VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

MĚŘENÍ V BEZDRÁTOVÉ SÍTI 802.11N SE SKRYTÝMI UZLY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

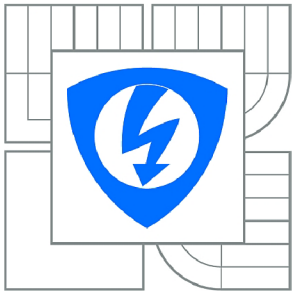
AUTOR PRÁCE
AUTHOR

Bc. ADAM VÁGNER

BRNO 2013

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

MĚŘENÍ V BEZDRÁTOVÉ SÍTI 802.11N SE SKRYTÝMI UZLY

MEASUREMENTS IN AN 802.11N RADIO NETWORK WITH HIDDEN NODES

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

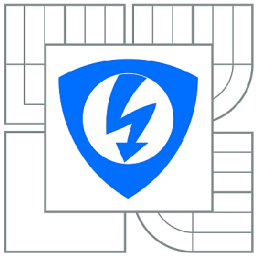
AUTOR PRÁCE — Bc. ADAM VÁGNER

AUTHOR

VEDOUCÍ PRÁCE — Ing. PETR MÜNSTER

SUPERVISOR

BRNO 2013



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Diplomová práce

magisterský navazující studijní obor
Telekomunikační a informační technika

Student:	Bc. Adam Vágner	***ID:***	109738
Ročník:	2	***Akademický rok:***	2012/2013

NÁZEV TÉMATU:

Měření v bezdrátové síti 802.11n se skrytými uzly

POKYNY PRO VYPRACOVÁNÍ:

Cílem diplomové práce je detailně prozkoumat určité parametry vybraných zařízení sítí 802.11n. V radiové měřicí síti projektu Wificolab na UTB ve Zlíně student vytvoří bezdrátovou síť se skrytými uzly. Provede měření minimální citlivosti, potlačení sousedních kanálů (adjacent channel rejection) a citlivosti CCA u vybraných zařízení. Dále provede měření propustnosti sítě se skrytými uzly při použití standardních 802.11 MAC a TDMA MAC vrstev na zařízeních Ubiquity Airmax, Mikrotik Nstreme polling a NV2. Získané výsledky porovná a analyzuje.

DOPORUČENÁ LITERATURA:

[1] Lakshmanan, S.; Jeongkeun Lee; Etkin, R.; Sung-Ju Lee; Sivakumar, R.; , "Realizing high performance multi-radio 802.11n wireless networks," Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2011 8th Annual IEEE Communications Society Conference on , vol., no., pp.242-250, 27-30 June 2011
[2] Zubow, A.; Sombrutzki, R.; , "Adjacent channel interference in IEEE 802.11n," Wireless Communications and Networking Conference (WCNC), 2012 IEEE , vol., no., pp.1163-1168, 1-4 April 2012

Termín zadání:	11.2.2013	***Termín odevzdání:***	29.5.2013

Vedoucí práce: Ing. Petr Münster
Konzultanti diplomové práce:

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

VLOŽIT PRVNÍ LIST LICENČNÍ SMLOUVY

VLOŽIT DRUHÝ LIST LICENČNÍ SMLOUVY

ABSTRAKT

Současná velká koncentrace bezdrátových sítí přináší nové obzory, ale také nové starosti. Při nedodržování základních pravidel mohou vznikat dalekosáhlé problémy, které přidělají vrásky všem dotčeným správcům a administrátorům. Cílem diplomové práce bylo změřit a porovnat rádiové parametry vybraných produktů, zjistit jejich chovaní v sousedním rušení, a určit rychlosti, které dosáhnou při skrytých uzlech.

Výsledné hodnoty byly změřeny v laboratorní síti Wificolab a porovnány s různými podpůrnými protokoly. V práci se pak dále rozebírají případné vlivy na konkrétní situace.

KLÍČOVÁ SLOVA

Mikrotik, Groove, Ubiquiti, Bullet, CCA, 802.11, skryté uzly, Wi-Fi, 802.11n

ABSTRACT

The current large concentration of wireless networks brings new horizons, but also new concerns. Failure to follow basic rules may produce far-reaching problems that could make more wrinkles to all affected managers and administrators. The aim of this thesis was to measure and compare the radio parameters of selected products and how they behave in neighboring interference and the speed they have while there are hidden nodes.

The resulting values were measured in the laboratory network Wificolab and compared with the various support protocols. Possible effects on the specific situation are also analyzed in this thesis.

KEYWORDS

Mikrotik, Groove, Ubiquiti, Bullet, CCA, 802.11, hidden nodes, Wi-Fi, 802.11n

VÁGNER, A. *Měření v bezdrátové síti 802.11n se skrytými uzly*. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2013. 63 s. Vedoucí semestrální práce Ing. Petr Münster.

PROHLÁŠENÍ

Prohlašuji, že svou diplomovou práci na téma „Měření v bezdrátové síti 802.11n se skrytými uzly“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících zákona č. 121/2000Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009Sb.

V Brně dne ....

(podpis autora)

PODĚKOVÁNÍ

Děkuji vedoucímu semestrální práce Ing. Petru Münsterovi za velmi užitečnou metodickou, odbornou a pedagogickou pomoc a další cenné rady při zpracování práce.

Děkuji také panu Ing. Tomáši Dulíkovi Ph.D. za technickou pomoc při testování zařízení a poskytnutí kvalifikovaného měřícího pracoviště.

V Brně dne ....

(podpis autora)

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Stále častěji jsou v médiích, zpravodajských webech a technologických magazínech skloňovány názvy jako: „Nové a vylepšené Wi-Fi sítě“, „S novým standardem Wi-Fi dosáhnete gigabitových rychlostí“ apod. Otázkou zůstává, jak moc jsou tyto zprávy pravdivé. Je však nutné si uvědomit základní principy fungování takových bezdrátových sítí. Jsou to hlavně omezené prostředky rádiového spektra, které nejsou nekonečné a je potřeba s nimi nakládat s rozumem a patřičnou rozvahou. Ve většině případů jsou instalace prováděny neodborně a jsou to právě tyto sítě, které jsou odpovědné za nefunkčnost, či špatné fungování ostatních sítí v okolí. V moderních bezdrátových kartách a zařízeních jsou obvody (vstupní filtry, moderní demodulátory), které se maximálně snaží o filtraci rušení okolních stanic, aby zajistily co nejlepší podmínky pro svou vlastní činnost. Ty dokáží pracovat i ve špatných rádiových podmínkách, ale jsou případy, kdy je rušení natolik extrémní, že tyto všechny jednotky selžou a bezdrátový spoj chybuje, či se úplně rozpojí.

Tato diplomová práce se zaměří na rádiové parametry bezdrátových zařízení a porovná změřené a papírové hodnoty, které jsou uváděny výrobcem. Především se jedná o udávanou minimální citlivost, potlačení sousedních kanálů (adjacent channel rejection) a citlivosti CCA. Dále pak měření propustnosti skrytých stanic u protokolů 802.11, NV2, Nstream a airMAX.

V první části této diplomové práce budou rozebrány základní standardy 802.11 a popsány jejich základní parametry.

V druhé části bude rozebrán standard 802.11n, který pak bude i předmětem všech našich měření.

Předmětem třetí části této práce bude popis měřící sítě pro bezdrátové technologie Wificolab.

V poslední části budou popsána jednotlivá měření a výsledky praktických měření na testovací síti Wificolab.

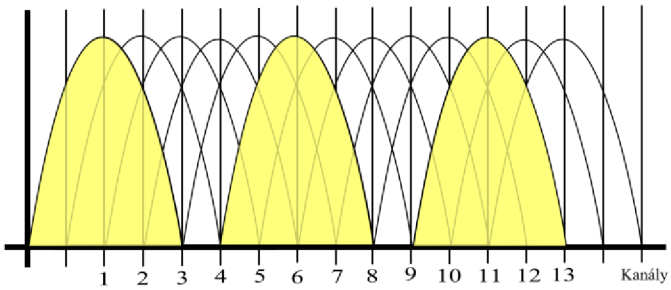
1 STANDARDY 802.11

Standard 802.11 označuje pracovní skupinu patřící pod mezinárodní profesionální organizaci IEEE (Institute of Electrical and Electronics Engineers), která se snaží o vzestup technologií souvisejících s elektrotechnikou a elektronikou. Tato skupina sdružuje odborníky z řad vědeckých a vzdělávacích oborů. IEEE se zasloužilo o více než 900 schválených průmyslových standardů. Využití najdeme v lékařských technologiích, zdravotní péčí, informačních technologiích, telekomunikacích, letectví, dopravě aj. Standard 802.11 je označován jako původní a jelikož byl postupem času pomalý a nevyhovující, vzniklo názvosloví 802.11x. Tento výraz nadále určuje skupiny upravujících doplňků, které jsou odlišeny písmeny. [4]

1.1 802.11b

Vznikl v roce 1999 jako rozšíření původního standardu 802.11 a umožnil tak teoretickou rychlost 11 Mb/s. V praxi je však maximální reálná rychlost 5,9 Mb/s pro TCP a 7,1 Mb/s pro UDP pakety. Využívá se zde přístupové metody CSMA/CA.

802.11b používá modulace DSSS (Direct-Ssequence Spread Spectrum) s CCK (Complementary Code Keying). To znamená, že hlavička a datová část rámce jsou modulovány na jednu nosnou. Proto představuje CCK nejjednodušší mechanismus. Rychlosti jsou na základě intenzity a okolního rušení signálu odstupňované od maximální rychlosti 11 Mb/s, 5,5 Mb/s, 2 Mb/s až po nejmenší rychlost 1 Mb/s. Standard pracuje na bezlicenčním ISM (Industrial Scientific and Medical) pásmu 2,4 GHz a disponuje v České republice 13 kanály. Díky malé šířce pásma jsou k dispozici jen 3 kanály, které se vzájemně nepřekrývají, viz Obr. 1.1. Pásmo 2,4 GHz je velmi náchylné na okolní rušení. Na tomto pásmu pracují i další technologie, jako bluetooth a mikrovlnné trouby. [1][2]



Obr. 1.1: Překrývání kanálu u 802.11b/g na frekvenci 2,4 GHz. [2]

1.2 802.11g

Jedná se o vylepšený standard 802.11b. Vznikl v roce 2003 a pracuje na stejné frekvenci 2,4 GHz. Používá stejné kanálování jako 802.11b. Hlavním rozdílem je použití modulačního schématu s rozprostřeným spektrem OFDM (Orthogonal Frequency-Fivision Multiplexing). Kvůli zachování kompatibility se standardem 802.11b jsou použity i mechanismy CCK. Současné používání b i g nese však jednu zásadní nevýhodu. Připojí-li se klient se starším standardem na vysílač podporující standard g, tak se automaticky rychlost celé WLAN sítě přepne na rychlost 11 Mb/s. [1]

Díky výše uvedenému modulačnímu schématu dosahuje maximální teoretickou rychlost 54 Mb/s. Reálné maximální rychlosti dosahují přibližně 22 Mb/s. Podporované rychlosti v závislosti na modulaci jsou následující: 54 Mb/s (64-QAM), 48, 36, 24 Mb/s (16-QAM), 18 a 12 Mb/s (QPSK), 9 a 6 Mb/s (BPSK). [3][4]

1.3 802.11a

Tento standard vznikl už v roce 1999 ve Spojených státech amerických a byl dovezen do Evropy. Ve většině evropských států tento standard kolidoval s předpisy jednotlivých zemí a provoz není nebo nebyl povolen. Standard disponuje modulačním schématem OFDM a pracuje v pásmu 5 GHz. Kvůli použitému jinému pásmu není kompatibilní s prvky 802.11b/g. V České republice bylo pásmo schváleno v roce 2005.

Velkou výhodou tohoto standardu je menší rušení v pásmu 5 GHz, ve kterém pracuje. Disponuje tak s velkou šířkou pásma a nabízí 8 vzájemně nezávislých a nepřekrývajících se kanálů. [1][4]

2 802.11N

S rostoucími nároky uživatelů rostou i nároky na stále větší rychlosti. Také se zvyšuje potřeba po přenosových technologiích, které jsou schopné takovéto objemy dat přenášet. Hlavním spotřebitelem datových linek jsou přenosy videa a hlavně videa ve vysoké kvalitě (HDTV). Takovéto přenosy mohou v určitých případech využívat jednotky až desítky megabitů za sekundu. Těmto rostoucím požadavkům se snaží vyhovět nový standard 802.11n. Mezi hlavní přínosy tohoto standardu se řadí velká datová propustnost. Ta může mít v ideálním případě rychlost až 600 Mb/s. Oproti předchozím standardům 802.11a/b/g, které umožňovaly rychlost maximálně 54 Mb/s je zřetelně vidět rapidní nárůst propustnosti. Jako další přínos k rychlosti, ale i k lepšímu pokrytí oblasti, slouží použití více antén.

2.1 Historie 802.11n

V lednu 2004 ohlásila organizace IEEE, že vytvořila novou skupinu 802.11 TGn (Task Group), která měla vyvinout nové změny standardu 802.11 pro lokální bezdrátové sítě (WLAN). V té době měla být rychlost nového standardu 540 Mb/s. V porovnání se současnými standardy byl až 40x rychlejší než 802.11b a až 10x rychlejší než 802.11a/g. Předpokladem bylo i dosažení větší provozní vzdálenosti, než současné WLAN sítě.

V té době byly dva konkurenční návrhy standardu 802.11n a to: WWiSE (World-Wide Spectrum Efficiency) opírající se o společnost Broadcom a TGn Sync spoléhající se na společnosti Intel a Philips. [6]

Konkurující si návrhy od TGn Sync, WWISE a třetí MITMOT koncem roku 2005 poslaly do IEEE své návrhy na standard 802.11n. Normalizační proces měl být dokončen v druhé polovině roku 2006. [6]

Bylo vytvořeno rozšířené bezdrátové konsorcium EWC (Enhanced Wireless Consortium) pro urychlení vývoje standardu 802.11n a mělo prosazovat technologie a specifikace pro interoperabilitu zařízení příští generace bezdrátové lokální sítě WLAN. [6]

Toto urychlení mělo za následek vytvoření dvoustupňového řešení, neboli pre-standardu, jinak také označeného jako Draft 1.0. Bylo to z důvodu vyhovění požadavkům trhu. Už v té době se objevovaly produkty 802.11n (draft 1.0), a to z důvodu přítomnosti alespoň minimální kompatibility pro vzájemnou komunikaci, než bude vytvořen definitivní standard. [6]

První verze 802.11n (draft 1.0) mohla být přijata už v roce 2006, ale v hlasování neprošla. Proto se musely nejdříve projednat připomínky k tomuto návrhu a až v březnu 2007 byla schválena druhá verze Draft 2.0. [6]

7.9.2009 bylo nakonec finálně schváleno znění standardu 802.11n. Návrh byl schválen už dříve, ale jen v rámci pracovní skupiny. Nyní však dává výrobcům určitou jistotu, že 802.11n bude opravdu fungovat a bude podporovat jeho maximální rychlost 600 Mb/s. [6]

2.2 Vlastnosti 802.11n

Velkou inovací u standardu 802.11n je fyzická vrstva MAC. Ta umožňuje, jak již bylo dříve řečeno, maximální rychlost 600 Mb/s v kombinaci antén 4x4. V reálném prostředí však těchto rychlostí dosáhnout nelze, a to z následujících důvodů.

Délka trasy spoje. Pokud máme dlouhý spoj, tak vlivem útlumu přenosové trasy dochází k poklesu signálu a spoj se nesynchronizuje na maximální rychlost. Dále s dlouhou trasou souvisí i více rušení, jak od zařízení pracujících ve stejném pásmu, tak i stejných zařízení pracujících v okolí.

Další velkou ztrátu režiemi způsobuje podvrstva MAC. Ta může ubrat z přenosové rychlosti 30-40%. [5]

Pracovní režim Wi-Fi způsobuje další ztráty a to sice Half-Duplex (stanice v jednom okamžiku buď data vysílá, nebo je přijímá). V praxi to znamená, že v ideálním prostředí (bez rušení a dalších ztrát) lze získat reálnou rychlost nanejvýš 300 Mb/s. [5]

Vlastní režii má i síťový protokol TCP/IP. Skutečná rychlost proto přibližně 260 Mb/s. [5]

Další vlastností 802.11n je funkce nazvaná Channel Bonding, neboli spojování kanálů. Standardní norma 802.11a/b/g má šířku 20 MHz. Spojením dvou kanálů získáme ve skutečnosti ještě o něco více než 40 MHz. Děje se tomu tak kvůli ochrannému pásmu mezi kanály. Tato funkce je použitelná pouze v 5 GHz pásmu. Počet nosných frekvencí se tak zvýšil z 52 na 108. Celé pásmo 2,4 GHz má šířku 70 MHz a navíc by bylo nutné povolení od regulačních úřadů. [7]

Na podvrstvě MAC bylo zavedeno spojování rámců. Odpadá tak nutnost čekání mezi rámci a potvrzuje se tak až celá sekvence rámců. Režie se tak snižuje o 25%. Jsou definované dva typy shlukování: [7]

Služby MAC servisní části datových jednotek MSDU (MAC service data unit)

Služby MAC protokolové části datových jednotek MPDU (MAC protocol data unit)

I přes všechna vylepšení a technologie MIMO je standard kompatibilní se staršími 802.11a/b/g. Ovšem i zde platí pravidlo nejslabšího článku v řetězu. Rychlost tedy bude taková, jako je nejpomalejší připojený klient.

2.3 Řízení přístupu k médiu, funkce DCF

Tato metoda je základní přístupová metoda v sítích standardu 802.11. Používá se řízení přístupu založené na metodě mnohonásobného přístupu s detekcí nosné a detekcí kolizí CSMA/CD (Carrier Sense Multiple Access with Collision Detection) nebo mnohonásobného přístupu s detekcí nosné a vyhýbáním se kolizím CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) [12].

Princip koordinační distribuované funkce spočívá v přístupu k médiu s tzv. oknem soutěžení. Velikost tohoto okna je pro každou stanici a třídu dána intervalem CW_{min} a $CW_{max.}$ V případě, že má stanice nachystané data k odeslání, tak detekuje, zda je volné médium. Pokud je médium volné, vygeneruje se náhodné číslo v intervalu <0, w – 1>, kdy w je rovno $CW_{min.}$ Poté začne od tohoto náhodného čísla odpočítávat. Během celého odpočtu stále kontroluje, zda je médium volné. Pokud není, odpočítávání je zastaveno [12].

Pro lepší využití přenosového pásma a zmenšení pravděpodobnosti kolizí je veškerý čas rozdělen na diskrétní úseky. Může se stát, že dojde ke shodné hodnotě dvou nebo více stanic. Díky rozdělení na diskrétní úseky dojde ke stejnému odpočtu a tedy ke kolizi. Tato kolize je detekována a řešena algoritmem, který přeruší vysílání. Následně je zvoleno nové náhodné číslo, avšak z většího intervalu $w=2^n$, kdy n udává počet předchozích neúspěšných pokusů. Odpočítávání poté pokračuje stejným způsobem [12].

2.4 Modulační schémata

Rychlosti u standardu 802.11n jsou určovány podle tzv. MCS (Modulation and Coding Scheme), neboli modulačního schémata. Mezi jednotlivé parametry patří šířka kanálu. Standardně je 20 MHz, ale norma 802.11n umožňuje připojit k řídícímu kanálu ještě další pomocný sousední kanál. Celkem tedy 40 MHz. Dalším parametrem ovlivňující rychlosti v MCS je GI (Guard Interval). Je to ochranný interval, kdy se nevysílá žádná nová informace a slouží tak pro správné přijetí vysílaného symbolu. Rychlost také závisí na kódovacím poměru, který udává poměr mezi počtem

informačních bitů a celkovým počtem bitů. Posledním parametrem je počet použitých antén. Tento parametr se označuje MIMO. V Tab. 2.1 jsou stručně uvedeny rychlosti dle MCS schématu. [8]

Tab. 2.1: Tabulka MCS schémat. [8]

MCS Index	Počet antén	Typ Modulace	Kódovací poměr	Datová rychlost (Mb/s)			
				20MHz kanál		40MHz kanál	
				GI 800ns	GI 400ns	GI 800ns	GI 400ns
0	1	BPSK	1/2	6,5	7,2	13,5	15
1	1	QPSK	1/2	13	14,4	27	30
2	1	QPSK	3/4	19,5	21,7	40,5	45
3	1	16-QAM	1/2	26	28,9	54	60
4	1	16-QAM	3/4	39	43,3	81	90
5	1	64-QAM	2/3	52	57,80	108	120
6	1	64-QAM	3/4	58,5	65	121,5	135
7	1	64-QAM	5/6	65	72,2	135	150
8	2	BPSK	1/2	13	14,4	27	30
…							
15	2	64-QAM	5/6	130	144,4	270	300
…							
23	3	64-QAM	5/6	195	216,6	405	450
…							
31	4	64-QAM	5/6	260	288,9	540	600

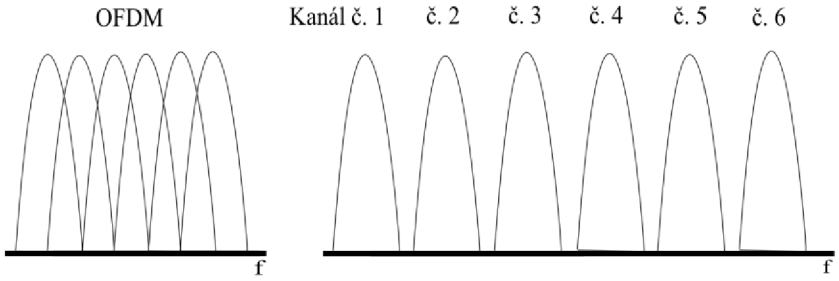
2.5 OFDM

Systém OFDM je dalším krokem ve standardech 802.11. Zkratka OFDM (Orthogonal Frequency Division Multiplexing) označuje techniku ortogonálního multiplexu s kmitočtovým dělením. Tento systém nachází uplatnění v mnoha bezdrátových technologiích. OFDM je také zaveden v pozemní televizi DVB-T, Wi-Fi, WiMax a mobilních sítích čtvrté generace LTE (Long Term Evolution).

Princip OFDM spočívá v použití desítek až tisíců nosných kmitočtů. Tyto

jednotlivé nosné jsou pak dále modulovány modulacemi (QPSK nebo vícestavové QAM). Jednotlivé nosné jsou vzájemně ortogonální. Z toho vyplývá, že maximum každé nosné se překrývá s minimy ostatních nosných. Datový tok se tedy dělí na stovky dílčích datových toků jednotlivých nosných. Poněvadž jsou ve výsledku toky na jednotlivých nosných malé, je možné vkládat ochranný interval (GI). To je čas, kdy se nevysílá žádná nová informace a na přijímací straně je tedy možné přijmout právě vysílaný symbol. OFDM využívá vícecestného šíření právě kvůli malé modulační rychlosti na jednotlivých nosných vlnách [14], [15].

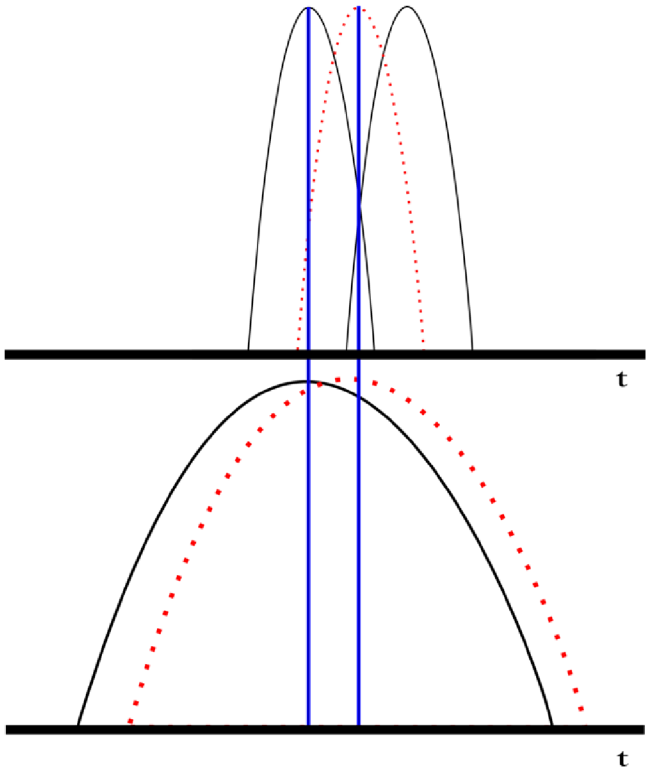
Srovnáním ortogonálního a neortogonálního spektra je vyobrazeno na obrázku 2.1. U klasického systému jsou kanály mezi sebou odděleny ochrannou mezerou, aby nedocházelo k překrývání. U ortogonálního systému se jednotlivé kanály překrývají, ale díky tomu, že jsou ortogonální, nedochází k vzájemnému ovlivňování. Děje se tomu tak kvůli podmínce ortogonality. Ta definuje, že nosné jednotlivých modulátorů jsou od sebe vzdáleny o celočíselný násobek převrácené hodnoty délky symbolu [14], [15].



Obr. 2.1: Srovnání spekter ortogonálního systému a neortogonálního [15].

V rádiovém venkovním prostředí se vyskytují překážky. Můžou to být ulice ve městech, budovy, různé geografické nerovnosti aj. Tyto překážky vedou k tomu, že se vysílaný signál odráží a vznikají intersymbolové interference ISI (Inter Symbol Interference). Těmito chybami vzniká BER (Bit Rate Error). Systém OFDM řeší intersymbolové odrazy mechanismem prodloužení bitové periody, jak je uvedeno na obrázku 2. [15]

Vliv odraženého signálu a vznik ISI je vyobrazen tečkovaným stylem čáry. V horní části obrázku je patrné velké posunutí v časové oblasti vlivem odraženého signálu při použití malé bitové periody. Velké posunutí tohoto signálu bude rapidně ovlivňovat výsledný signál. Vlivem toho roste bitová chybovost BER. V dolní části obrázku je vyobrazení přijímaného signálu za použití velké bitové periody. Při stejně velkém zpoždění, vyobrazeném modrými svislými čarami, dochází k posunutí odraženého signálu o malou hodnotu. Rušivý signál bude v druhém případě ovlivňovat pouze nepatrně. Touto technikou se omezí ISI a i bitová chybovost BER bude nízká [14], [15].



Obr. 2.2: Srovnání odraženého signálu při různých bitových periodách

2.6 Modulace

Modulace je nelineární proces, pomocí něhož se vysokofrekvenční nosná vlna ovlivňuje pomocí nízkofrekvenčního informačního signálu. Modulace rozdělujeme na analogové a digitální. Modulaci zavádíme z důvodu přizpůsobení signálu, na takový signál, aby jej bylo možné efektivně přenášet. Na každý určitý typ přenosové technologie je optimální jiný typ modulace. Určité modulace mají své výhody a nevýhody a podle něj se určuje použitelnost určitého typu modulace. V tabulce 2.2 jsou uvedeny modulace standardu 802.11a/g a jejich základní parametry.

S ohledem na téma práce se zaměříme na modulace, které jsou obsaženy ve standardech Wi-Fi 802.11 a to jsou: [15]

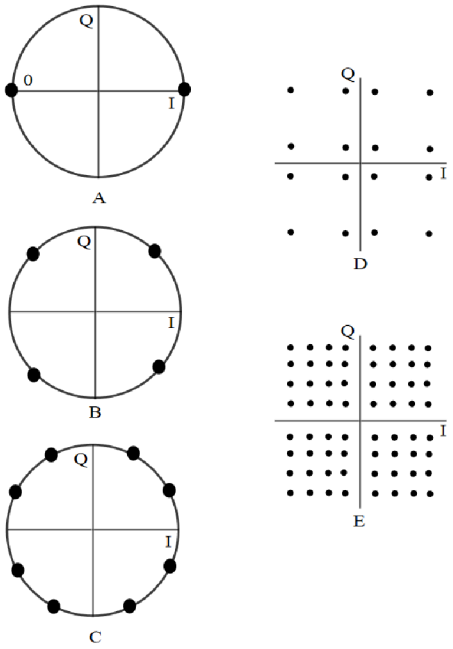
PSK (Phase-Shift Keying)

2PSK nebo také BPSK

4PSK nebo také QPSK

8PSK

QAM (Quadrature Amplitude Modulation)



Obr. 2.3: Konstelační diagramy a) BPSK b) QPSK c) 8PSK d) 16-QAM e) 64-QAM [15].

Na obrázku 2.3 jsou vyobrazeny stavové diagramy jednotlivých modulací. U PSK modulací je využívána změna velikosti úhlu fáze a podle počtu fázi jsou 2PSK, 4PSK a 8PSK. QAM modulace je kombinace amplitudové a fázové modulace a umožňuje nám zvýšit počet stavů a tím i vetší přenosovou rychlost. QAM modulace je však náročná na rozpoznání signálu v přijímači a vyžaduje lepší poměr odstupu signál/šum [15].

Tab. 2.2: Přehled modulací v 802.11a/g [2].

Modulace	Kódový poměr	Počet všech bitů na subkanál	Počet bitů na OFDM symbol	Počet datových bitů na OFDM symbol	Přenosová rychlost pro 20 MHz kanál [Mb/s]
BPSK	1/2	1	48	24	6
BPSK	3/4	1	48	36	9
QPSK	1/2	2	96	48	12
QPSK	3/4	2	96	72	18
16-QAM	1/2	4	192	96	24
16-QAM	3/4	4	192	144	36
64-QAM	1/2	6	288	192	48
64-QAM	3/4	6	288	216	54

3 WIFICOLAB

Wificolab je měřící a testovací rádiová síť přizpůsobená na měření bezdrátových technologií Wi-Fi v pásmech 2,4 GHz a 5 GHz. Tato síť vznikla v letech 2009 – 2012 na univerzitě Tomáše Bati ve Zlíně pod vedením Ing. Tomáše Dulíka, Ph.D. a stále se vylepšuje. Na této síti je možné měřit rádiové parametry jakéhokoliv Wi-Fi zařízení na standardech 802.11a/b/g/n. Síť obsahuje spoustu profesionálních měřících přístrojů, které zajistí velmi kvalitní výstup pro další aplikace.

3.1 Popis měřící sítě

Měřící síť Wificolab dokáže pojmout až 24 zařízení při konfiguraci jedné antény MIMO 1x1. Při použití 2 antén MIMO 2x2 se počet zařízení sníží na 12. Z toho vyplývá, že máme k dispozici celkem 24 portů typu F male. Na každém vstupu před slučovačem jsou zapojeny pevné útlumové články o hodnotě -10/-20/-30 dB pro různé větve měřící sítě. Tyto články jsou především na prvotní utlumení signálu z rádiových částí. Dále jsou ze systematicky oddělených částí sloučeny trasy, které dále vedou do programovatelných útlumových článků. Tyto články lze využít k mnoha simulacím, ať už se jedná o skryté uzly, vložení libovolného útlumu apod. Tyto programovatelné útlumové články jsou zapojeny ve skupině 3 x 4 vstupy. To nám dává jistou variabilitu zapojení koncových zařízení ke konkrétnímu testu. Bylo by dobré mít programovatelné útlumové články u každého zařízení, ale jelikož jsou tyto články velmi nákladné, vznikl tak určitý kompromis v podobě sloučení několika zařízení na jeden článek. Určitou náhradou za programovatelné články může být regulace výkonu provedená přímo na měřeném zařízení.

Tyto 3 větve jsou dále propojeny se slučovači, které neobsahují programovatelné články. V centru této vzájemně propojené sítě je pomocí děliče vyveden přívod pro signálový analyzátor, kterým se může sledovat úroveň signálu, parametry rádiových částí jako jsou konstelační diagramy, frekvenční masky, spektrum a mnoho dalšího. Použitý analyzátor umí však i analyzovat kompletní standard 802.11a/b/g/n a porovnává s normou IEEE pro 802.11a/b/g/n. Analyzátor je však možné díky redukcím připojit na téměř libovolné místo v měřící síti.

Další velmi významnou částí této sítě je přítomnost signálového generátoru. Při testech bylo zjištěno, že při rušení ve vedlejším kanále a při měření CCA, nejsme schopni garantovat nepřerušený provoz. Proto zde máme k dispozici tento signálový generátor, který je schopen vygenerovat tok dat standardu 802.11a/b/g/n. Při použití

těchto dvou generátorů jsme schopni vytvořit vedlejší kanály z obou stran spektra. Takový nepřetržitý surový signál by nám žádné obyčejné zařízení nemohlo vygenerovat.

V další části měřící sítě se zaměříme na vybavení programové a hardwarové části. Veškeré zařízení se nachází v 19“ racku. Měřící síť obsahuje několik serverů. Mezi ně patří 3 malé nettop PC s operačním systémem linux. Tyto servery jsou využívány především na generování datového toku přes testovaná zařízení. Další hlavní části jsou 2 nastavitelné přepínače. Ty plní hlavní funkci propojení všech serverů, jednotek a možnosti vzdáleného ovládání. Pro tyto účely se používá technologie VLAN. Ta nám v rámci přepínače udělá oddělené virtuální sítě. Pak můžeme vzdáleně měnit strukturu sítě, aniž bychom museli fyzicky přepojovat kabely. Pro vzdálené ovládání, či vypínání nám poslouží zařízení Netio, které umí ovládat napájecí zásuvky. Toho lze dobře využít v případě, kdy se nám nějaké zařízení zasekne nebo bude z jakéhokoliv důvodu nedostupné a bude vyžadovat vzdálený restart.

Poslední částí vybavení měřící sítě jsou záložní zdroje UPS. Ty si nakonec uživatel může volitelně nastavit, jak bude potřebovat. Primárně jsou zálohovány všechny linuxové servery, protože při neregulérním ukončení může hrozit poškození těchto serverů a nemusí už správně nastartovat.

Jak již bylo zmíněno, celé měření je při správném nastavení možné realizovat vzdáleně. Prvky, jako jsou testovaná zařízení, která mají standardně jednu adresu a přidělený interní rozsah skrytý za překladačem adres NAT, jsou přístupná pouze z vnitřní sítě. Zařízení typu server, analyzátory nebo přepínače, mají nastaveny jak pevné veřejné IP, tak i interní. Do interní sítě je možné se připojit pomocí VPN a pracovat téměř jako fyzicky na daném místě. Omezený počet docházejících veřejných IP adres nám nedovolí přiřazení každému zařízení veřejnou IP. Také valná většina námi používaných a testovaných zařízení neumožnuje, či nepodporuje nový protokol IPv6. Proto je zde IP síť řešena takto hybridně.

3.2 Příprava konkrétní měřící sítě a vzdálený přístup

Před samotným zapojováním bylo nutné danou síť navrhnout a naplánovat rozložení jednotlivých komponent. V takové měřící síti, kdy chceme mít v jednom přepínači zapojené všechny prvky, bylo prvotním úkolem zabezpečit, aby nevznikaly smyčky. Bezdrátové jednotky jsme měli kvůli maximální transparentnosti nastaveny v módu WDS bridge. Tento mód umožňuje plně transparentní přenos rámců a IP paketů. Tím pádem se chová, jakoby byly porty v přepínači vzájemně přímo propojené kabelem. To

by způsobilo vznik smyčky v přepínači a síť by nefungovala.

Při zkušebním zapojení jsme vyzkoušeli, zda jev smyček opravdu nastane. Po připojení zařízení Ubiquiti Bullet M5 v modu WDS bridge se tomu tak stalo. Síť po malé chvíli přestala fungovat a bylo nutné prvky odpojit. Ten samý test jsme provedli se zařízením Mikrotik Groove. Zde však zmíněný jev nenastal a síť fungovala dále bez problému.

Jak již bylo řečeno, použili jsme technologii VLAN. Ta v rámci přepínače dokáže oddělit porty, které mezi sebou nemohou vzájemně na linkové vrstvě komunikovat. V nastavení přepínače jsme tedy izolovali porty klientských měřených prvků. Jednotlivé porty jsme přiřadili do VLAN skupin typicky podle portu ve které byly zapojeny. V konečném stavu byly nakonec vytvořeny 4 VLAN skupiny. Přístup na klientské zařízení byl potom možný pouze přes spoj vytvořený rádiovou sítí. Pokud bychom však přeci jenom chtěli vzdáleně vstoupit do tohoto zařízení, tak je nutné rozpojit rádiový spoj a odpojit konkrétní port z dané VLAN skupiny.

V návaznosti na tyto vytvořené 4 virtuální sítě můžeme libovolně měnit seskupení portů, které budou právě v těchto skupinách. Pro účely testu bylo tedy nutné ke každé z 2 připojených stanic připojit server pro vytvoření datového toku. Tímto docílíme toho, že datový tok k serverům půjde přes měřené jednotky a ne přímou cestou v přepínači.

V posledním kroku bylo nutné vytvořit vzdálený přístup do lokální sítě. V měřící síti je k dispozici vyhrazený privátní rozsah 192.168.100.0/24 pro přístup v rámci univerzity UTB. Tento rozsah nemá standardně přístup k internetu a není možné se do této sítě běžně připojit. Dále je v sítí dostupný veřejný rozsah univerzity, který poskytuje veřejné IP adresy z DHCP serveru. Do sítě se tedy připojil další router Mikrotik RB600, který plní funkci VPN serveru. Router si vezme z DHCP serveru veřejnou IP, přes kterou se pak následně bude možné připojit do interní LAN sítě. VPN připojení funguje na protokolu PPTP a vytvořený tunel je šifrován. VPN server je nastaven tak, že jednotlivým uživatelům přiřazuje IP adresy přímo do interního rozsahu 192.168.100.0/24 pro měřící síť. Tváří se pak, jakoby byli fyzicky připojení v lokální síti. Router dále zajišťuje přístup do internetu, kde pomocí NATu jsou překládány interní adresy na veřejnou IP z DHCP serveru. Uživatel má tedy možnost připojení na interní rozsah díky VPN serveru a zároveň může přistupovat i do internetu.

3.3 Soupis vybavení

Servery:

2x Intel ATOM se systémem OS Linux Debian pro testy Iperf

1x Alix 1D se systémem OS Linux Debian pro testy Iperf

1x Alix 3D3 s OS Linux pro řízení programovatelných útlumových článků

Rádiové měřící pole:

Programovatelné útlumové články Aeroflex Weinschel 3406T-55, 3406T-103

Pevné útlumové články Mini-Circuits VAT -30/-20/-10 dB

Slučovače Mini-Circuits ZN4PD1-64-S+ 4 x vstup, 1 x výstup

Slučovače Mini-Circuits ZX10R-14-S+ 2 x vstup, 1 x výstup

Propojovací kabely N male/RSMA

IP síť

2x Nastavitelné přepínače DLink DGS-1210-24 a 3Com4210

3x Ubiquiti Bullet M5 verze 5.5.4

3x Mikrotik Groove 5Hn verze 5.25

1x WaveRF 12ti portový pasivní POE injektor panel

1x Signálový analyzátor R&S FSV7

1x Signálový generátor R&S SMBV100A

1x Dálkově ovládané zásuvky NETIO-230A

1x RB600 s OS Mikrotik pro VPN přístup

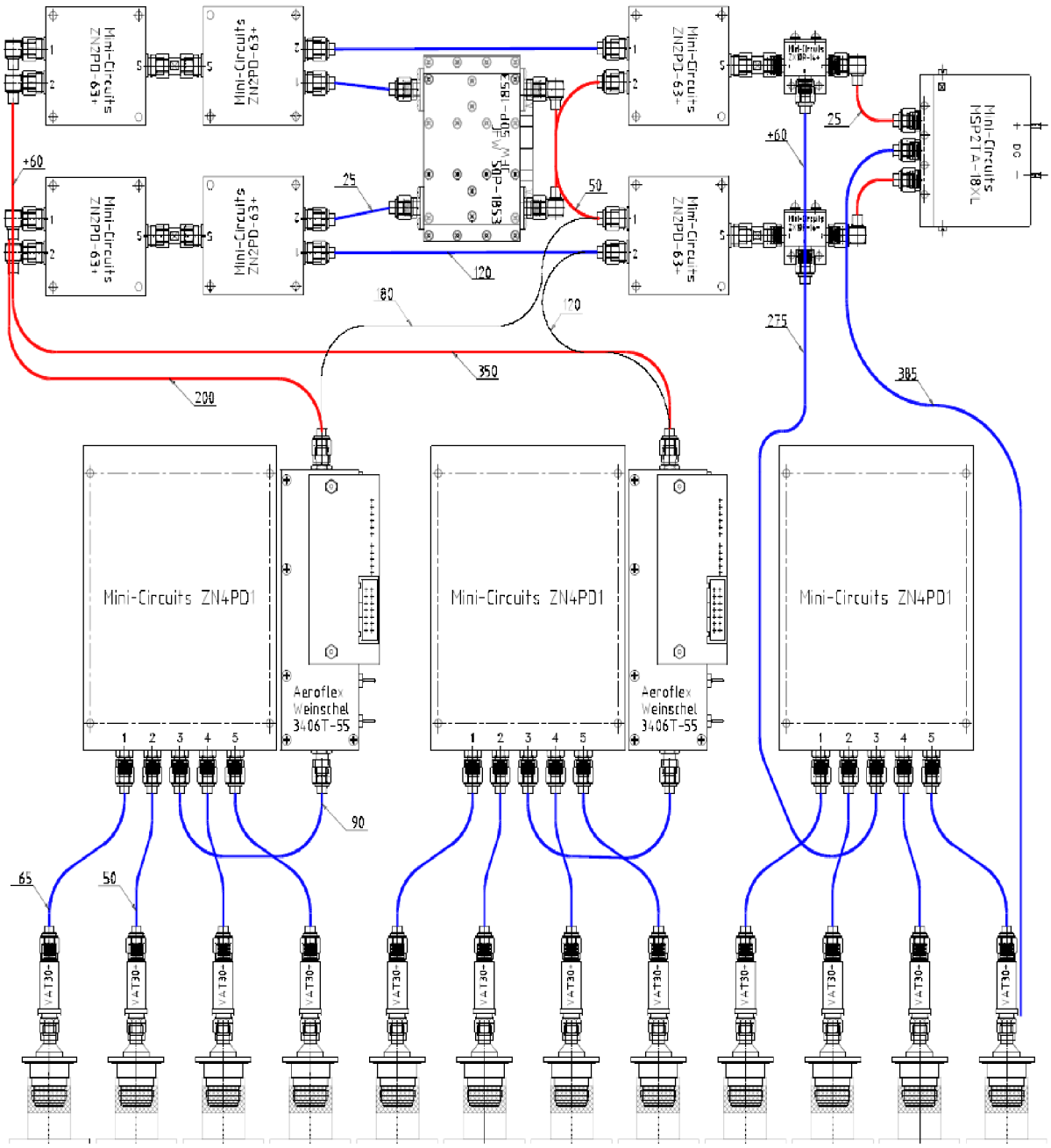
3.4 Schéma zapojení

3.4.1 Propojení rádiové části

Obr. 3.1: Vnitřní propojení rádiové části [9]

Celkové reálné schéma zapojení rádiové části je vyobrazeno na obr. 3.1. Přední panel tvoří 24 F male konektoru. Ty jsou vyvedeny do slučovačů. Vývod ze slučovače vede do programovatelného útlumového článku. Ty jsou pak dále sloučeny a spojeny s ostatními bloky. Uprostřed se nachází řídící jednotka pro útlumové články. Ta je následně přes sériový port řízena příkazy z linuxového serveru.

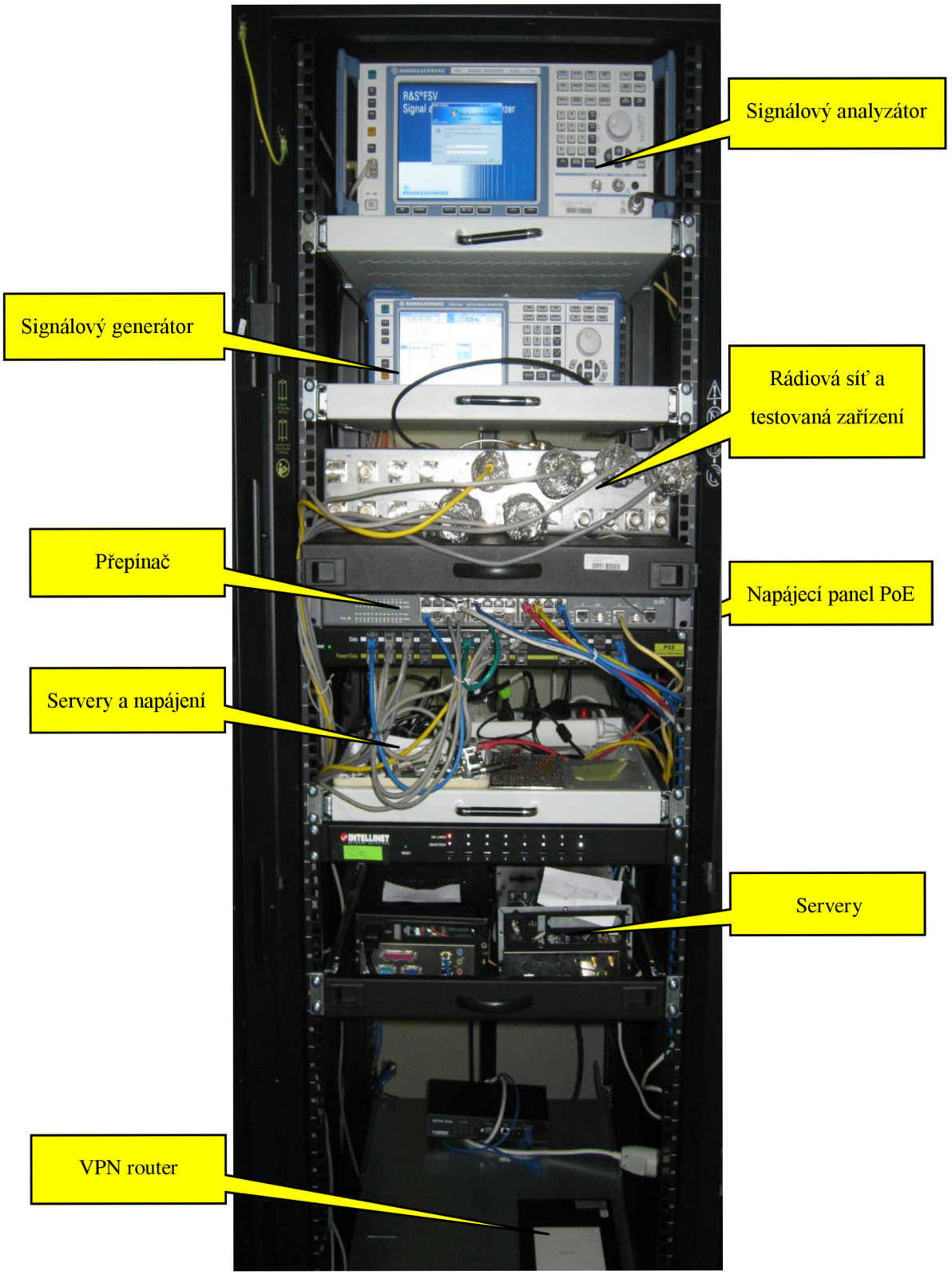
3.4.2 Schématické zapojení rádiové části



Obr. 3.2: Schématické zapojení rádiové části [9].

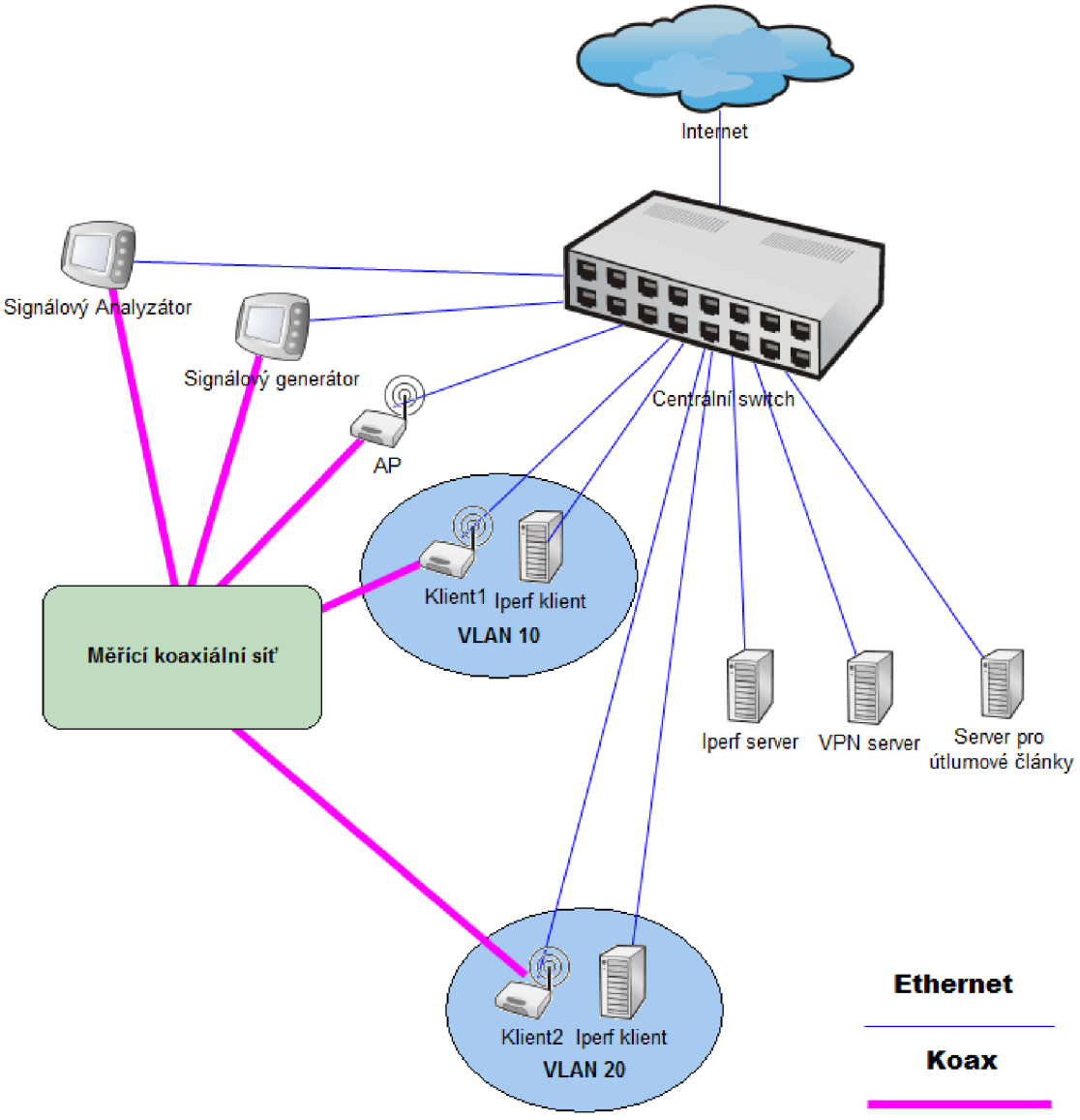
Na obr. 3.2 je detailně a přesně vyobrazeno zapojení rádiové sítě

3.4.3 Celkový náhled na pracoviště



Obr. 3.3: Celkový náhled na zapojený rack.

3.4.4 Detailní zapojení IP sítě



Obr. 3.4: Zapojení IP a rádiové sítě

4 PRAKTICKÉ MĚŘENÍ

Praktická část této diplomové práce spočívá ve změření rádiových parametrů standardu 802.11n. Pro měření byla zvolena 2 testovaná zařízení. Jsou to Ubiquiti Bullet M5 a Mikrotik Groove 5Hn

4.1 Měřící metody

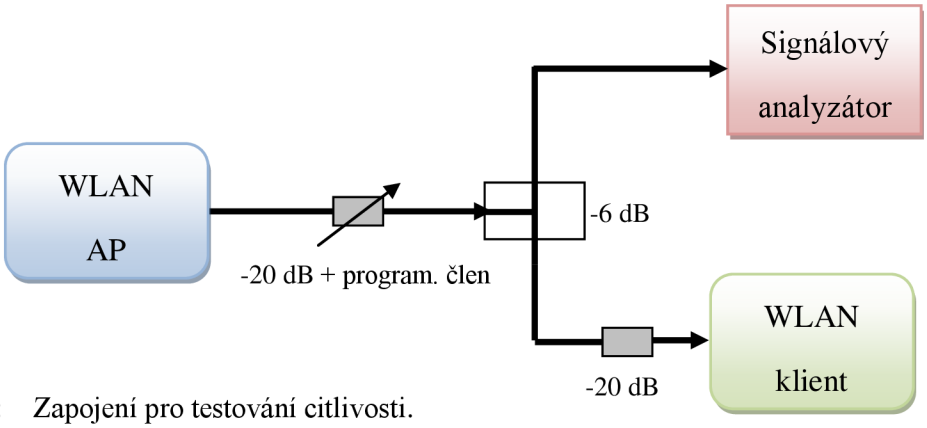
4.1.1 Měření minimální citlivosti

V tomto měření se bude zjišťovat minimální úroveň citlivosti zařízení. Prakticky se bude jednat o test, kdy se zapojí do testovací sítě Wificolab 2 zařízení, která budou spojena, a přes tyto spojené jednotky bude probíhat síťový provoz z generátoru datového toku. Při tomto testu budou otestována modulační schémata MCS 0 – 7 dle tabulky Tab. 2.1. Prakticky se bude zvyšovat útlum pomocí programovatelného útlumového článku na trase mezi jednotkami a podle ztrátovosti paketů, která dle normy pro měření IEEE u 802.11n nesmí přesáhnout paketové ztrátovosti PER 10%. [9]

Pro příklad je zde uvedena tabulka s modulačními rychlostmi a minimálními citlivostmi dle normy IEEE pro standard 802.11n, které by mělo splňovat každé zařízení nesoucí tuto certifikaci.

Tab. 4.1: Požadavky na přijímač pro standard 802.11n [8].

MCS Index	Typ Modulace a rychlost v Mb/s	Kódovací poměr	Potlačení vedlejšího kanálu [dB]	Potlačení vzdálenějšího kanálu [dB]	Min. citlivost 20 MHz Kanál [dBm]	Min. citlivost 40 MHz Kanál [dBm]
0	BPSK (6,5)	1/2	16	32	-82	-79
1	QPSK (13)	1/2	13	29	-79	-76
2	QPSK (19,5)	3/4	11	27	-77	-74
3	16QAM (26)	1/2	8	24	-74	-71
4	16QAM (39)	3/4	4	20	-70	-67
5	64QAM (52)	2/3	0	16	-66	-63
6	64QAM (58,5)	3/4	-1	15	-65	-62
7	64QAM (65)	5/6	-2	14	-64	-61

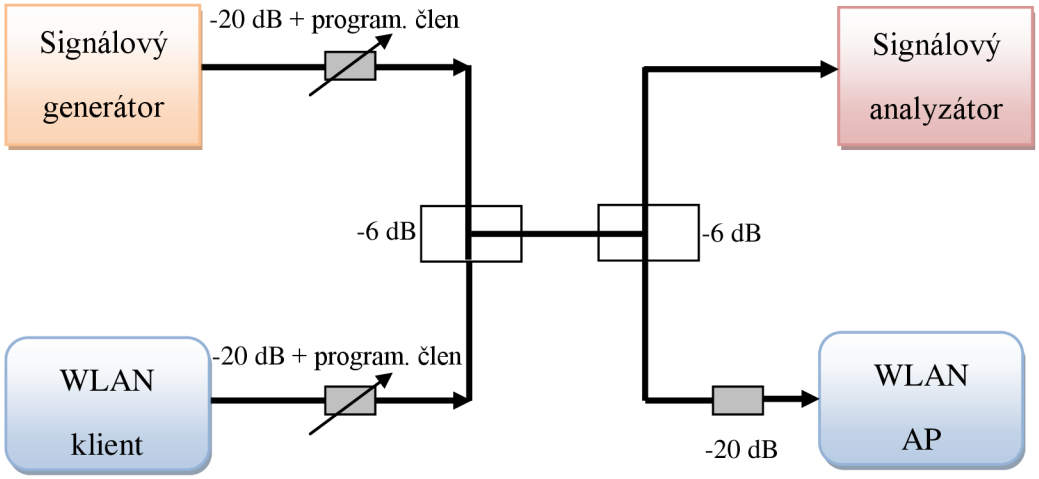


Obr. 4.1: Zapojení pro testování citlivosti.

4.1.2 Potlačení sousedních kanálů (Adjacent Channel Rejection)

Pro spolehlivý souběh zařízení pracujících na stejném místě či vysílači je nutné, aby tato zařízení dokázala pracovat při těsném kanálovém upořádání. Tyhle problémy jsou řešitelné více způsoby. Např. existují zařízení, která vysílají na stejném kanále na jednom vysílači a přitom se vzájemně neruší. Toho dosáhnou díky synchronizaci TDMA, kdy všechna zařízení mají k dispozici přesně synchronizovaný čas z GPS a podle toho vysílají jen v tom okamžiku, kdy ostatní stanice nevysílají. V našem případě se však bude jednat o měření koexistence kanálů vedle sebe. Toto měření bude vycházet opět z doporučeného měření IEEE pro 802.11n, které udává nastavení úrovně sousedního kanálu nad hranicí citlivosti z tabulky 4.1 o 3dB. Dále zvyšováním výkonu sousedního kanálu do paketové ztrátovosti PER 10%.

Obrázek 4.2 znázorňuje jednoduché schéma situace, kdy je rovnocenně umístěno WLAN AP proti své stanici s rušícím generátorem. Pokud chceme napodobit reálnou situaci, tak je nutné, aby signál z připojeného klienta byl menší, než z generátoru. Programovatelné útlumové členy v obou signálových cestách nám umožní stanovení úrovně signálu na libovolné hodnoty.



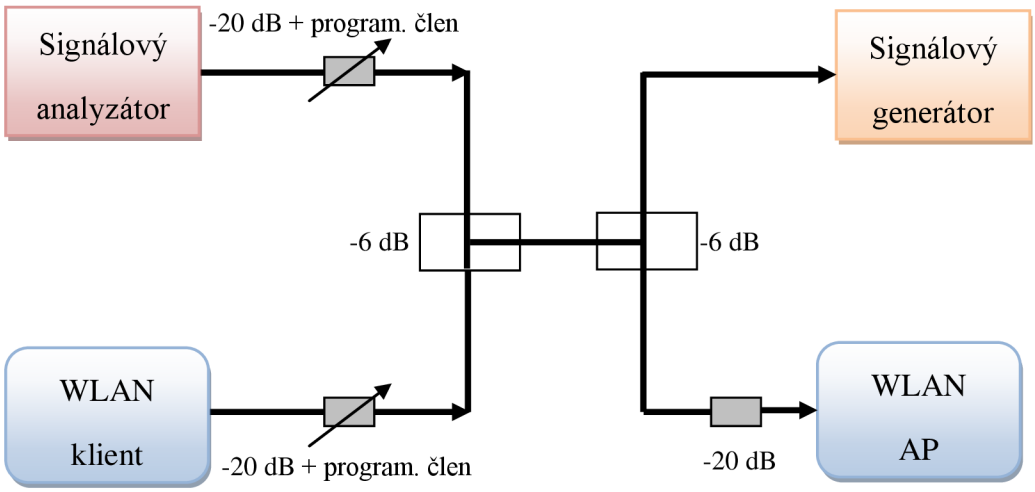
Obr. 4.2: Zapojení pro testování potlačení rušeni v přilehlém kanále.

4.1.3 Citlivost CCA (Clear Channel Assessment)

Wi-Fi sítě využívají pro přístup k médiu přístupové metody CSMA/CA. Ty fungují na principu naslouchání okolí. Před začátkem vlastního vysílání přístupový bod naslouchá v okolí určitou dobu a na základě zda je prostředí volné, zahájí vysílání. Pokud z nějakého důvodu zjistí, že je prostředí obsazené, tak vyčkává. Jakmile bude prostředí volné, zahájí své vysílaní.

Právě tento mechanismus zajišťuje funkce CCA, která je implementovaná v podvrstvě PLCP (Physical Layer Convergence Procedure) a určuje připravenost fyzického média k vysílání. Cílem tohoto měření je prokázat, že tyto funkce pracují u zařízení správně. Hlavním důvodem je fakt, že vysílač, který zjistí svým měřením, že je rádiové prostředí volné, a tedy může vysílat, v jistých případech stejně nevysílá. To má za následek degradaci rychlosti takového spoje.

V tomto měření budeme pozorovat chování WLAN AP při okolním rušení, které vygenerujeme signálovým generátorem. Ten nám zajistí nepřetržitý datový provoz. Souběžně s tímto datovým tokem budeme pouštět přes spoj data a sledovat, kdy přestane zařízení vysílat. Schéma tohoto zapojení je vyobrazeno na Obr. 4.3. Signálový generátor zde bude sloužit jako kontrola signálů a náhled ve spektru [9].



Obr. 4.3: Zapojení pro testování CCA.

4.1.4 Skryté uzly

Problém skrytého uzlu vychází ze samotné standardů 802.11a/b/g/n, který byl navržen především do interních prostor, domů, kanceláří apod. S tím počítají i techniky, které řídí přístup na médium a to je metoda CSMA/CA. Ideální stav je ten, kdy jsou klientské

stanice blízko sebe, slyší se a navzájem se domlouvají, kdy budou vysílat. S tím počítá i metoda CSMA/CA.

Problém nastává v okamžiku, kdy je klientská stanice připojena z větší vzdálenosti než ostatní stanice, nebo při použití vysoce směrových antén. V tomto případě ostatní stanice o této vzdálené nevědí. Jakmile začne datový tok stoupat a vysílá více stanic a současně i vzdálená stanice, tak vlivem toho, že o ní ostatní stanice nevědí, nastávají situace, kdy vysílají 2 stanice najednou. V tomto případě na přístupovém bodě nastává kolize a rychlost rapidně klesá. Nejvíce se z podstaty problému projevuje odchozí rychlost od uživatele.

Proti této špatně identifikovatelné příčině se dá použít mechanismus pod zkratkou RTS/CTS. Odesláním rámce RTS žádá stanice o rezervaci média na dobu, po kterou bude trvat přenos následujícího datového rámce, včetně jeho potvrzení rámcem ACK (Acknowledgement). Pokud cílová stanice obdrží požadavek RTS a je schopná přijímat data, potvrdí příjem vysláním rámce CTS. Z důvodu výskytu různých přenosových rychlostí musí být RTS/CTS vysíláno tak, aby je byly schopny zachytit všechny stanice. To znamená, že jsou vysílány nejnižší přenosovou rychlostí, která se v síti může vyskytnout, a tím pádem může být doba jejich přenosu srovnatelná s dobou přenosu delších datových rámců vysílaných vyšší rychlostí. Při nepodporování RTS/CTS dochází k tomu, že klientská stanice nepošle CTS a přestane vysílat. Těmito režijními požadavky velmi klesá přenosová rychlost. Problematickou částí je i špatná správa klientů, kdy je nutné hodnoty RTS a CTS nastavovat u každého klienta zvlášť.

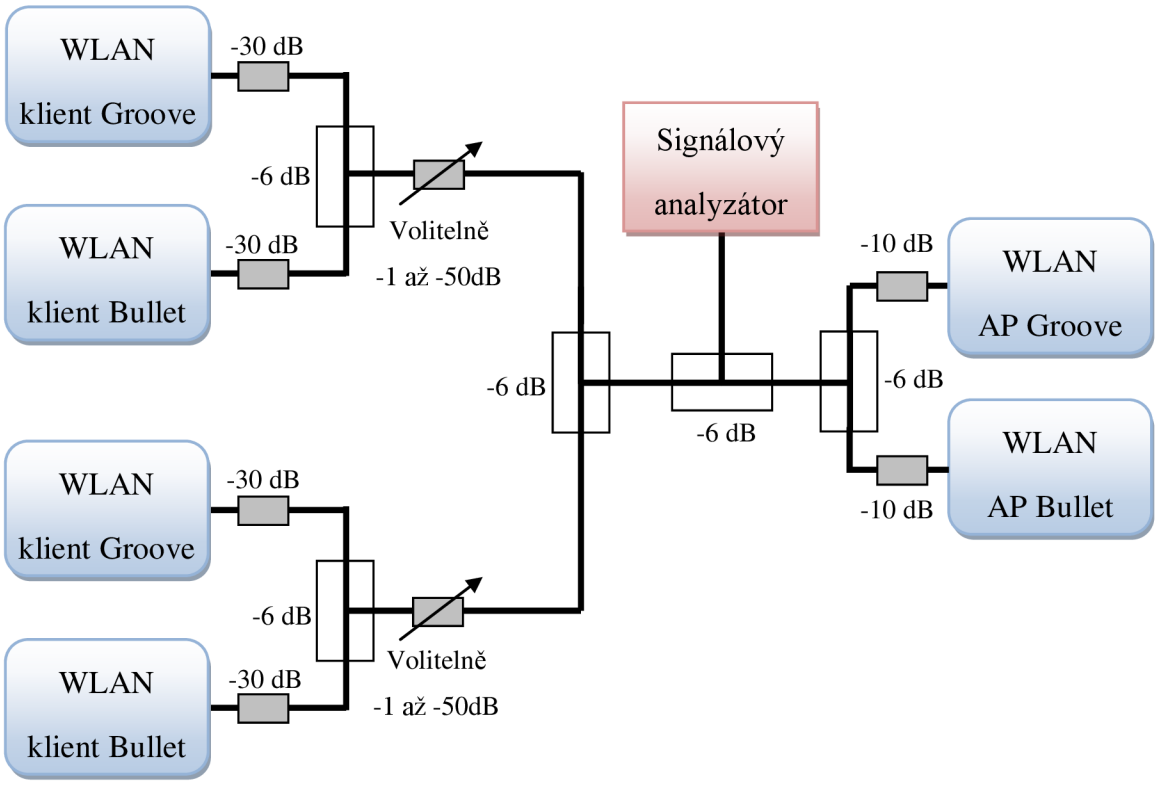
V našem měření vyzkoušíme, jak se s těmito problémy vyrovnají testovaná zařízení. Právě speciální protokoly airMAX a NV2 založené na technologii TDMA (Time Division Multiple Access) by měly problém skrytých uzlů odstranit. Technologie TDMA je známá především z mobilních GSM technologií. Funguje na principu přidělování časových úseků neboli timeslotů. Tímto má každá stanice rezervován čas na své vysílaní.

Na obrázku 4.4 je uvedeno schéma zapojení pro měření skrytých uzlů. Výhodou měřící sítě Wificolab je dostatečná kapacita na připojení všech námi požadovaných testovaných vzorků. Proto se zde zapojily obě technologie najednou a není nutné při měření dále manipulovat se sítí. Soustava je složená z 2 WLAN AP, které pracují v režimu přístupového bodu. Na tyto WLAN AP se připojují příslušné klientské stanice dané technologie. Pro sledování rádiového prostředí v měřící koaxiální síti slouží připojený signálový analyzátor. Pro kompletní zapojení pro test nejsou v obrázku uvedeny servery pro generování datového toku. Ty jsou vyobrazeny na obr. 3.4. Pomocí

technologie VLAN jsou připojeny k WLAN klientům servery Iperf, které generují datový tok přes tyto spoje k hlavnímu Iperf serveru. Při následné změně VLAN skupin můžeme nadefinovat ke kterému zařízení daný Iperf server připojíme.

Měřící síť dále tvoří útlumové články. Tyto články mají buď pevné hodnoty 10 dB u WLAN AP anebo 30 dB u WLAN klientů. Dále pak rozbočovače, které disponují útlumem mezi vývody 6 dB a programovatelné útlumové články, které lze libovolně nastavovat v rozmezí -1 až -50 dB. Hlavní důraz byl kladen na vzájemné odstínění klientů jedné technologie. Tedy tak, aby mezi oběma klienty Groove nebo Bullet byla dostatečná bariéra, která zajistí, že se tito klienti neuslyší. Z obrázku je patrné, že klient Groove má k druhému klientu Groove útlum na trase 118 dB. Což je dostatečný útlum, který simuluje skrytý uzel. K přístupovému bodu pak má každý klient útlum 84 dB. V obou případech je brána hodnota proměnného článku 20 dB.

Před měřením se provedl test, kdy se nastavil na libovolném klientovi režim AP a zkoušelo se, jestli klient v druhé větvi tento signál zachytí. V prvním případě se tak stalo a hledalo se dále, kde signál uniká. Jako slabé místo se ukázaly kryty obou testovaný vzorku. Na odstranění tohoto problému posloužil alobal, kterým se obalila testovaná zařízení a to hned několika vrstvami. Po tomto kroku se už zařízení neslyšely a mohlo se přikročit k testu.



Obr. 4.4: Zapojení sítě pro měření skrytých uzlů.

Protokol airMAX

Je to proprietární protokol vytvořeny firmou Ubiquiti pro své bezdrátové portfolio Wi-Fi produktů. Jelikož je protokol uzavřený, tak není možné zjistit detailní informace, jak pracuje.

Jak již řečeno, srdcem tohoto protokolu je metoda přístupu TDMA. Čili každému připojenému klientovi je přiřazen časový úsek, respektive můžeme vzít kapacitu přístupového bodu a rozdělit jí pomocí časových úseků spravedlivě mezi všechny připojené stanice. Avšak přidělování velikosti těchto úseků závisí na mnoha faktorech. Výrobce udává, že protokol airMAX zlepší parametry jakéhokoliv spoje, když bude tato funkce aktivována. Především vylepší odolnost vůči rušení a zvětší přenosovou rychlost. Další funkcí zahrnutou v protokolu airMAX je podpora QoS (quality of service). Ta řeší problém s klienty, kteří mají hodnotu signálu menší, než ostatní klienti. Tento klient pak potřebuje na přenesení svých dat více času a může tím zpomalit rychlost celého přístupového bodu. QoS se postará, aby tento klient dostal menší prioritu, a tím pádem nezpomalí klienty s lepším přijímaným signálem.

Protokol NV2

Tento protokol vzniknul jako reakce na výše zmiňovaný protokol airMAX. Protokol vychází ze staršího protokolu Nstream. Doslova z něj vychází i název: Nstream Version 2. Je proprietární a funguje pouze s produkty Mikrotik.

I tento protokol je založen na přístupu TDMA. NV2 na přístupovém bodu dělí čas do pevných úseků, které jsou dynamicky přidělovány pro downlink (od AP ke klientovi) a uplink (od klienta k AP). Uplink je pak dále rozdělen mezi klienty podle toho, jakou potřebují šířku pásma. Na začátku periody přístupový bod rozešle klientům informaci, kdy mají vysílat a jaký čas jim je k tomu přidělen.

Pro nově připojené klienty, kteří se připojí na NV2 je vyhrazen tzv. nespecifikovaný čas. Tento čas pak používá klient pro registraci k přístupovému bodu. Ten pak odhaduje zpoždění šíření mezi nimi a začne jej zabudovávat do TDMA systému. Protokol NV2 také podporuje mechanismus QoS s proměnným mechanismem prioritních front a standardním QoS plánovačem. Maximální počet připojených klientů je teoreticky až 511. [12]

Protokol Nstream

Nstream zavádí tzv. pooling. AP tedy určuje, kdy mohou klienti vysílat svá data. AP dá každému z nich cyklicky vědět, kdy můžou odesílat data. Tímto mechanismem se zvedne odezva, ale jitter zůstane malý. Nstream i upravuje velikosti přenášených rámců.

4.2 Testované zařízení

Jako testované zařízení jsme zvolili zařízení Ubiquiti Bullet M5. V testovací síti budou zapojeny tyto 3 jednotky v režimu AP – 2x klient a přes ně budou probíhat zátěžové datové testy. Tato zařízení pracují v pásmu 5 GHz. Výhodou tohoto zařízení je především jeho konstrukce. Ta je vyobrazena na obr. 4.5. Tělo zařízení se skládá z desky plošného spoje, který je umístěn v plastovém krytu a zakončen přímo N male konektorem. V tomto zapojení by neměla vznikat žádná přechodná rušení na kabeláži, protože je konektor přímo vyveden do rádiové části.

Obr. 4.5: Ubiquiti Bullet M5

Specifikace výrobce:

Tab. 4.2: Rádiové parametry Ubiquiti Bullet M5. [10]

MCS schéma	Vysílaný výkon	Citlivost	Tolerance
-	[dBm]	[dBm]	[dB]
0	25	-96	+/- 2
1	25	-95	+/- 2
2	25	-92	+/- 2
3	25	-90	+/- 2
4	23	-86	+/- 2
5	22	-83	+/- 2
6	20	-77	+/- 2
7	19	-74	+/- 2

Z těchto parametrů jsou patrné jednotlivé citlivosti a k příslušným MCS schématům jsou vypsány maximální vysílací výkony. Pokud bychom chtěli srovnat citlivosti s tabulkou 4.1, která specifikuje IEEE standard 802.11n, tak jsou patrné velké rezervy. Například největší rozdíl je v kódovacím schématu č. 5, kdy rozdíl mezi IEEE

a manuálem výrobce dosahuje 17 dB.

Druhým zástupcem v našem testu je víceméně srovnatelné zařízení od výrobce Mikrotik a nese označení Groove 5Hn. Toto zařízení se začalo prodávat přibližně před 2 roky jako reakce na v té době unikátní designové zařízení Bullet od firmy Ubiquiti. Co se týče konstrukce, tak v plastovém těle je obsažena deska s rádiovým modulem a síťovým konektorem pro napájení po ethernetu. Vývod kabelu je opatřen šroubovací těsnící maticí, která chrání vývod proti vniknutí vody. Na přední straně se nachází konektor N male pro připojení antény.

Obr. 4.6: Mikrotik Groove 5Hn

Specifikace výrobce:

Tab. 4.3: Rádiové parametry Mikrotik Groove Hn [11].

MCS schéma	Vysílaný výkon	Citlivost
-	[dBm]	[dBm]
0	22	-93
7	15	-71

V manuálu výrobce se bohužel nenachází detailnější parametry ohledně citlivosti na ostatních MCS schématech. Pokud znovu srovnáme hodnoty s tabulkou 4.1, která specifikuje IEEE standard 802.11n, tak i zde jsou velké rezervy k těmto hraničním hodnotám. Pro schéma 0 vychází rezerva od standardu 14 dB. Naopak pro schéma MCS 7 vychází rezerva na 10 dB.

Při srovnání citlivostí obou testovaných zařízení nám vychází jako papírový vítěz Ubiquiti Bullet M5. Ten udává na stejných kódových schématech lepší hodnoty citlivosti. V obou případech jsou rozdíly mezi nimi 3 dB. V oficiálních manuálech obou zařízení se však nenachází informace, zda jsou to citlivosti při 40 MHz nebo 20 MHz kanále. Není tudíž možné stoprocentně porovnat rozdíly od standardu.

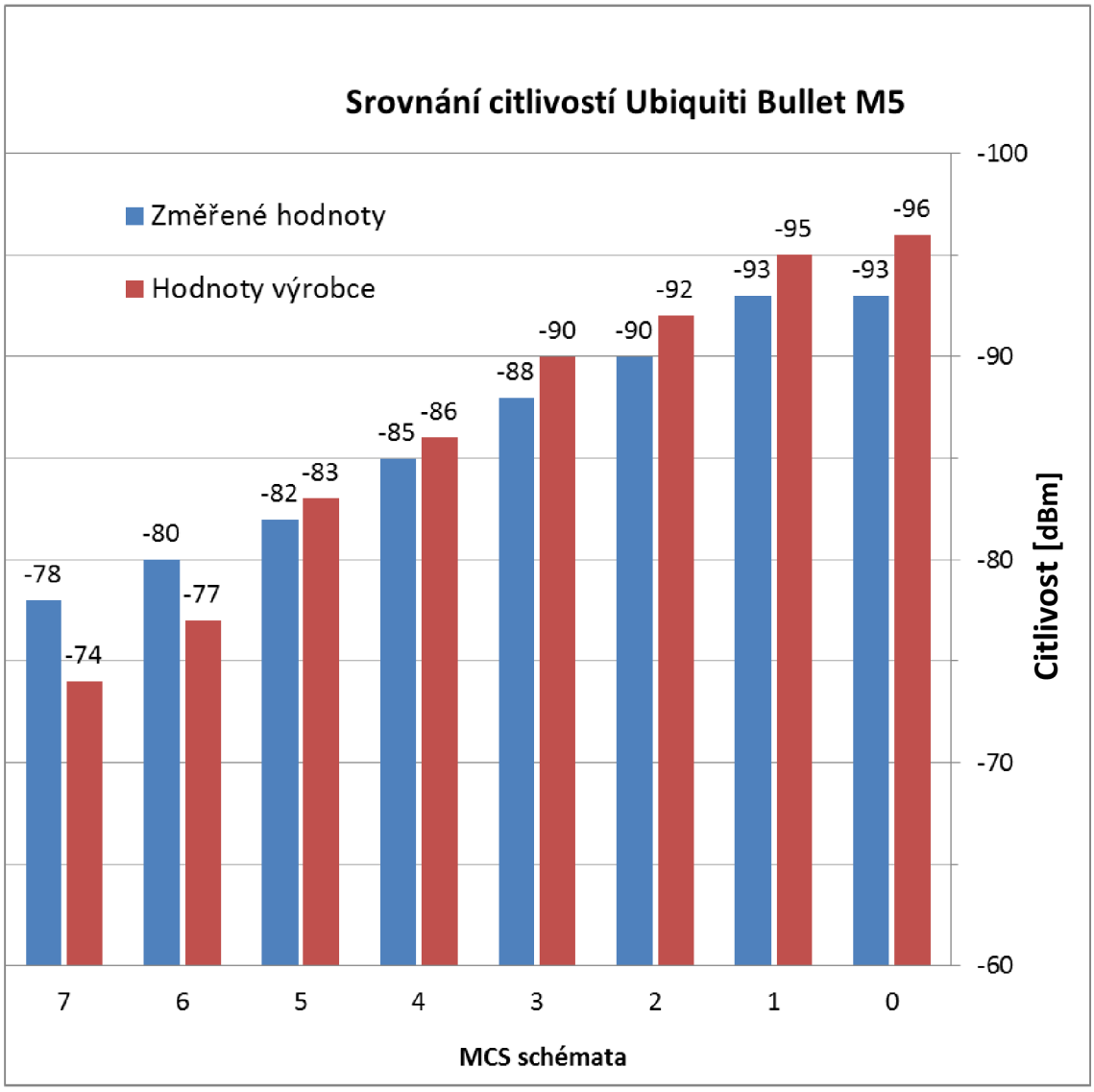
5 VÝSLEDKY MĚŘENÍ

5.1 Citlivost Bullet M5

Před samotným měřením bylo nutné upravit síť do takové podoby, aby byla přizpůsobená na měření námi požadovaného testu. Nejdřív však bylo nutné přepojit měřící pracoviště do schématu, jaké je uvedeno na Obr. 4.1. Ze složité sítě se odpojily nepotřebné komponenty a zůstaly jen ty, které jsou nezbytné k měření. Před samotným měřením jsme pomocí signálového analyzátoru otestovali kabely a propojení jednotlivých prvků. Po tomto úvodním testu jsme měli kalibrovanou síť a mohli jsme zapojit zařízení. Jako startovací hodnotu pro všechny testy MCS schémat se zvolila hodnota signálu -56 dBm.

Tab. 5.1: Naměřené hodnoty citlivosti Ubiquiti Bullet M5.

MCS	Vložený útlum	Síla signálu	Citlivost daná výrobcem	Ztrátovost paketů
-	[dB]	[dBm]	[dBm]	[%]
7	31	-76	-74	0
	32	-77		90
	33	-78		100
6	32	-78	-77	0
	33	-79		0
	34	-80		100
5	34	-80	-83	0
	35	-81		0
	36	-82		100
4	37	-83	-86	0
	38	-84		0
	39	-85		100
3	41	-86	-90	0
	42	-87		20
	43	-88		100
2	44	-88	-92	0
	45	-89		50
	46	-90		100
1	47	-91	-95	20
	48	-92		80
	49	-93		100
0	47	-91	-96	0
	48	-92		0
	49	-93		100



Obr. 5.1: Srovnání citlivostí u Ubiquiti Bullet M5.

Tabulka 5.1 vyobrazuje stručně změřené hodnoty citlivostí a porovnání s katalogovou hodnotou. Změřených hodnot bylo velké množství, a proto jsou zde jen ty zásadní hodnoty, při kterých docházelo k rozpojení na testovaném spoji. Vlevo jsou MCS schémata, ve kterých měření probíhalo. Zároveň je i u citlivostí vyobrazen sloupec s katalogovými hodnotami od výrobce. Změřené hodnoty až na schémata 7 a 6, která mají dokonce lepší hodnoty než od výrobce, odpovídaly katalogovým hodnotám. Při schématu MSC 0 se však podařilo spoj rozpojit i nad hranicí tolerance a to citlivostí -93 dBm oproti deklarovaným -96 dBm.

5.2 Citlivost Mikrotik Groove 5Hn

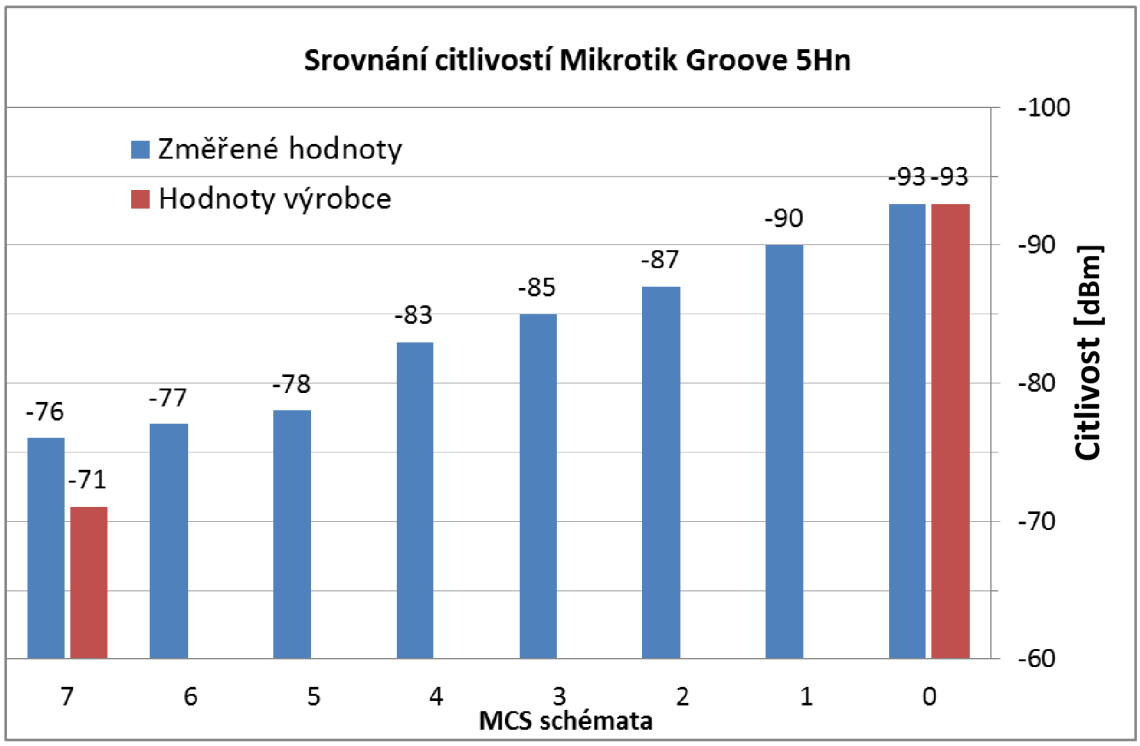
Jako v předešlém testovaném vzorku Bullet M5 bylo nutné nachystat měřící síť. Jelikož jsou to typově naprosto stejná zařízení, stačilo pouze odmontovat vzorky z předešlého měření a namontovat druhé.

Tab. 5.2: Naměřené hodnoty citlivosti Mikrotik Groove 5Hn.

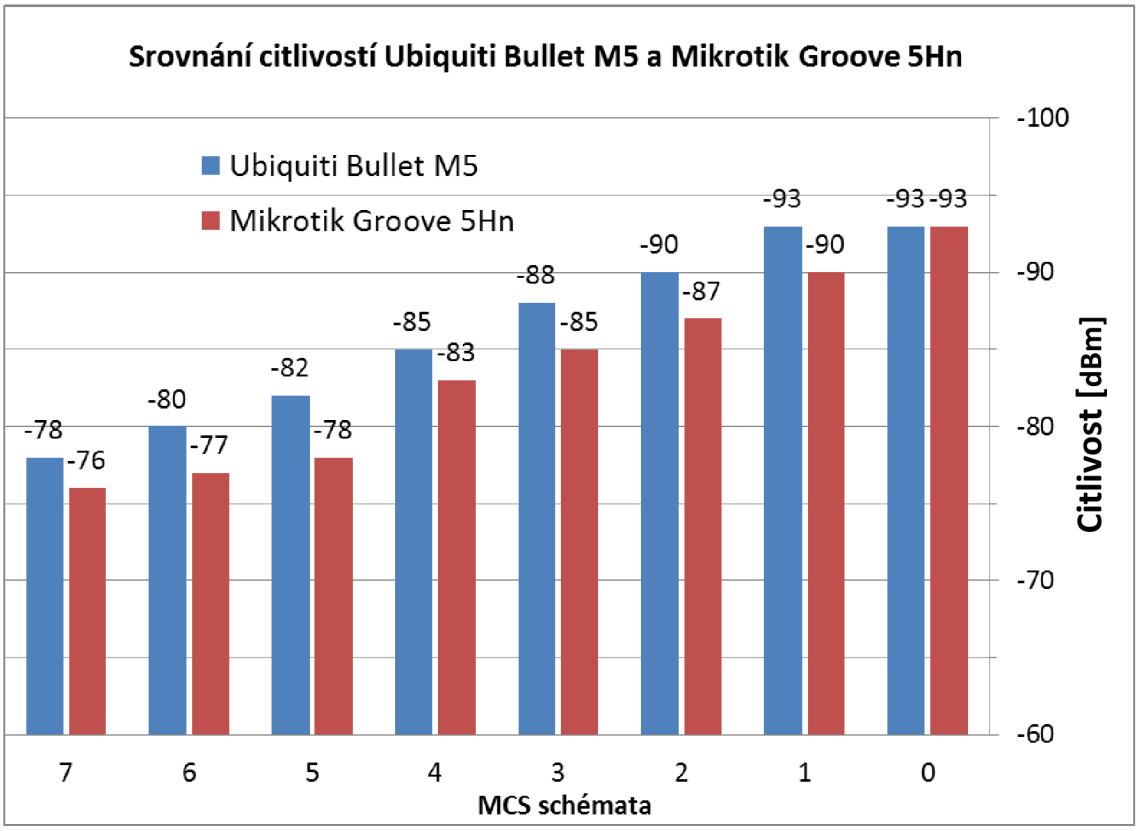
MCS	Vložený útlum	Síla signálu	Citlivost daná výrobcem	Ztrátovost paketů
-	[dB]	[dBm]	[dBm]	[%]
7	33	-74	-71	0
	34	-75		0
	35	-76		100
6	35	-75	neuvedeno	0
	36	-76		0
	37	-77		100
5	36	-76	neuvedeno	0
	37	-77		0
	38	-78		100
4	40	-80	neuvedeno	0
	41	-82		0
	42	-83		100
3	43	-83	neuvedeno	0
	44	-84		0
	45	-85		100
2	45	-85	neuvedeno	0
	46	-86		0
	47	-87		100
1	49	-88	neuvedeno	0
	50	-89		0
	51	-90		100
0	50	-91	-93	20
	51	-92		70
	52	-93		100

Výsledné hodnoty citlivostí jsou uvedeny v tabulce 5.2. I zde jsou přiloženy katalogové hodnoty od výrobce. Bohužel výrobce specifikuje hodnoty pouze na schématech MCS 7 a MCS 0. Porovnávat tedy můžeme jen tyto 2 hodnoty. Ze změřených hodnot je patrné, že při schématu MCS 7 byla dosažena hraniční citlivost přijímače -76 dBm. Oproti hodnotě dané výrobcem, který uvádí -71 dBm je rozdíl markantní. Zařízení dokázalo přenášet data i s 5 dB horším signálem, než udává výrobce. Naproti tomu u schématu MCS 0 byla změřená hodnota -93 dBm stejná jako

katalogová. Na obrázku 5.2 jsou graficky vyobrazeny hodnoty dle měřených schémat.



Obr. 5.2: Srovnání citlivostí u Mikrotik Groove 5Hn.



Obr. 5.3: Srovnání citlivostí u Ubiquiti Bullet M5 a Groove 5Hn.

Ze srovnání, které je vyobrazeno na obrázku 5.3 jsou patrné rozdíly obou zařízení. Mikrotik Groove 5Hn dosahuje téměř na všech MSC schématech horší citlivost, než konkurent Ubiquiti Bullet M5. Největší rozdíl hodnot je na schématu MCS 5, kde zařízení Groove přestává pracovat na hodnotě signálu -78 dBm, zatímco Bullet dokázal pracovat až do hodnoty signálu -82 dBm. Průměrný rozdíl obou testovaných zařízení se pohybuje od 2 do 3 dB ve prospěch Ubiquiti Bullet M5.

5.3 Potlačení sousedních kanálů

Pro měření potlačení sousedních kanálu bylo nutné měřící síť přestavit, jak je uvedeno na obrázku 4.2. Základem tohoto měření je zjištění úrovně sousedního kanálu, kdy se na pracovním kanále projeví jeho vliv. Dle standardu je hraniční hodnota chybovosti PER 10%. Tabulka 5.3 ukazuje výsledky úrovně sousedního kanálu a tabulka 5.4 pouze přepočítává rozdíly hodnot signálů. V této tabulce jsou pak dále uvedeny průměrné hodnoty těchto odstupů.

Tab. 5.3: Změřené hodnoty úrovně rušícího signálu do PER 10%.

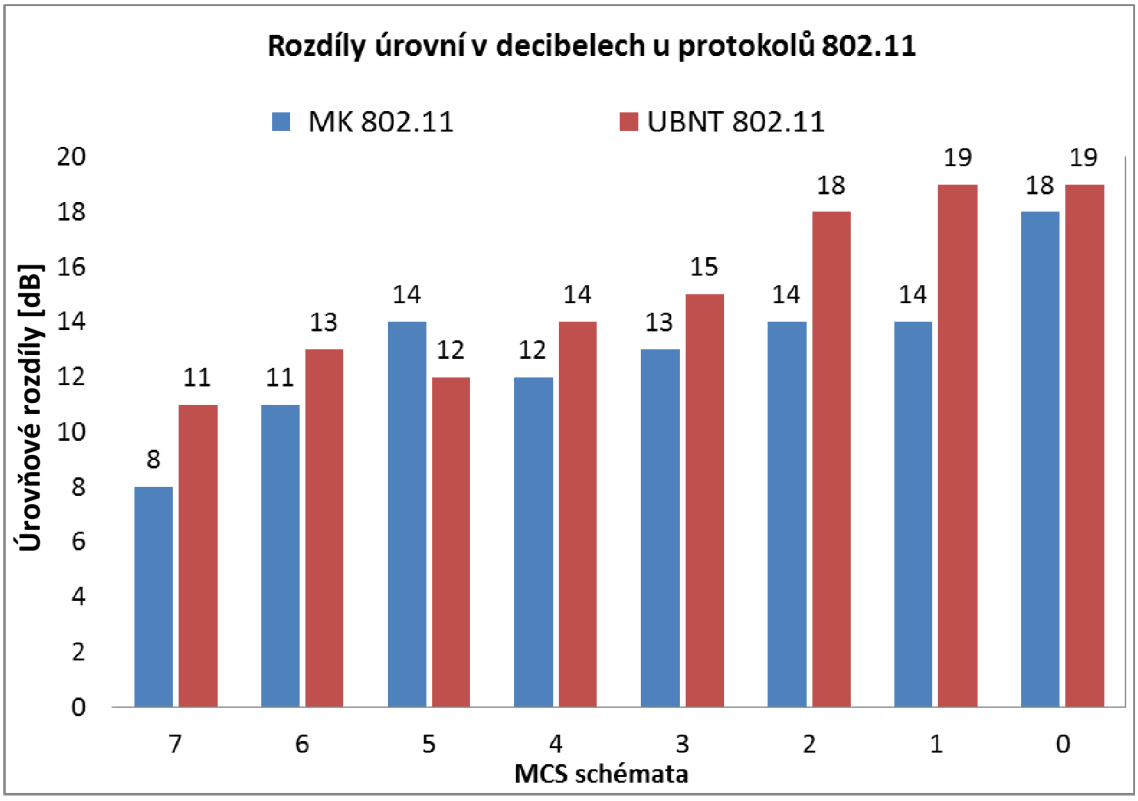
MCS	**Úroveň spoje**	**Úroveň sousedního rušícího signálu nad 10% PER**				
		MK 802.11	**UBNT 802.11**	**MK NV2**	**UBNT airMAX**	**MK Nstream**
-	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
7	-61	-52	-50	-46	-52	-51
6	-62	-49	-49	-47	-50	-52
5	-63	-48	-51	-47	-52	-52
4	-67	-55	-53	-53	-54	-57
3	-71	-62	-56	-55	-57	-57
2	-74	-63	-56	-59	-58	-61
1	-76	-64	-57	-61	-60	-64
0	-79	-62	-60	-61	-62	-62

V tabulce 5.3 jsou rozepsána jednotlivá MCS schémata a k nim příslušné úrovně signálů spoje, při nichž se měřilo. Následně jsou pro každou platformu uvedeny příslušné úrovně rušícího sousedního kanálu, kdy došlo k chybovosti spoje PER 10%. Co se týče standardního 802.11 protokolu, tak zde jasně lepší hodnoty vykazuje zařízení firmy Ubiquiti. Pro rovnocenné protokoly NV2 a airMAX založených na TDMA jsou rozdíly srovnatelné. NV2 však dosáhnul lepších výsledků. Další protokol firmy Mikrotik v tomto testu zaznamenal nejhorší úrovně. Lepší porovnání hodnot ukazuje tabulka 5.4.

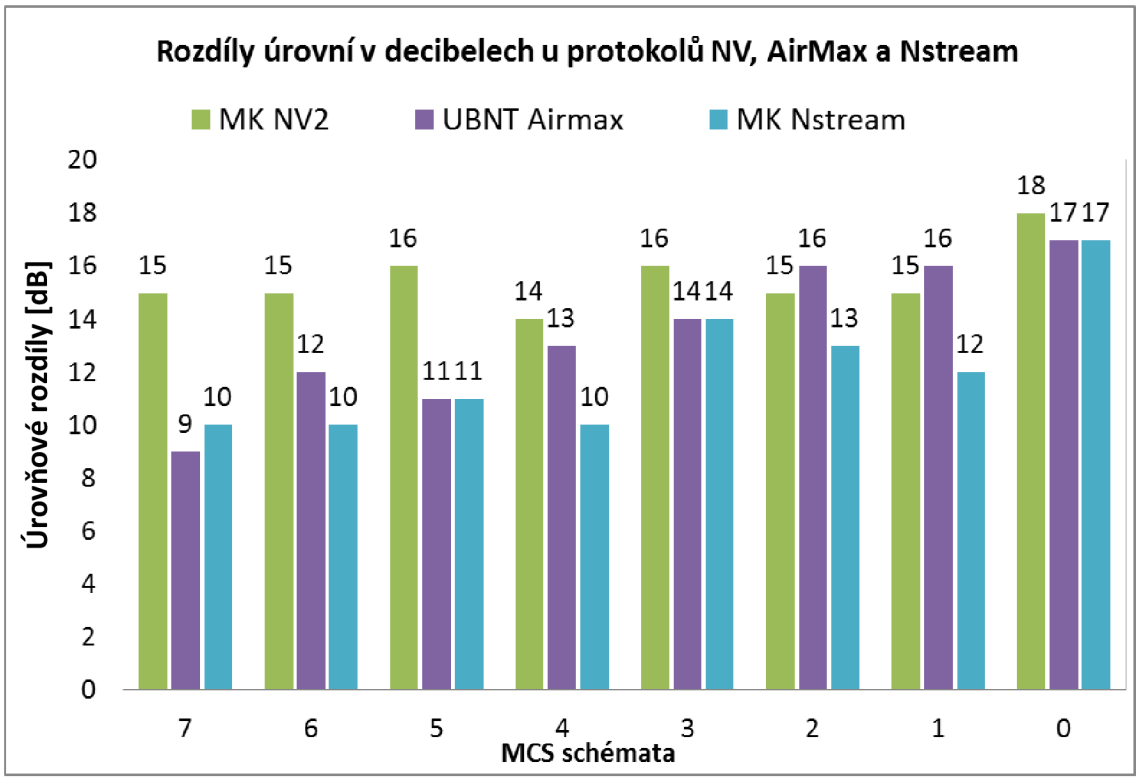
Tab. 5.4: Přepočítané hodnoty na dB z rozdílů signálu.

MCS	Úroveň spoje	Přepočet na dB v rozdílu úrovní signálů				
		MK 802.11	UBNT 802.11	MK NV2	UBNT airMAX	MK Nstream
-	[dBm]	[dB]	[dB]	[dB]	[dB]	[dB]
7	-61	8	11	15	9	10
6	-62	11	13	15	12	10
5	-63	14	12	16	11	11
4	-67	12	14	14	13	10
3	-71	13	15	16	14	14
2	-74	14	18	15	16	13
1	-76	14	19	15	16	12
0	-79	18	19	18	17	17
Průměr hodnot		**13**	**15**	**16**	**14**	**12**

Zde se nachází přepočítané hodnoty úrovní na rozdíly v decibelech.



Obr. 5.4: Srovnání rozdílu úrovní u 802.11 Ubiquiti Bullet M5 a Groove 5Hn.



Obr. 5.5: Srovnání rozdílu úrovní sousedního kanálu u airMAX, NV2, Nstream.

Výsledné hodnoty z grafů 5.4 a 5.5 ukazují, že u standardu 802.11, až na MCS schéma 5, dosahují hodnoty zařízení Ubiquiti lepších hodnot, než Mikrotik Groove 5Hn. Největší rozdíl naměřených hodnot byl na schématu MCS 1, a to 5 dB.

Avšak při pohledu na srovnání přídavných protokolů do grafu 5.5 je situace jiná. V tomto srovnání ve většině schémat dosahuje lepších hodnot protokol NV2 od společnosti Mikrotik. Graf také ukazuje stejné chování jinak fungujících protokolů Nstream a AirMax. V tabulce 5.4 je patrné, že v celém měření si vedl nejlépe Mikrotik NV2 s průměrnou hodnotou 16 dB. Naopak nejhůře protokol Nstream.

5.4 Citlivost CCA

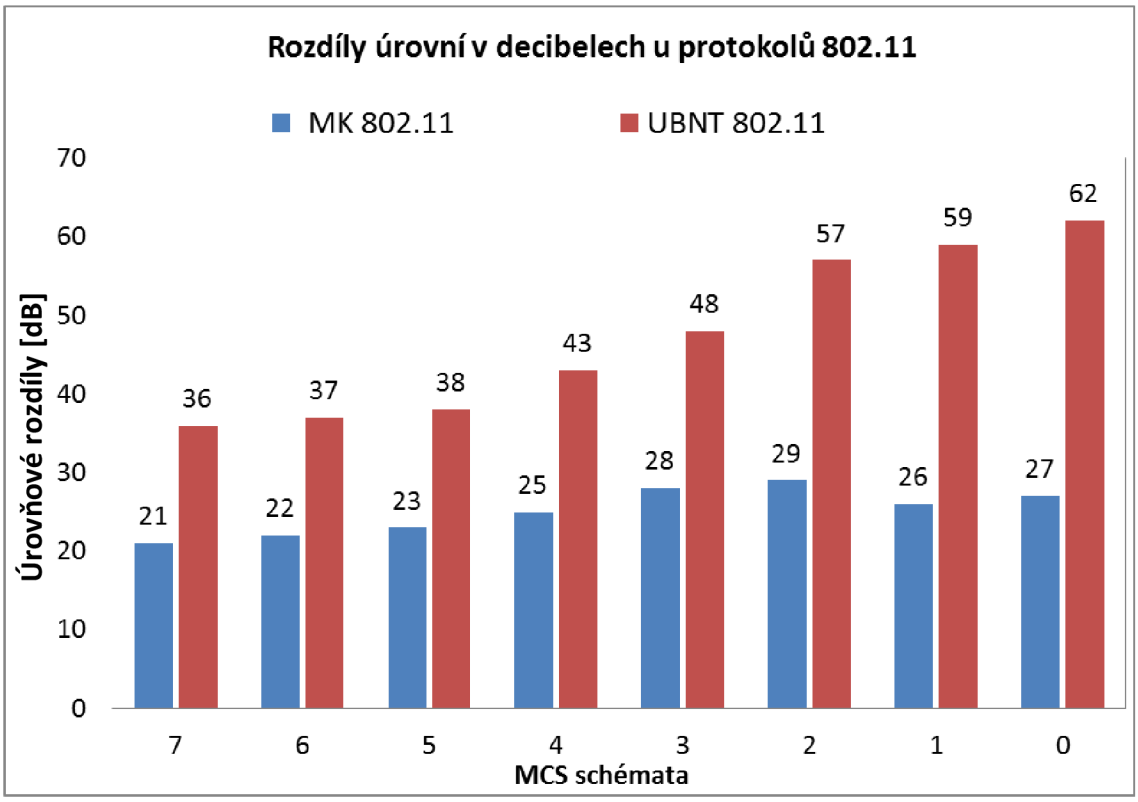
Hlavním úkolem tohoto měření bylo zjistit úrovně signálu sousedního kanálu, kdy vysílač detekuje okolní prostředí a zjišťuje, že je obsazené. Na základě toho nezahájí vysílání a čeká náhodně dlouhou dobu do dalšího pokusu. Tato funkce je implementovaná v standardu 802.11. V tabulce 5.5 jsou uvedeny výsledky měření a v následující tabulce 5.6 jsou opět pro přehlednost uvedeny přepočítané hodnoty rozdílu signálů.

Tab. 5.5: Přepočítané hodnoty na dB z rozdílů signálu.

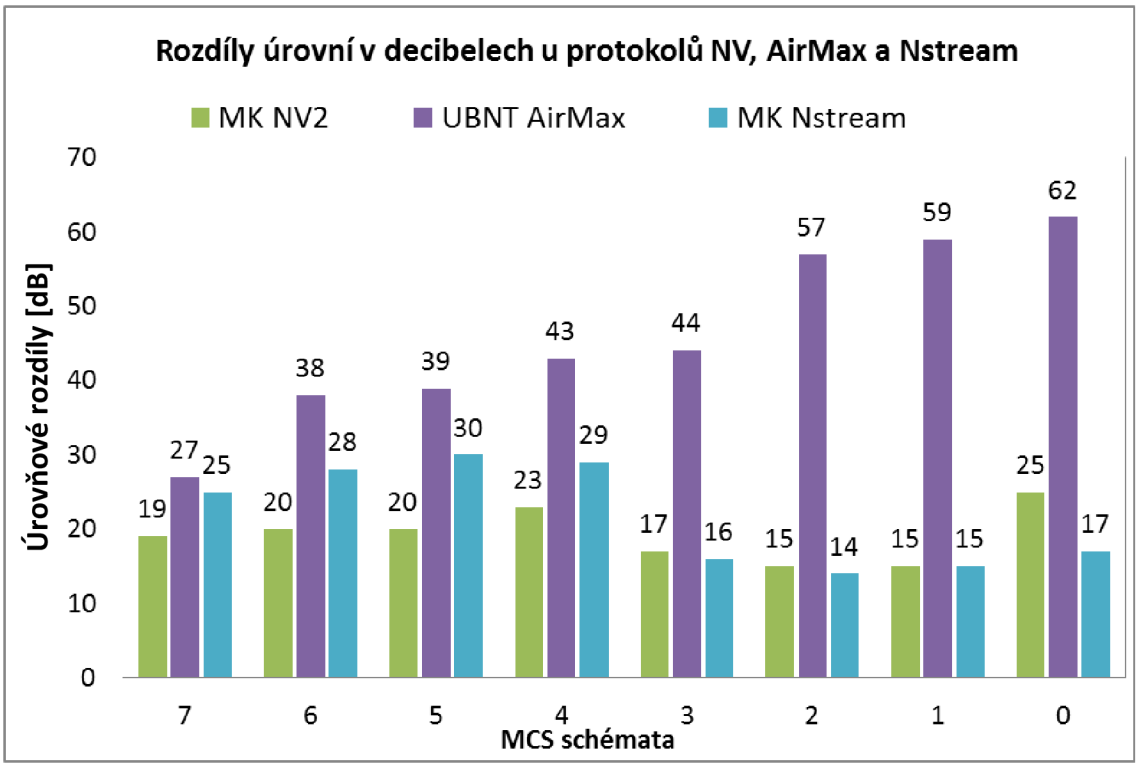
MCS	Úroveň spoje	Úroveň sousedního signálu kdy vysílač nezahájí vysílání				
		MK 802.11	UBNT 802.11	MK NV2	UBNT AirMax	MK Nstream
-	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]	[dBm]
7	-61	-40	-25	-42	-34	-36
6	-62	-40	-25	-42	-24	-34
5	-63	-40	-25	-43	-24	-33
4	-67	-42	-24	-44	-24	-38
3	-71	-43	-23	-54	-27	-55
2	-74	-45	-17	-59	-17	-60
1	-76	-50	-17	-61	-17	-61
0	-79	-52	-17	-54	-17	-62

Tab. 5.6: Přepočítané hodnoty na dB z rozdílů signálu.

MCS	Úroveň spoje	Přepočet na dB v rozdílu úrovní signálů				
		MK 802.11	UBNT 802.11	MK NV2	UBNT AirMax	MK Nstream
-	[dBm]	[dB]	[dB]	[dB]	[dB]	[dB]
7	-61	21	36	19	27	25
6	-62	22	37	20	38	28
5	-63	23	38	20	39	30
4	-67	25	43	23	43	29
3	-71	28	48	17	44	16
2	-74	29	57	15	57	14
1	-76	26	59	15	59	15
0	-79	27	62	25	62	17
Průměr hodnot		**25**	**48**	**19**	**46**	**22**



Obr. 5.6: Srovnání rozdílu CCA úrovní u AirMax, NV2 a Nstream.

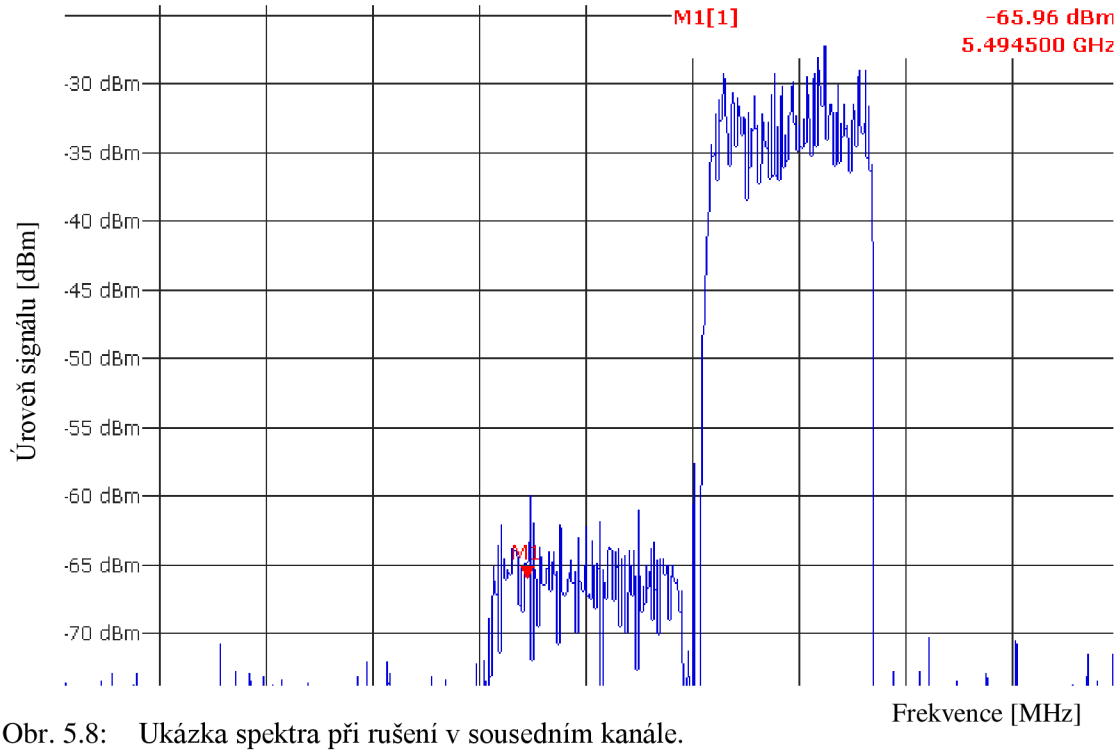


Obr. 5.7: Srovnání rozdílu CCA úrovní u AirMax, NV2 a Nstream.

V tomto měření jsme se zaměřili na vysílací část testovaných vzorků. Bylo úkolem zjistit, při jak vysoké úrovni sousedního kanálu nastane stav, kdy vysílač detekuje provoz v okolí a nezahájí komunikaci.

Z teorie by stanice, která detekuje provoz, neměla zahájit komunikaci a čekat náhodně dlouhou dobu na další pokus. To je případ při obsazenosti pracovního kanálu. V praxi se však vyskytují případy, kdy takový stav způsobuje i rušení ze sousedního kanálu.

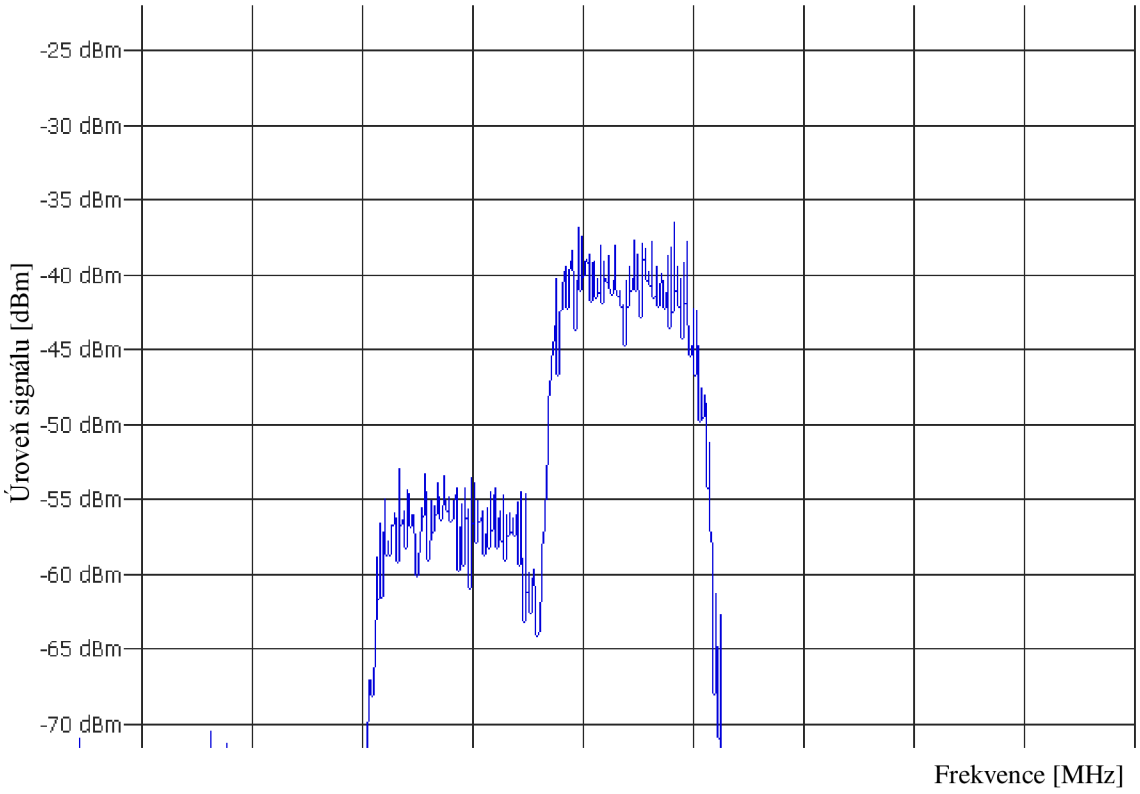
Při pohledu na tabulku 5.5 s výslednými hodnotami jsou patrné velké rozdíly napříč testovanými platformami. Jako jasným vítězem se na první pohled může jevit zařízení Ubiquiti. Při měření MCS schémat 0 – 7 dosahovaly hodnoty téměř vždy skoro dvojnásobných rozdílů oproti platformě Mikrotik. Při měření hodnot Ubiquiti nastal však jiný problém. Testovaný spoj Ubiquiti se nepodařilo rozpojit i za velmi značné výkonové úrovni. Spoj vykazoval určitou nestabilitu v podobě klesající přenosové rychlosti v závislosti na úrovně rušícího signálu, ale pořád přenášel data a komunikoval. Pro ověření tohoto faktu bylo nutné zkontrolovat, jak se chová zařízení ve spektru. Zobrazené spektrum na obrázku 5.8 potvrdilo, že vysílač, ač přes velmi vysoké hodnoty signálu v sousedním kanále, stále vysílá. Rozdíl hodnot činil více než 30 dB. Spoj byl však velmi degradovaný a přenosová rychlost se pohybovala na hranici 3 Mb/s oproti rychlosti 55 Mb/s bez sousedního kanálu.



Obr. 5.8: Ukázka spektra při rušení v sousedním kanále.

Vlivem tohoto faktu jsou tedy v tabulkách uvedeny hodnoty sousedního kanálu, kdy došlo úplnému rozpojení spoje, a neprocházely žádná data. Tento první rozdíl je brán pro schéma MCS 7, kde figurují modulace QAM64 a spoj by měl být relativně náchylný na rušení. Při postupném proměřování nižších schémat, kde jsou odolnější modulace, tak rozdíly ještě narůstaly. Na posledním schématu MCS 0, kde spoj pracuje s jednoduchou modulací BPSK, tak se hranice zastavila na hodnotě 62 dB. I při tak obrovském rozdílu hodnot spoj přenášel data. Hodnoty jsou ale tak extrémní, že v klasickém pojetí protokolu 802.11 by takové hodnoty měly způsobit bezpochyby nefunkčnost spoje. V tomto případě nastává otázka, zda se zařízeni firmy Ubiquiti drží standardů a dodržuje všechny parametry. Druhý testovaný protokol AirMax dosahoval podobných výsledků jako ve standardním protokolu 802.11.

Konkurenční zařízení Mikrotik Groove 5Hn dosáhlo oproti konkurentovi velmi špatných výsledků. Nutno říci, že zařízení firmy Mikrotik se chovalo tak, jak by mělo. Při postupném navyšování výstupního výkonu rušícího signálu z generátoru, zařízení bez problému komunikovalo. Po přiblížení ke své hranici se spoj mírně degradoval a to snížením přenosové rychlosti. Po přidání 1 – 3 dB výkonu se spoj rozpojil a vysílač vůbec nevysílal. Dosažené výsledky v některých případech nedosáhly ani rozdílu 20 dB. Paradoxně u zařízení Mikrotik s klesajícím stupněm schématu a tedy s odolnějšími modulacemi rozdíly hodnot ještě klesaly.



Obr. 5.9: Ukázka spektra při rušení v sousedním kanále.

K tomuto druhému extrému jsme opět využili spektrální analyzátor, který na obr. 5.9 zobrazuje spektrum těsně před hranicí, kdy vysílač Mikrotik přestal vysílat na MCS schématu 0 na hranici 17 dB u protokolu Nstream.

Protokoly NV2 a Nstream, které by měly pomoci s okolním rušením, svou úlohu nevzaly za správný konec a výsledky jsou ještě horší než u protokolu 802.11. Při pohledu do tabulky 5.6 a i následně do grafů, lze vyčíst dosažené průměrné hodnoty. Nejlepších zprůměrovaných hodnot dosáhlo zařízení firmy Ubiquiti a to rozdílu 48 dB u protokolu 802.11. Naopak nejhorším průměrným výsledkem byla hodnota 19 dB u zařízení Mikrotik s protokolem NV2.

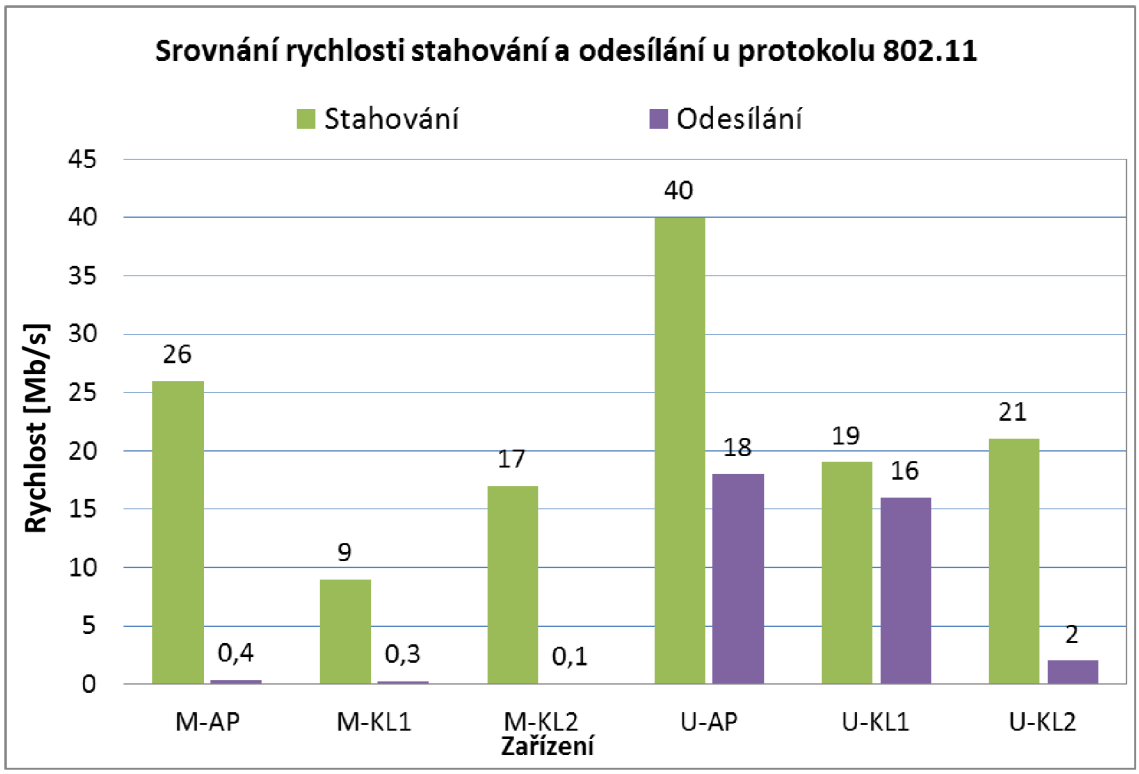
Z těchto skutečností lze usuzovat, že zařízení Ubiquiti jsou velmi odolná vůči okolnímu rušení. Dokáží se vypořádat s velkými rušícími signály v okolním rádiovém spektru a jsou vhodná na umístění do měst a vytížených oblastí. Výhodou Ubiquiti je, že i při velkých rušeních, se spoj nerozpadne, ale pouze sníží svoji přenosovou rychlost. Tento fakt může být velice výhodný pro spoje, které nemají za úkol přenášet velké objemy dat, ale pouze řídící, či signalizační informace.

5.5 Skryté uzly

Skryté uzly jsou fenoménem ve Wi-Fi sítích. Stanice, které jsou od ostatních vzdáleny nebo jsou jiným způsobem zakryty, způsobují na vysílači nemalé komplikace. Na takovém vysílači, který funguje na klasickém CSMA/CA přístupu, mohou tímto vznikat kolize. Takové kolize pak způsobují výkonnostní problémy především rychlost přenosu dat od stanic. Všechny změřené rychlosti odpovídají šířce kanálu 20 MHz při použití jedné antény a tedy maximální linkovou rychlost 65 Mb/s.

Tab. 5.7: Rychlosti skrytých uzlů pro standard 802.11.

802.11	Provoz jednoho klienta							Současný provoz obou klientů						
	D	UP	D/U		Ping			D	UP	D/U		Ping		
					D	U	D/U					D	U	D/U
	[Mb/s]				[ms]			[Mb/s]				[ms]		
M-AP	-	-		-	-	-	-	26	0,4	3	2	-	-	-
M-KL1	23	23	12	15	67	84	>1000	9	0,3	-	-	>1000	>1000	>1000
M-KL2	28	22	14	14	23	9	29	17	0,1	3	2	>1000	>1000	>1000
U-AP	-	-		-	-	-	-	40	18	29	16	-	-	-
U-KL1	54	47	21	20	164	163	>1000	19	16	9	4	148	>1000	>1000
U-KL2	43	47	22	22	531	164	>1000	21	2	20	12	153	>1000	>1000



Obr. 5.10: Srovnání rychlostí u standardu 802.11.

V tabulce 5.7 a na obrázku 5.10 jsou uvedeny rychlosti při skrytých uzlech pro standard 802.11. Při měření se testovaly oba směry přenosu dat a odezva. Jako první se testoval provoz pouze k jedné stanici. Tam by měly být hodnoty maximální bez jakýchkoliv vlivů. Což se i potvrdilo. Pro první testované zařízení firmy Mikrotik však nedopadly výsledky vůbec dobře. Dá se říct, že v klasickém módu 802.11n a přístupu k médiu 802.11 toto zařízení neumí vůbec pracovat. Rychlosti i bez skrytých uzlů byly velmi nízké. Dosahovaly hodnot maximálně 28 Mb/s, což byla téměř poloviční hodnota oproti konkurenčnímu zařízení Ubiquiti. Co se týče odezvy ping přes testovaný spoj, lepších výsledků dosahovaly hodnoty zařízení Mikrotik, avšak na téměř poloviční rychlosti. U zařízení Mikrotik se navíc vyskytovaly problémy se stabilitou spoje. Rychlosti byly velmi nestabilní a docházelo k rozpojování spoje.

Po základním testu, kdy komunikovala s přístupovým bodem jen jedna nebo druhá stanice, se přistoupilo k testu obou stanic zároveň. I tento test nebyl výjimkou a nejlepších výsledků dosáhlo zařízení od firmy Ubiquiti. Při jednosměrném provozu byla celková agregovaná rychlost na přístupovém bodě 40 Mb/s při stahování a 18 Mb/s při odesílání z pohledu klienta. V testu si zařízení vedlo dobře i v obousměrném provozu (full duplex), kdy dosáhlo rychlosti 29 Mb/s stahování a 16 Mb/s odesílání. Mikrotik nakonec dosáhnul velmi špatných výsledků a při současném provozu obou klientů.

V jednom případě dokonce jeden klient nekomunikoval vůbec. V poměru rozdělení datového toku mezi klienty, byly u Mikrotiku dosti nevyvážené rozdíly u stahování 9 Mb/s a 17 Mb/s. U rychlosti odesílání se hodnoty pohybovaly v řádech kilobitu za sekundu. Odezvy spoje v takto vytížených situacích byly nad hranicí nepoužitelnosti a vykazovaly hodnoty převyšující 1000 ms. Proto jsou tyto hodnoty v tabulce uvedeny jako >1000. I v tomto případě se velmi projevily skryté uzly především na rychlosti odesílání od klienta k přístupovému bodu.

Jako vítěze v tomto testu můžeme jednoznačně považovat zařízení Ubiquiti. To se dokázalo se skrytými uzly vypořádat. Výsledné agregované hodnoty 40 Mb/s pro stahování a 18 Mb/s pro odesílání také potvrdily skryté uzly, ale hodnoty oproti maximální hranici 54 Mb/s pro stahování a 47 Mb/s pro odesílání jsou velmi dobré. Jak již bylo řečeno, standard 802.11 nemá žádné mechanismy proti skrytým uzlům. Proto i výsledky odezvy ping přes tyto plně vytížené spoje jsou hluboko za hranicemi použitelnosti. V případě, že by byl na tomto spoji zapojený uživatel a chtěl např. poslouchat hudbu, prohlížet web, apod., tak vlivem plně vytíženého spoje se jeho požadavky vůbec nedostanou k příjemci.

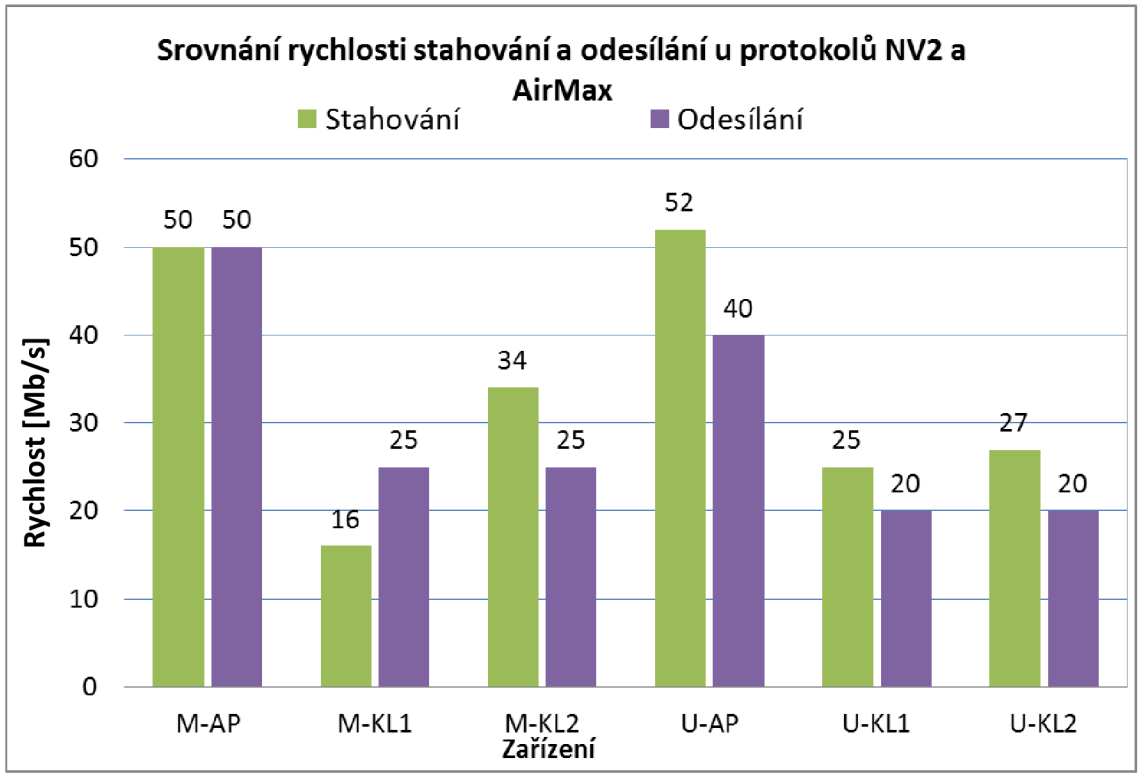
Tab. 5.8: Rychlosti skrytých uzlů pro protokoly NV2 vs. AirMax.

NV2 vs. AirMax	Provoz jednoho klienta							Současný provoz obou klientů						
	D	**UP**	**D/U**		**Ping**			**D**	**UP**	**D/U**		**Ping**		
					D	**U**	**D/U**					**D**	**U**	**D/U**
	[Mb/s]				[ms]			[Mb/s]				[ms]		
M-AP	-	-		-	-	-	-	50	50	20	20	-	-	-
M-KL1	55	52	25	25	40	8	72	16	25	10	10	46	11	80
M-KL2	55	49	25	25	10	10	39	34	25	10	10	45	10	83
U-AP	-	-		-	-	-	-	52	40	23	20	-	-	-
U-KL1	52	51	24	23	68	13	>1000	25	20	11	9	49	14	>1000
U-KL2	41	43	24	26	60	18	>1000	27	20	12	11	48	9	>1000

V tabulce 5.8 a obrázku 5.11 jsou uvedeny výsledky testů skrytých uzlů za použití protokolů NV2 u výrobce Mikrotik a airMAX u Ubiquiti. Oba tyto protokoly jsou založeny na TDMA protokolu. Právě tento mechanismus by měl dopomoci rovnoměrnému rozdělení šířky pásma a zajistit, aby na vysílači nedocházelo ke kolizím kvůli skrytým uzlům.

V prvním měření se změřily rychlosti bez skrytých uzlů. Z naměřených hodnot vyplývá, že spoje jsou v pořádku a rychlost je pro danou konfiguraci maximální. Té

dosáhlo zařízení Mikrotik a to rychlosti 55 Mb/s pro stahování a 52 Mb/s pro odesílání. V obousměrném režimu jedné stanice dosáhl Mikrotik 25 Mb/s jak pro stahování tak



Obr. 5.11: Srovnání rychlostí u standardů NV2 a AirMax.

současně i odesílání. Protokol NV2 nemá problémy ani s odezvou. Ta byla maximálně 72 ms. Spoj se tak jevil nezahlcen a i při jeho plném vytížení spoje bylo možné přes něj fungovat.

Ty samé testy se provedly i u zařízení Ubiquiti. Datová propustnost byla oproti platformě Mikrotik menší. Maximální hodnotu rychlosti, kterou zařízení dosáhlo, bylo 52 Mb/s pro stahování a 43 Mb/s pro odesílání. Při obousměrném provozu byly hodnoty také vyrovnané, jako u platformy Mikrotik. Horších výsledků však zařízení Ubiquiti dosáhlo v odezvě ping. Při jednosměrném provozu byly hodnoty na použitelné hranici a to max. 68 ms. Naopak při obousměrném provozu byly hodnoty odezvy větší než 1000 ms. Za takových podmínek je spoj nepoužitelný pro ostatní komunikaci.

Pravý test protokolů NV2 a Nstream začal při testu z obou klientských stanic zároveň. Z naměřených hodnot v tabulce 5.8 vyplývá, že hodnoty jsou více méně vyrovnané. Lepších výsledků však dosahuje zařízení Mikrotik s protokolem NV2. Při agregované rychlosti z obou klientů dosahují stahovaní i odesílání rychlosti 50 Mb/s. Hlavní co nás zajímá je rychlost odesílání od klientů. Ta dosahovala rovnoměrné hodnoty 25 Mb/s od každého klienta. NV2 tedy rovnoměrně rozděluje šířku pásma mezi

klientské stanice a využívá k tomu téměř maximální rychlost kterou má reálně k dispozici. Umí tedy velmi efektivně a spravedlivě nakládat s datovými prostředky. Velmi překvapivé výsledky byly i u obousměrného provozu, kdy obě stanice zároveň přijímají i vysílají. Zde byla rychlost naprosto vyvážená a to 10 Mb/s v obou směrech od obou klientských stanic. Šířka pásma se dělí přesně mezi všechny klienty připojené na konkrétní přístupový bod. V neposlední řadě i odezva u protokolu NV2 byla velmi slušná a nepřekračovala použitelnou hranici 100 ms.

Ubiquiti se vypořádalo s testem po svém. V agregovaném provozu na přístupovém bodě dosáhlo slušných rychlostí stahování i odesílání. Zaostává jen mírně v rychlosti odesílání. V porovnání s protokolem NV2 je protokol AirMax pomalejší o 10 Mb/s. Zajímavý výsledek se naskytnul při obousměrném provozu od obou klientských stanic. Rychlost byla vyšší než u protokolu NV2 a to 23 Mb/s pro stahování a 20 Mb/s pro odesílání. I přes tyto větší rychlosti však nastává problém s odezvou spojů. V obou měřených spojích, které obousměrně vytížíme, nastává problém, kdy jsou linky vytížené na 100% a odezva je větší než 1000ms.

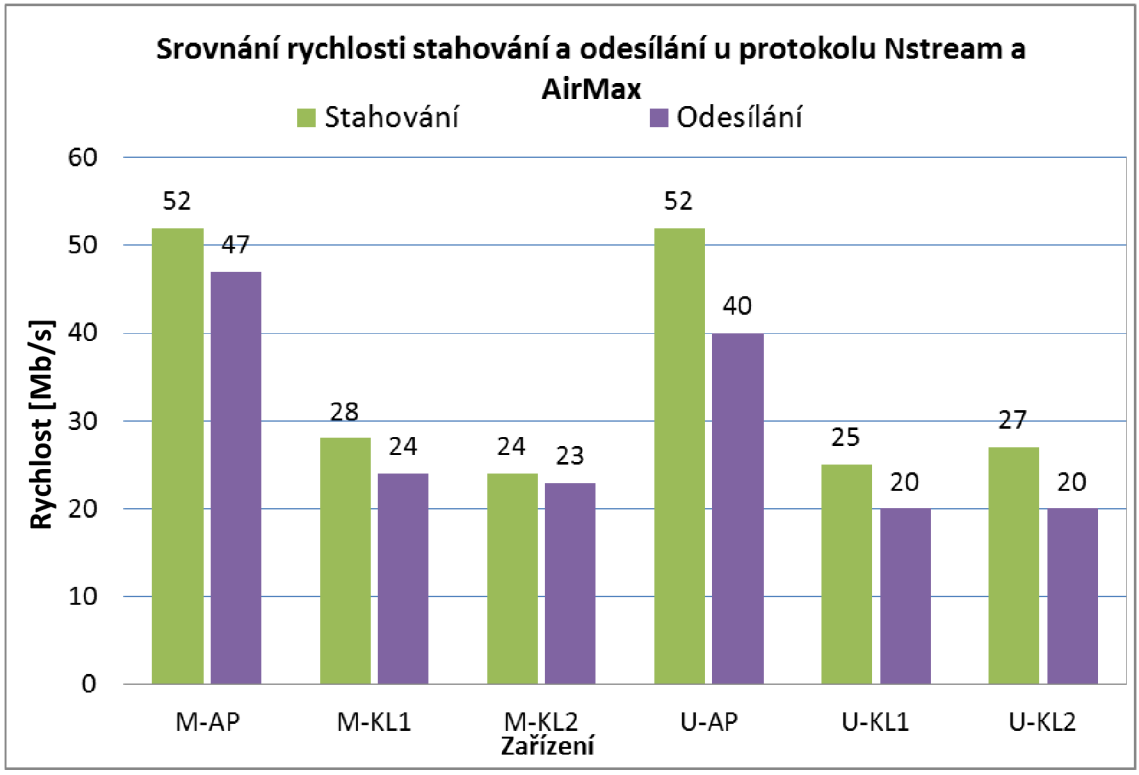
Tab. 5.9: Rychlosti skrytých uzlů pro standard Nstream.

Nstream	Provoz jednoho klienta							Současný provoz obou klientů						
	D	UP	D/U		Ping			D	UP	D/U		Ping		
					D	U	D/U					D	U	D/U
	[Mb/s]				[ms]			[Mb/s]				[ms]		
M-AP	-	-		-	-	-	-	52	47	25	24	-	-	-
M-KL1	55	55	23	24	80	35	220	28	24	14	12	42	76	230
M-KL2	50	52	24	23	83	33	200	24	23	11	12	47	82	190

Nakonec přišel na řadu test skrytých uzlů i protokol Nstream. Ten podporuje pouze zařízení Mikrotik. Porovnávat je tedy budeme s protokoly NV2 respektive AirMax. Při srovnání rychlostí provozu od jednoho klienta jsou výsledky stejné. Maximálně 55 Mb/s pro stahování a 52 Mb/s pro odesílání. Jediný a celkem i podstatný rozdíl je v odezvě ping. U protokolu Nstream jsou odezvy srovnatelné s protokolem AirMax. Nstream dosahuje ale lepších výsledků odezvy při obousměrném provozu a to maximálně 220 ms oproti hodnotám nad 1000 ms.

V případě testu provozu obou stanic si protokol Nstream vedl obstojně a dosáhl i srovnatelných výsledků, jako protokoly NV2 či Air Max. Nstream si také dobře poradil se skrytými uzly a rychlosti odesílání. V agregované rychlosti na přístupovém bodě dosáhnul hodnoty 47 Mb/s a dokonce v obousměrném režimu měl výsledky

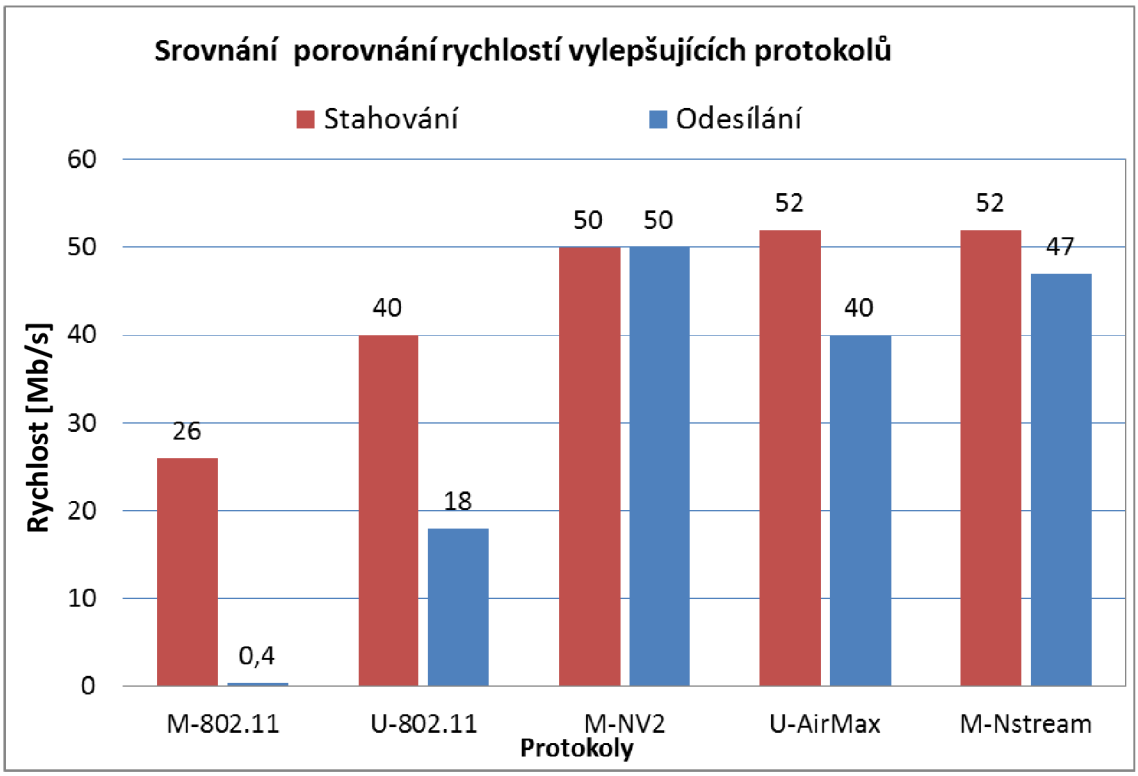
nejlepší mezi protokoly 802.11, NV2, či AirMax. Jedinou nevýhodou protokolu byla



Obr. 5.12: Srovnání rychlostí u standardů Nstream a AirMax.

odezva v těchto obousměrných testech. Ta se pohybovala lehce přes hranici 200 ms. Srovnáme-li odezvy s protokoly NV2 či AirMax, tak Nstream je zlatá střední cesta. NV2 má velmi nízké odezvy do 100 ms, následuje Nstream s maximem kolem 200 ms a nakonec nejhorší odezvy v testu dosáhl protokol AirMax, kdy ve všech obousměrných testech byla odezva nad hranicí 1000 ms.

V posledním grafu na obrázku 5.13 je celkové srovnání a vyobrazení testovaných protokolů. Z předešlé teorie je jasné, že skryté uzly jsou postrachem pro standard 802.11. Jak se potvrdilo v testech, tyto hodnoty byly oproti standardnímu modelu bez skrytých uzlů nižší. Především na to doplácela rychlost odesílání od koncové stanice. Na obrázku 5.13 tedy vidíme rozepsány jednotlivé protokoly a jejich maximální rychlosti stahovaní a odesílání se skrytými uzly. Vlevo je zobrazen standard 802.11 a jeho výsledky. Jak si můžeme všimnout, tak u zařízení Mikrotik jsou výsledky především rychlosti odesílání katastrofické. U zařízení Ubiquiti můžeme vidět relativně slušné hodnoty a je zřejmé, že do určité míry je standard 802.11 použitelný. Dále jsou uvedeny podpůrné protokoly NV2, AirMax a Nstream. Pro zařízení Mikrotik jsou tyto protokoly záchranou a podstatným zlepšením rychlostí. I u protokolu AirMax firmy Ubiquiti došlo ke zlepšení rychlosti stahování i odesílání.



Obr. 5.13: Srovnání rozdílu rychlostí u standardů 802.11, Nstream a AirMax.

6 ZÁVĚR

Tato diplomová práce se zabývá měřením základních parametrů rádiových částí vybraných komponent. Jmenovitě jsou to Ubiquiti Bullet M5 a konkurenční Mikrotik Groove 5Hn. Jsou provedena měření citlivosti, potlačení sousedního kanálu, citlivost CCA a přenosové rychlosti se skrytými uzly. Změřené hodnoty jsou zapsány v tabulkách, vyobrazeny v grafech a následně diskutovány.

V prvním měření byla stanovena minimální citlivost přijímače na obou testovaných zařízeních. Lepších výsledků dosáhlo zařízení Ubiquiti Bullet M5. Výsledné hodnoty dosahovaly rozdílu oproti druhému testovanému zařízení v průměru 2 – 3 dB. Když bychom porovnali změřené a katalogové hodnoty výrobce, tak v případě Ubiquiti byly výsledné citlivosti jednotlivých MCS schémat horší, než uvádí výrobce. Avšak krom schémat MCS 0 a 1 se držely rozdíly v udávané toleranci +/- 2 dB. V případě výrobce Mikrotik, který uvádí pouze 2 hodnoty citlivosti, byly hodnoty v pořádku.

Dalším testem bylo měření chybovosti spoje za přítomnosti sousedního rušení. V základním standardu MAC protokolů 802.11 dosáhlo opět lepších výsledků zařízení Ubiquiti a to v celkovém průměru rozdílů úrovní signálů o 2 dB. Naopak v testech podpůrných protokolů jako jsou NV2, airMAX a Nstream, byly výsledky na straně výrobce Mikrotik a protokolu NV2. Celkovým průměrným rozdílem úrovní hodnot 16 dB předstihnul jak protokol Nstream (12 dB) téhož výrobce, tak i protokol airMAX (14 dB) firmy Ubiquiti.

Měření CCA bylo podobné jako měření rušení v sousedním kanále, avšak zde se hledala hranice, kdy zařízení usoudí, že je prostředí obsazené a nezahájí vysílání. V tomto měření absolutně dominovalo zařízení firmy Ubiquiti. I při enormním rozdílu úrovní sousedního kanálu >40 dB stále komunikovalo. Oproti tomu zařízení Mikrotik dosáhlo téměř polovičních hodnot konkurenta. Tento test měl ukázat slabiny protokolu 802.11 a jeho přístupové metody CSMA/CA. Z výsledků je však patrný pravý opak a podpůrné protokoly situaci nezlepšily.

Posledním testem bylo měření přenosových rychlostí stanic ve skrytých uzlech. Skryté uzly se očekávaně projevily především u protokolu 802.11 a to v rychlosti odesílání od stanic. Důležitým parametrem byla i odezva spoje, kdy za použití protokolu 802.11 dosahovala ve většině testů nad hranici 1000 ms. Dále byly změřeny propustnosti spojů s podpůrnými protokoly, které by měly především díky mechanismům TDMA problém skrytých stanic vyřešit. Za vítěze se v tomto testu dá považovat zařízení Mikrotik s protokolem NV2. Zaznamenalo velmi slušných výsledku

v rychlosti, kde čísla byla téměř na úrovni bez skrytých uzlů a použitelné odezvy spoje do 100 ms i při obousměrném provozu. Ubiquiti nezůstalo pozadu a předvedlo srovnatelné výsledky, avšak při obousměrném provozu vykazoval spoj odezvy nad 1000 ms.

LITERATURA

[1] KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-Fi*. 2004. Brno : Computer Press, 2004. Úvod do bezdrátových sítí, s. 29-58. ISBN 80-251-0391-9.

[2] KOCUR, Zbyněk a Miroslav ŠAFRÁNEK. *Access server* [online]. 2008 [cit. 2010-12-07]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2008050006.

[3] VÁVRA, Štěpán. *Access server* [online]. 2006 [cit. 2010-12-09]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2005112301.

[4] PRAVDA, Ivan. *Access server* [online]. 2005 [cit. 2010-12-01]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2005113002.

[5] HRÁČEK, Jiří. *Intelek* [online]. 2009 [cit. 2010-12-09]. Dostupné z: http://www.intelek.cz/art_doc-5C56A0147621A13AC12575510053AE3E.html.

[6] RYAZDI, Ramin. *History and Status of IEEE 802.11.n standard* [online prezentace]. Carleton University, [cit. 2010-12-15]. Dostupné z http://www.doe.carleton.ca/~ryazdi/IEEE_802.ppt.

[7] TUREK, Lukáš. *802.11n - Cesta za rychlejším Wi-Fi.* [Online] 2007, [cit. 2010-12-15]. Dostupné z: <http://8an.praha12.net/talks/80211n.pdf>.

[8] ŠIMANDL. IEEE 802.11n: Jak na rychlé Wi-Fi doma i venku. *IEEE 802.11n* [online]. 2010 [cit. 2012-12-15]. Dostupné z: http://pctuning.tyden.cz/hardware/site-a-internet/16921-ieee-802-11n-jak-na-rychle-wi-fi-doma-i-venku?start=1.

[9] DULÍK, Tomáš. *Methods for interference mitigation in wireless networks*. Zlín, 2012. Disertační práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce doc. RNDr. Vojtěch Křesálek, CSc.

[10] Ubiquiti Bullet M5 Datasheet. In: *Www.ubnt.com* [online]. 2008 [cit. 2013-05-20]. Dostupné z: http://dl.ubnt.com/datasheets/bulletm/bm_ds_web.pdf

[11] Groove 5Hn Brochure. In: *Www.routerboard.com* [online]. 2011 [cit. 2012-12-12]. Dostupné z: http://routerboard.com/RBGroove5Hn

[12] Manual:Nv2. In: *Mikrotik Wiki* [online]. 2012-07-06 [cit. 2013-05-20]. Dostupné z: http://wiki.mikrotik.com/wiki/Manual:Nv2

[13] Přístupové metody bezdrátových sítí. NOVOTNÝ, Vít a Pavel KOVÁŘ. *Access server* [online]. 25. 11. 2008. [cit. 2013-05-05]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2008100003

[14] BUMBÁLEK, Zdeněk. *Access server* [online]. 8.2.2010 [cit. 2010-12-09]. Modulační techniky v moderních bezdrátových sítích. Dostupné z WWW:

<http://access.feld.cvut.cz/view.php?cisloclanku=2010020004>.

[15] HANUS, Stanislav. *RÁDIOVÉ A MOBILNÍ KOMUNIKACE : Přednášky* [online]. Brno : [s.n.], 3.5.2009 [cit. 2010-12-02]. Dostupné z WWW: <https://www.vutbr.cz/www_base/priloha.php?dpid=20097>.

SEZNAM ZKRATEK

Wi-Fi	Wireless Fidelity
IEEE	Institute of Electrical and Electronics Engineers
WLAN	Wireless Local Area Network – Bezdrátová lokální síť
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DSSS	Direct-Sequence Spread Spectrum
CCK	Complementary Code Keying
ISM	Industrial Sscientific and Medical
OFDM	Orthogonal Frequency Division Multiplexing
QPSK	Quadrature Phase Shift Keying
BPSK	Binary-Phase Shift Keying
MAC	Media Access Control
FSK	Frequency-shift keying
AP	Access Point – Přístupový bod
mW	miliWat
FHSS	Frequency Hopping Spread Spectrum
FFHSS	Fast Frequency Hopping Spread Spectrum
SFHSS	Slow Frequency Hopping Spread Spectrum
GI	Guard Interval – Ochranný interval
BER	Bit Rate Error – Bitová chybovost
PSK	Phase-shift keying
QAM	Quadrature Amplitude Modulation
TCP/IP	Transmission Control Protocol/Internet Protocol

PER	Packet error rate
CCA	Clear Channel Assessment
PLCP	Physical Layer Convergence Procedure
dBm	Decibel vztažený k jednomu miliwatu
MSDU	MAC service data unit
MPDU	MAC protocol data unit
MCS	Modulation and Coding Scheme
SISO	Single-Input Single-Output
SIMO	Single-Input Multiple-Output
MISO	Multiple-Input Single-Output
MIMO	Multiple-Input Multiple-Output
VPN	Virtuál private network – Virtuální privátní síť
NAT	Network address translation – Překlad adres
RTS/CTS	Request to Send and Clear to Send
VLAN	Virtual local area network – virtální lokální síť
DHCP	Dynamic Host Configuration Protocol