je Netstumbler, ktorý nám zobrazuje pomerne podrobné informácie o bezdrôtových sieťach a ich rôzne parametre. V prípade, že by program nepracoval správne, budeme používať program Vistumbler a Inssider, ktoré ponúkajú obdobné možnosti. Zistíme, aké všetky bezdrôtové siete sú dostupné v našom okolí a porovnáme získané výsledky s výsledkami štandardného rozhranie OS.

Okrem sledovania intenzity signálu sa zameriame aj analýzu znižovania prenosovej rýchlosti v sieti s narastajúcou vzdialenosťou od AP. Prakticky realizujeme merania za prekážkou ako je stena, chodba, výťah i poschodie.

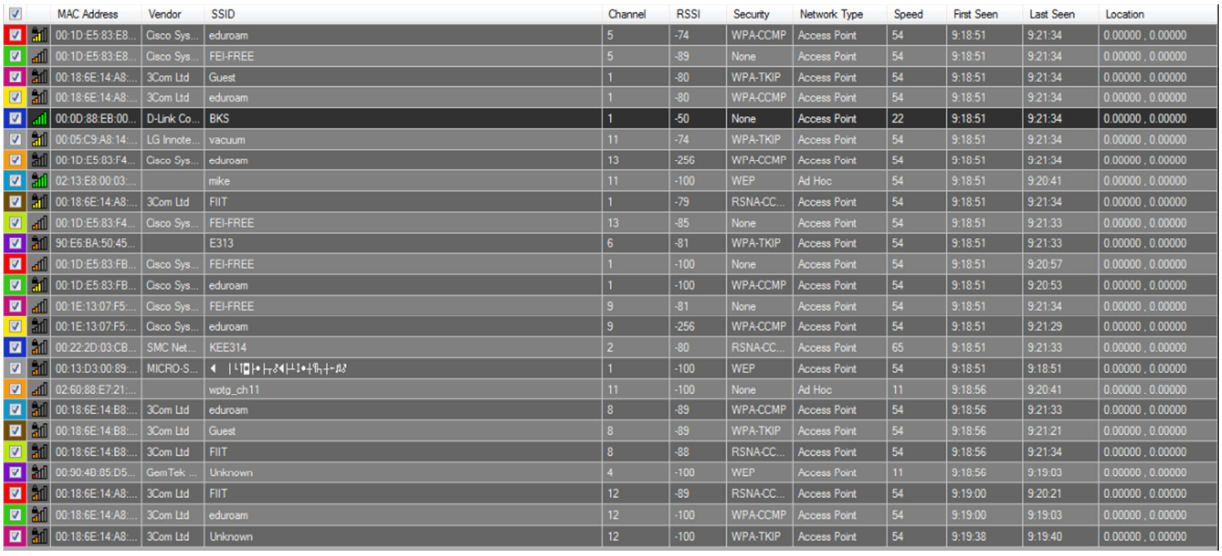
V praxi sa používajú štyri základné jednotky reprezentujúce silu signálu bezdrôtovej siete: mW, dBm(db - mW), RSSI (Receive Signal Strength Indicator) a percentuálne ohodnotenie. Zistime aké možnosti ponúkajú programy, s ktorými pracujete a vyberieme si niektorú možnosť. Namerané výsledky graficky znázornime a odôvodnime.

5. Výsledky skúmania

Pomocou programu inSSIDer sme skúmali parametre a intenzitu signálu dostupných sietí. Takisto sme pomocou tohto programu zistili informácie o testovanej sieti:

- SSID: BKS
- Typ siete: Prístupový bod
- Verzia protokolu: 802.11 g
- Metóda zabezpečenia: žiadna
- Kanál: 1
- RSSI: -50
- Pásmo vysielania: 2.4 GHz
- Výrobca AP: D-link Corporation
- AP MAC adresa: 00:0D:88:EB:00:3E

Na obrázku Obrázok 1 môžeme vidieť zoznam všetkých bezdrôtových sietí zachytených programom inSSIDer. Označený záznam je nami skúmaná sieť s SSID BKS. Každý záznam má informáciu o MAC adrese AP, výrobcovi AP, vysielané SSID. Okrem týchto základných veličín môžeme z obrázku vyčítať aj vysielací kanál, rýchlosť a intenzitu signálu – RSSI, zabezpečenie danej siete, typ siete a časové informácie detegovania siete (posledný a prvý čas detekcie).



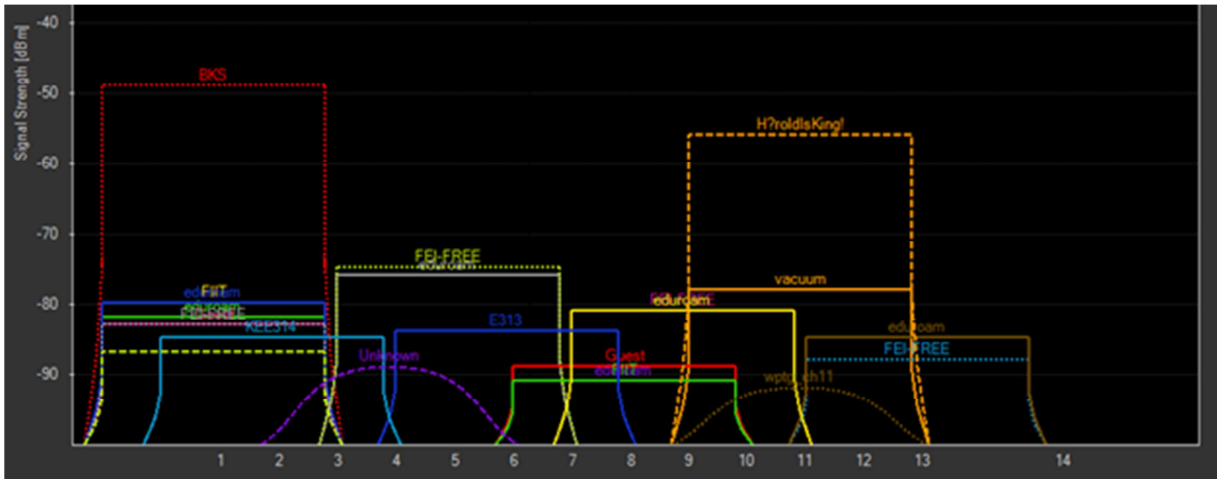
MAC Address	Vendor	SSID	Channel	RSSI	Security	Network Type	Speed	First Seen	Last Seen	Location
00:1D:E5:83:E8...	Cisco Sys...	eduroam	5	-74	WPA-CCMP	Access Point	54	9:18:51	9:21:34	0.00000 , 0.00000
00:1D:E5:83:E8...	Cisco Sys...	FEI-FREE	5	-89	None	Access Point	54	9:18:51	9:21:34	0.00000 , 0.00000
00:18:6E:14:A8:...	3Com Ltd	Guest	1	-80	WPA-TKIP	Access Point	54	9:18:51	9:21:34	0.00000 , 0.00000
00:18:6E:14:A8:...	3Com Ltd	eduroam	1	-80	WPA-CCMP	Access Point	54	9:18:51	9:21:34	0.00000 , 0.00000
00:0D:88:EB:00...	D-Link Co...	BKS	1	-50	None	Access Point	22	9:18:51	9:21:34	0.00000 , 0.00000
00:05:C9:A8:14:...	LG Innote...	vacuum	11	-74	WPA-TKIP	Access Point	54	9:18:51	9:21:34	0.00000 , 0.00000
00:1D:E5:83:F4...	Cisco Sys...	eduroam	13	-256	WPA-CCMP	Access Point	54	9:18:51	9:21:34	0.00000 , 0.00000
02:13:E8:00:03:...		mike	11	-100	WEP	Ad Hoc	54	9:18:51	9:20:41	0.00000 , 0.00000
00:18:6E:14:A8:...	3Com Ltd	FIIT	1	-79	RSNA-CC...	Access Point	54	9:18:51	9:21:34	0.00000 , 0.00000
00:1D:E5:83:F4...	Cisco Sys...	FEI-FREE	13	-85	None	Access Point	54	9:18:51	9:21:33	0.00000 , 0.00000
90:E6:BA:50:45:...		E313	6	-81	WPA-TKIP	Access Point	54	9:18:51	9:21:33	0.00000 , 0.00000
00:1D:E5:83:FB...	Cisco Sys...	FEI-FREE	1	-100	None	Access Point	54	9:18:51	9:20:57	0.00000 , 0.00000
00:1D:E5:83:FB...	Cisco Sys...	eduroam	1	-100	WPA-CCMP	Access Point	54	9:18:51	9:20:53	0.00000 , 0.00000
00:1E:13:07:F5:...	Cisco Sys...	FEI-FREE	9	-81	None	Access Point	54	9:18:51	9:21:34	0.00000 , 0.00000
00:1E:13:07:F5:...	Cisco Sys...	eduroam	9	-256	WPA-CCMP	Access Point	54	9:18:51	9:21:29	0.00000 , 0.00000
00:22:2D:03:CB...	SMC Net...	KEE314	2	-80	RSNA-CC...	Access Point	65	9:18:51	9:21:33	0.00000 , 0.00000
00:13:D3:00:89:...	MICRO-S...	[illegible]	1	-100	WEP	Access Point	54	9:18:51	9:18:51	0.00000 , 0.00000
02:60:88:E7:21:...		wptg_ch11	11	-100	None	Ad Hoc	11	9:18:56	9:20:41	0.00000 , 0.00000
00:18:6E:14:B8:...	3Com Ltd	eduroam	8	-89	WPA-CCMP	Access Point	54	9:18:56	9:21:33	0.00000 , 0.00000
00:18:6E:14:B8:...	3Com Ltd	Guest	8	-89	WPA-TKIP	Access Point	54	9:18:56	9:21:21	0.00000 , 0.00000
00:18:6E:14:B8:...	3Com Ltd	FIIT	8	-88	RSNA-CC...	Access Point	54	9:18:56	9:21:34	0.00000 , 0.00000
00:90:4B:85:D5:...	GemTek ...	Unknown	4	-100	WEP	Access Point	11	9:18:56	9:19:03	0.00000 , 0.00000
00:18:6E:14:A8:...	3Com Ltd	FIIT	12	-89	RSNA-CC...	Access Point	54	9:19:00	9:20:21	0.00000 , 0.00000
00:18:6E:14:A8:...	3Com Ltd	eduroam	12	-100	WPA-CCMP	Access Point	54	9:19:00	9:19:03	0.00000 , 0.00000
00:18:6E:14:A8:...	3Com Ltd	Unknown	12	-100	WPA-TKIP	Access Point	54	9:19:38	9:19:40	0.00000 , 0.00000

Obrázok 1 - zoznam dostupných bezdátových sietí a informácie o nich programom inSSIDer

Pre lepšie grafické znázornenie dostupných sietí, zabezpečenia a ich intenzity signálu ponúka program inSSIDer prehliadanie sietí ako je znázornené na obrázku Obrázok 2. Pre pochopenie diagramu si treba vysvetliť charakteristiku osí a čiar:

- Os X: kanály na ktorých daná sieť vysiela
- Os Y: sila signálu v dBm
- Zaoblené krivky signálu: siete štandardu 802.11 b
- Ostré krivky signálu: siete štandardu 802.11 a/g/n
- Podkovaná krivka: žiadne zabezpečenie komunikácie
- Čiarkovaná krivka: zabezpečenie komunikácie WEP
- Plná krivka: zabezpečenie komunikácie WPA/WPA2

Ako môžeme teda na obrázku Obrázok 2 vidieť, nami skúmaná sieť BKS má podľa týchto pravidiel nezabezpečenú sieť štandardu 802.11g s veľkou intenzitou signálu, ktorá je vysielaná na kanály jeden s prekryvom až na kanál tri.



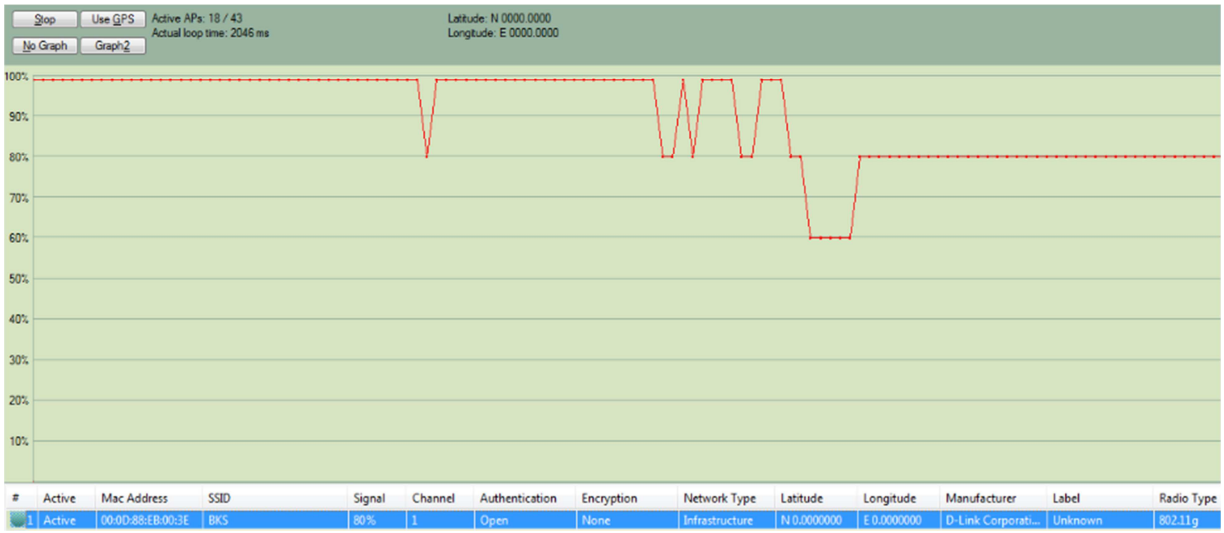
Obrázok 2 - grafické znázornenie intenzity a zabezpečenia sietí programom inSSIDer

Zoznam dostupných sietí sme prezerali aj programom Vistumbler (Obrázok 3) . Program Vistumbler ponúka veľmi podobný pohľad ako inSSIDer. Rozdiel môžeme pozorovať v jednotke intenzity signálu (percentá) a v nových informačných stĺpcoch status siete (aktívna, nedostupná a pod) a použité kryptovanie (tkip, wep, none ...). Osobne mi prišlo grafické používateľské rozhranie prívetivejšie ako pri programe inSSIDer.

#	Active	Mac Address	SSID	Signal	Channel	Authentication	Encryption	Network Type	Latitude	Longitude	Manufacturer
1	Active	00:0D:88:EB:00:3E	BKS	99%	1	Open	None	Infrastructure	N 0.0000000	E 0.0000000	D-Link Corporati...
2	Dead	02:13:E8:00:13:C8	HeroldIsKing!	0%	11	Open	WEP	Adhoc	N 0.0000000	E 0.0000000	Unknown
3	Active	00:18:6E:14:A8:80	FIIT	40%	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	3Com Ltd
4	Active	00:18:6E:14:B8:00	FIIT	25%	8	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	3Com Ltd
5	Dead	00:18:6E:14:A8:84	eduroam	0%	1	WPA-Enterprise	TKIP	Infrastructure	N 0.0000000	E 0.0000000	3Com Ltd
6	Active	00:1D:E5:83:E8:71	eduroam	46%	5	WPA-Enterprise	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Cisco Systems
7	Active	00:18:6E:14:B8:04	eduroam	20%	8	WPA-Enterprise	TKIP	Infrastructure	N 0.0000000	E 0.0000000	3Com Ltd
8	Active	00:1E:13:07:F5:21	eduroam	43%	9	WPA-Enterprise	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Cisco Systems
9	Active	00:1D:E5:83:F4:A1	eduroam	20%	13	WPA-Enterprise	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Cisco Systems
1.	Active	00:1D:E5:83:FB:50	FEI-FREE	41%	1	Open	None	Infrastructure	N 0.0000000	E 0.0000000	Cisco Systems
1.	Active	00:1D:E5:83:E8:70	FEI-FREE	46%	5	Open	None	Infrastructure	N 0.0000000	E 0.0000000	Cisco Systems
1.	Active	00:1E:13:07:F5:20	FEI-FREE	38%	9	Open	None	Infrastructure	N 0.0000000	E 0.0000000	Cisco Systems
1.	Dead	00:1D:E5:83:F4:A0	FEI-FREE	0%	13	Open	None	Infrastructure	N 0.0000000	E 0.0000000	Cisco Systems
1.	Active	00:18:6E:14:A8:86	Guest	40%	1	WPA-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	3Com Ltd
1.	Active	00:18:6E:14:B8:06	Guest	25%	8	WPA-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	3Com Ltd
1.	Active	00:05:C9:A8:14:BD	vacuum	41%	11	WPA-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	LG Innotek Co., ...
1.	Active	90:E6:BA:50:45:27	E313	20%	6	WPA-Personal	TKIP	Infrastructure	N 0.0000000	E 0.0000000	ASUSTek COMP...
1.	Dead	00:22:2D:03:CB:0C	KEE314	0%	2	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	SMC Networks I...
1.	Active	00:22:2D:03:CE:C0	KEE415	18%	2	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	SMC Networks I...
2.	Active	00:1D:E5:83:FB:51	eduroam	41%	1	WPA-Enterprise	TKIP	Infrastructure	N 0.0000000	E 0.0000000	Cisco Systems
2.	Dead	02:60:88:E7:21:0A	wptg_ch11	0%	11	Open	None	Adhoc	N 0.0000000	E 0.0000000	Unknown
2.	Dead	00:90:4B:85:D5:49		0%	4	Open	WEP	Infrastructure	N 0.0000000	E 0.0000000	GemTek Techno...
2.	Dead	00:23:CD:15:93:42	ZOOWIFI	0%	1	WPA2-Personal	CCMP	Infrastructure	N 0.0000000	E 0.0000000	TP-LINK TECHN...
2.	Active	00:18:6E:14:A8:44	eduroam	18%	12	WPA-Enterprise	TKIP	Infrastructure	N 0.0000000	E 0.0000000	3Com Ltd

Obrázok 3 - zoznam dostupných bezdátových sietí a informácie o nich programom Vistumbler

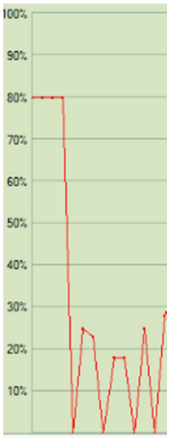
Na obrázku Obrázok 3 môžeme vidieť, že intenzita signálu bola 99%. Táto vysoká hodnota bola spôsobená bezprostrednou blízkosťou pri AP. Aby sme mohli sledovať klesajúcu závislosť intenzity signálu od vzdialenosti od AP začali sme sa pohybovať po miestnosti a skrývať sa za rôzne prekážky. Výsledky možno vidieť na obrázku Obrázok 4. Os X znázorňuje časový priebeh merania a os Y intenzitu meranej bezdrôtovej siete (BKS).



Obrázok 4 - sledovanie závislosti intenzity signálu od vzdialenosti AP programom Vistumbler

Intenzita bola zo začiatku veľmi vysoká, preto sme sa pokúsili pohybovať po miestnosti. Keď sme sa schovávavali za stĺpy alebo stáli na opačnej strane miestnosti, intenzita signálu klesala na 80 %. Po opustení miestnosti intenzita klesla na 60 %. Po návrate späť sa intenzita opäť zvýšila. Podobné správanie sme pozorovali aj v programe inSSIDer.

Po veľkom vzdialení sa od prístupového bodu sme pozorovali prudké poklesy intenzity a výpadky siete (Obrázok 5). Po nastúpení do výťahu sme signál stratili úplne.



Obrázok 5 - pokles intenzity a strata signálu

Na základe analýzy závislosti intenzity od vzdialenosti AP sme došli k zisteniam uvedených v tabuľke Tabuľka 1. Namerané výsledky sa zhodovali s našimi predpokladmi a intenzita s narastajúcou vzdialenosťou naozaj klesala. Hodnoty uvedené v tabuľke nie sú presné, keďže kvalita a intenzita signálu nie je konštantná ale ovplyvnená množstvom faktorov, ako napr.:

- Vzdialenosť AP
- Viditeľnosť AP
- Počet klientov
- Ostatné AP, ktoré vysielajú na rovnakom kanály
- Pohyb ľudí

Intenzita signálu [dBm]	Vzdialenosť od AP [m]
-49	0
-55	4
-67	10
-74	10 (s prekážkou)
-92	15 (poschodie nižšie)

Tabuľka 1 -závislosť intenzity signálu od vzdialenosti AP

Ďalej sme odchytávali a pozorovali rámce bezdrôtovej siete BKS na danom sieťovom rozhraní. K tomu nám poslúžil program WireShark. Následná analýza rámcov sa nám nepodarilo vykonať, keďže sa nám nepodarilo zachytávať riadiace rámce siete zvolenými softvérovými riešeniami Wireshark a Omnipeek.

6. Záver

Na praktickom cvičení č. 1 sme sa oboznámili s parametrami bezdrôtových sietí a s pomocou vhodne zvolených softvérových riešení sme sa naučili tieto parametre merať a analyzovať. Svoje experimenty a zistenia sme vykonávali na testovacej nezabezpečenej sieti BKS a náhodných okolitých sieťach.

Na základe pozorovania a merania parametrov siete BKS, sme dokázali, že intenzita a kvalita signálu na strane prijímača je závislá od vzdialenosti prístupového bodu a od počtu a materiálu prekážok po ceste. Intenzita najvýraznejšie klesala pri väčších vzdialenostiach.

Pozorovali sme intenzitu signálu pri rovnakej vzdialenosti od AP, no raz s prekážkou a raz bez. Zistili sme, že kvalita signálu pri takýchto situáciách výrazne klesá a že priama viditeľnosť AP je najlepším spôsobom pre zachovanie dobrej kvality a intenzity signálu.