

UNIVERZITA PARDUBICE

Fakulta elektrotechniky a informatiky

Metodika měření propustnosti bezdrátové sítě

Bc. Filip Holík

Diplomová práce

2014

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Filip Holík**
Osobní číslo: **I11378**
Studijní program: **N2646 Informační technologie**
Studijní obor: **Informační technologie**
Název tématu: **Metodika měření propustnosti bezdrátové sítě**
Zadávající katedra: **Katedra softwarových technologií**

Z á s a d y p r o v y p r a c o v á n í :

Cílem práce je vytvořit a prakticky ověřit metodiku pro měření propustnosti bezdrátových sítí postavených na základě standardu IEEE 802.11 a jeho dodatků. Autor provede podrobnou rešerši metod pro měření propustnosti bezdrátových sítí. Provede SWOT analýzu jednotlivých řešení a na základě analýzy jejich nedostatků navrhne metodiku pro měření propustnosti bezdrátové sítě v reálném prostředí se zohledněním vlivu reálného prostředí pro šíření signálu. Navrženou metodiku ověří na sadě navržených experimentálních měření. Získané hodnoty a zkušenosti využije k závěrečné SWOT analýze své metodiky a provede krátkou komparativní analýzu s vybranými metodami z rešerše.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

GAST, Matthew. 802.11 wireless networks: the definitive guide. 2nd ed.

Sebastopol: O'Reilly, 2005, xxi, 630 s. ISBN 978-0-596-10052-0.

PERAHIA, Eldad a Robert STACEY. Next generation wireless LANs: 802.11n, 802.11ac, and Wi-Fi direct. Second edition. xxviii, 452 pages. ISBN 11-070-1676-2.

PEJMAN ROSHAN, Jonathan Leary. 802.11 Wireless LAN fundamentals: a practical guide to understanding, designing, and operating 802.11 WLANs. 3rd printing. Indianapolis, Ind: Cisco Press, 2004. ISBN 978-158-7142-246.

O'HARA, Bob a Al PETRICK. IEEE 802.11 handbook: a designer's companion. 2nd ed. New York, NY: IEEE, c2005, xxxvi, 364 p. ISBN 978-073-8144-498.

Vedoucí diplomové práce:

Mgr. Josef Horálek

Katedra softwarových technologií

Datum zadání diplomové práce: **31. října 2013**

Termín odevzdání diplomové práce: **16. května 2014**



prof. Ing. Simeon Karamazov, Dr.
děkan



L.S.



prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2013

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 1. 5. 2014

Bc. Filip Holík

Poděkování

Tímto bych rád poděkoval Mgr. Josefu Horálkovi Ph.D. za poskytnutí cenných rad a připomínek v průběhu vypracování této práce. Také bych chtěl poděkovat svým rodičům za podporu, kterou mi během mého studia věnovali.

Anotace

Tato práce se zabývá měřením výkonnostních parametrů bezdrátových sítí, a to zejména měřením propustnosti. V teoretické části práce jsou popsány typy měření propustnosti a představeny vybrané metody experimentálního měření propustnosti. Tyto metody jsou podrobně rozepsány a pro každou je provedena SWOT analýza. Na základě odhalených nevýhod je navržena nová metodika měření propustnosti, která je v praktické části práce otestována na sadě experimentálních měření. V závěru práce je provedena analýza metodiky a její porovnání s existujícími metodami měření propustnosti.

Klíčová slova

IEEE 802.11, WLAN , propustnost, měření výkonu sítě, bezdrátové sítě

Title

The methodology of measuring throughput of a wireless network

Annotation

This thesis discusses measuring wireless network performance, specifically data throughput. In the theoretical part of the paper, types of measuring throughput are described and chosen methods of experimental throughput measuring techniques are introduced. These methods are examined more thoroughly with SWOT analysis being completed for each. Based on identified disadvantages, new methodology of measuring throughput is developed and tested on a set of experimental measurements detailed in the practical part of the paper. In conclusion, analysis of the methodology is conducted and methodology is compared with existing methods of measuring network throughput.

Keywords

IEEE 802.11, WLAN, throughput, measuring network performance, wireless networks

Obsah

Seznam zkratek.....	10
Seznam obrázků.....	12
Seznam tabulek.....	12
Úvod.....	13
1 Literární rešerše měření propustnosti bezdrátových sítí.....	14
1.1 Měření výkonu bezdrátových sítí	14
1.2 Základní typy měření propustnosti	15
1.2.1 Analytické modelování.....	15
1.2.2 Počítačová simulace	16
1.2.3 Experimentální měření	17
1.3 Vybrané metody experimentálního měření	18
1.3.1 Metoda šíření signálu	18
1.3.2 Měření propustnosti metodou „packet-by-packet“	19
1.3.3 Metody měření dostupné kapacity.....	20
1.3.4 Měření vlivu rádiového rušení na propustnost	23
1.3.5 Měření propustnosti více toků	23
1.3.6 Měření dalších parametrů sítě.....	24
2 Úvod do bezdrátových sítí.....	25
2.1 Rozprostřené spektrum.....	25
2.1.1 Historie vzniku rozprostřeného spektra.....	25
2.1.2 Popis rozprostřeného spektra.....	26
2.1.3 FHSS.....	27
2.1.4 DSSS.....	27
2.1.5 OFDM.....	28
2.2 Přehled standardů IEEE 802.11	29
2.2.1 IEEE 802.11	29
2.2.2 IEEE 802.11b	29
2.2.3 IEEE 802.11a.....	29
2.2.4 IEEE 802.11g	29
2.2.5 IEEE 802.11n	30
2.2.6 IEEE 802.11ac	30

2.2.7	Shrnutí základních vlastností standardů 802.11	31
2.3	Základní pojmy bezdrátových sítí	31
2.3.1	Základní fyzikální pojmy rádiového přenosu	32
2.3.2	Parametry výkonu sítě	32
2.3.3	Parametry úrovně signálu	35
2.3.4	Prvky bezdrátových sítí	36
2.3.5	Architektury bezdrátových sítí	37
2.4	Faktory ovlivňující propustnost bezdrátové sítě	38
2.4.1	Režie MAC protokolu – velikost paketu	38
2.4.2	Úroveň rádiového signálu	41
2.4.3	Další faktory	43
3	Experimentální metody měření propustnosti bezdrátových sítí	45
3.1	Metoda šíření signálu	45
3.2	Měření propustnosti metodou „packet-by-packet“	49
3.3	Metody měření dostupné kapacity	51
3.4	Měření vlivu rádiového rušení na propustnost	54
3.5	Měření propustnosti více toků	56
3.6	Přehled nástrojů pro měření výkonnostních parametrů WLAN	58
4	Metodika pro měření propustnosti	59
4.1	Návrh nové metodiky	59
4.1.1	Model teoretické maximální propustnosti bezdrátové sítě	59
4.1.2	Shrnutí nedostatků zmíněných metod	61
4.1.3	Analýza nedostatků zmíněných metod	61
4.1.4	Použitý software	62
4.1.5	Použitý hardware	62
4.1.6	Ověření určitých předpokladů zmíněných metod	62
4.2	Metodika komplexního měření propustnosti v reálném prostředí	69
4.2.1	Schéma metodiky	69
4.2.2	Detaily metodiky	70
4.2.3	Konfigurace HW a SW nástrojů	71
4.2.4	Postup provedení experimentálního měření	74
4.2.5	Shrnutí stěžejních vlastností metodiky	77
5	Experimentální měření v cihlovém domě	78

5.1 Úvod do experimentu	78
5.1.1 Popis prostředí	78
5.1.2 Popis experimentů	79
5.1.3 Ukázka z postupu provádění metodiky	79
5.2 Experiment 1 – nevhodné umístění AP	81
5.3 Experiment 2 – typické umístění AP	82
5.4 Analýza výsledků	83
6 Porovnání metodiky	85
6.1 SWOT analýza metodiky.....	85
6.2 Komparativní analýza s ostatními metodami	85
Závěr	88
Literatura	90
Seznam příloh	95
Příloha A – hodnoty teoretického modelu maximální propustnosti	96
Příloha B – ukázka z programu WiFi Analyzer	97

Seznam zkratek

ACK	Acknowledgement
AES	Advanced Encryption Standard
AIFS	Arbitration Interframe Space
AP	Access Point
ARS	Adaptive Rate Selection
BA	Block ACK
bps	bits per second – počet bitů za sekundu
BSS	Basic Service Set
BTC	Bulk Transfer Capacity
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DCF	Distributed Coordination Function
DIFS	Distributed Coordination Function Interframe Space
DMZ	Demilitarized Zone
DRS	Dynamic Rate Shifting
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Interframe Space
ESS	Extended Service Set
ESSID	Extended Service Set Identifier
FCS	Frame Check Sequence
FE	Fast Ethernet
FHSS	Frequency Hopping Spread Spectrum
FW	Firewall
FWA	Fixed Wireless Access
GHz	Gigahertz
HW	Hardware
IBSS	Independent Basic Service Set
ID	Identifier
IEEE	Institute of Electrical and Electronic Engineers
IFS	Interframe Space
IP	Internet Protocol
IPsec	IP security
ISO	International Organization for Standardization
L2PT	Layer 2 Protocol Tunneling
MAC	Media Access Control
MIMO	Multiple-Input Multiple-Output
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection

P2P	Peer-to-peer
PC	Personal Computer
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PIFS	Point Coordination Function Interframe Space
PoE	Power over Ethernet
PPTP	Point-to-Point Tunneling Protocol
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTS	Request to Send
SIFS	Short Interframe Space
SS	Spread Spectrum
STBC	Space-Time Block Coding
SWOT	Strengths, Weaknesses, Opportunities, Threats
TCP	Transmission Control Protocol
TMT	Theoretical Maximum Throughput
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
US	United States
Win	Windows
WLAN	Wireless Local Area Network
WNIC	Wireless Network Interface Card
WPA2	Wi-Fi Protected Access II

Seznam obrázků

Obrázek 1 – Model diskrétního dvourozměrného Markovova řetězce	15
Obrázek 2 – Obecné schéma experimentálního měření	18
Obrázek 3 – Technologie fyzické vrstvy standardu IEEE 802.11	25
Obrázek 4 – Porovnání standardního a rozprostřeného signálu	26
Obrázek 5 – Rozložení kanálů DSSS	28
Obrázek 6 – Ortogonální uspořádání sub-kanálů OFDM.....	28
Obrázek 7 – Struktura typického rámce 802.11	38
Obrázek 8 – Schémata jednotlivých scénářů	46
Obrázek 9 – Měření propustnosti v experimentálním prostředí	47
Obrázek 10 – Naměřené propustnosti v závislosti na hodnotě SNR.....	50
Obrázek 11 – Schéma měření dostupné kapacity	51
Obrázek 12 – Dostupná kapacita naměřená iterativními metodami.....	52
Obrázek 13 – Experiment měření vlivu rušení bezdrátového robota na WLAN	54
Obrázek 14 – Grafy rozložení propustnosti pro více klientů.....	56
Obrázek 15 – Vliv velikosti paketu na teoretickou propustnost sítě 802.11g.....	60
Obrázek 16 – Schéma měření ověření předpokladů metod	63
Obrázek 17 – Graf naměřené propustnosti v závislosti na rušení od ostatních sítí	66
Obrázek 18 – Graf vlivu velikosti paketu na propustnost	68
Obrázek 19 – Schéma rozložení metodiky měření propustnosti	70
Obrázek 20 – Rozhraní programu Jperf	74
Obrázek 21 – Plán bytů pro provádění experimentálního měření	78
Obrázek 22 – Plán bytů pro provádění experimentálního měření	79
Obrázek 23 – Porovnání rozdílů naměřených propustností.....	82
Obrázek 24 – Graf porovnání naměřených propustností.....	84

Seznam tabulek

Tabulka 1 – Přehled základních parametrů standardů 802.11	31
Tabulka 2 – Porovnání propustností v závislosti na měřeném scénáři.....	46
Tabulka 3 – Naměřené výsledky propustnosti	55
Tabulka 4 – Přehled nástrojů pro měření výkonnostních parametrů WLAN.....	58
Tabulka 5 – Parametry pro výpočet teoretické propustnosti	60
Tabulka 6 – Rozdíl mezi TCP a UDP propustností.....	67
Tabulka 7 – Popis základních parametrů programu Iperf	72
Tabulka 8 – Naměřené hodnoty propustnosti experimentu 1	81
Tabulka 9 – Naměřené hodnoty propustnosti experimentu 2.....	82
Tabulka 10 – Naměřené hodnoty propustnosti experimentu 2.....	83

Úvod

Za posledních patnáct let dosáhly bezdrátové sítě neuvěřitelného rozmachu. Rozšířily se od pomalé nespolehlivé a drahé technologie, která sloužila pouze jako doplněk ke klasickým sítím a byla použitelná pouze ve velice specifických případech, téměř do každé domácnosti. Jak udává Negus a Petrick (2008), zařízení Wi-Fi tvoří druhý největší trh v kategorii bezdrátových komunikací s plánovaným prodejem jednoho bilionu zařízení v roce 2010. Před nimi už stojí pouze trh s mobilní telefonii. Bezdrátové sítě nyní pronikají do všech oblastí, kde je vyžadováno mobilní připojení k internetu, od domácností přes veřejné prostory až po školy a firemní instituce. Bezdrátové sítě přinášejí kromě mobility, která je hlavním důvodem jejich rozmachu, i další výhody jako například nízkou cenu za vybudování sítě a možnost snadného vytvoření či zrušení sítě. Tyto výhody jsou však vyváženy několika nedostatky, mezi které patří vyšší energetická náročnost v porovnání s kabelovými sítěmi, nižší rychlost, spolehlivost a úroveň zabezpečení.

Bezdrátové sítě Wi-Fi jsou dnes často synonymem pro připojení k internetu, i když s ním nemusí mít nic společného a mohou být úspěšně provozovány i bez něj. Toto zmatení je způsobeno faktem, že společnosti poskytující kabelové či DSL připojení k internetu často dodávají modem obsahující Wi-Fi přístupový bod a koncový uživatel tedy „vidí“ pouze Wi-Fi připojení, skrze které má přístup k internetu. Na druhou stranu bezdrátové sítě mohou být použity i přímo jako technologie „poslední míle“, nicméně v tomto případě se jedná o technologii WiMAX definovanou standardem 802.16e či FWA než Wi-Fi definovanou standardem 802.11 (BANERJI a CHOWDHURY, 2013).

Tato práce popisuje měření výkonnostních parametrů bezdrátové sítě, a to zejména propustnost, která je pro koncového uživatele nejvíce vypovídající veličinou, protože určuje, jaká rychlost je pro uživatele reálně dostupná. Přesná znalost propustnosti sítě sice pro typického uživatele není nijak zajímavá, protože pod konkrétními čísly si jen těžko představí „jak rychle bude internet fungovat“. Síťovému administrátorovi však poslouží v průběhu celého životního cyklu sítě. Při návrhu sítě může podle nároků jednotlivých uživatelů odhadnout, zda bude výkon sítě dostatečný, nebo zda bude potřeba přidat více přístupových bodů či zvolit standard poskytující vyšší přenosové rychlosti. Při implementaci sítě pak může pomocí terénního průzkumu ověřit kvalitu signálu na každém místě, na kterém bude síť používána a odhalit tak potenciálně problémové místa. Po nasazení sítě pak administrátor může monitorovat výkon sítě, což mu umožňuje odhadnout, zda síť funguje v pořádku, nebo zda nenastal čas pro její upgrade.

Práce uvádí základní typy měření propustnosti a do hloubky se věnuje experimentálním metodám měření, které vynikají zejména v reálných prostředích s komplikovaným šířením signálu. Na základě nedostatků existujících metod pro měření propustnosti je ve druhé části práce navržena nová metodika komplexního měření propustnosti v reálném prostředí, která přináší několik zásadních vylepšení stávajících metod. Následně je provedeno experimentální měření ověřující kvalitu metodologie a závěrečná komparativní analýza metodiky s existujícími metodami.

1 Literární rešerše měření propustnosti bezdrátových sítí

V této kapitole budou shrnuty základní typy měření propustnosti a popsány vybrané práce zabývající se měřením výkonnostních parametrů bezdrátových sítí, a to zejména jejich propustností. Základní pojmy zmíněné v této kapitole jsou podrobněji vysvětleny v následující kapitole. Implementační detaily, podrobné výsledky a porovnání jednotlivých metodologií měření propustnosti budou rozebrány ve třetí kapitole.

1.1 Měření výkonu bezdrátových sítí

Schopnost přesně změřit a mít možnost porovnávat výkon bezdrátové sítě je extrémně důležitá. Už při návrhu sítě je dobré mít představu, kolik uživatelů bude k síti připojeno, jaké budou jejich nároky na přenosovou rychlost a jak budou síť využívat (mobilita, používané aplikace) (GAST, 2005, s. 570–573). Při prvotním testování implementace sítě je vhodné prakticky ověřit předpokládané teoretické vlastnosti bezdrátové sítě, což probíhá metodou „*site survey*“. Při této metodě jsou na klíčových místech ověřovány parametry přístupového bodu, jako je pokrytí, přenosová rychlost a chybovost přenosu (ZANDL, 2003, s. 102–104). Po ostrém spuštění sítě je dále nutné její výkon monitorovat a v případě potřeby reagovat na jakékoliv nepřípustné události.

Hlavní otázkou však zůstává, jaké vlastnosti porovnávat a jakými metodami a postupy? Existuje celá řada metodologií pro určování „úzkých míst“ sítě, ale jak udávají Prasad a další (2003, s. 27–28), není vždy zřejmé, který výkonnostní parametr je vlastně měřen. Mohou za to značné rozdíly v použité terminologii různých prací i měřicích nástrojů, a tak někdy není ani jasné, co přesně daná metodologie zkoumá. Situaci dále komplikuje fakt, že použití podobných metodologií může přinést kompletně odlišné výsledky. V této práci budou jednotlivé metody porovnány a u každé bude uvedeno, co přesně měří a jak. Dále budou shrnuty jejich výhody a nevýhody.

Obvykle měřené výkonnostní parametry bezdrátových sítí jsou: propustnost, kapacita, dostupná kapacita, zpoždění, přijímaná úroveň signálu a odstup signál / šum. Vzhledem k tomu, že nejvíce uváděný parametr bude právě propustnost, neuškodí už na úvod uvést velice stručnou definici propustnosti: Propustnost je jedním z klíčových parametrů při měření výkonu jakékoliv počítačové sítě. Nejčastější definice propustnosti je jako počet přenesených užitečných dat za časovou jednotku a obvykle se udává v bitech za sekundu (*bps*) (EKPENYONG a ISABONA, 2010, s. 16). Propustnost lze měřit různými způsoby, které jsou dále podrobněji rozebrány.

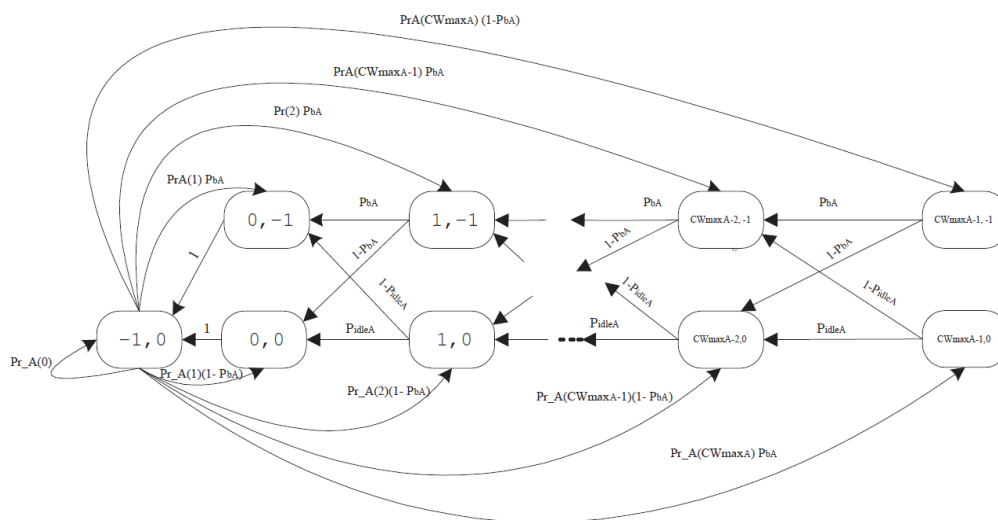
1.2 Základní typy měření propustnosti

Lo (2007, s. 3) ve své disertační práci uvádí tři základní typy měření výkonu bezdrátových počítačových sítí, které mohou být využity pro měření propustnosti. Jsou to analytické modelování, počítačová simulace a experimentální měření metodou šíření signálu.

1.2.1 Analytické modelování

Analytické modelování popisuje počítačovou síť jako soustavu rovnic, což přináší značné zjednodušení oproti realitě. Tato abstrakce neumožňuje dynamický popis povahy sítí (CHANG, 1999, s. 307). Při sestavování tradičního analytického modelu se často využívají modely Markovových řetězců. Jedná se o bezpaměťové modely, kde přechod do následujícího stavu závisí pouze na současném stavu a ne na stavech předchozích. Tyto modely se znázorňují stavovými diagramy zobrazující stavy systému a jejich možnými přechody určenými pravděpodobnostmi. Stavové diagramy lze následně vyjádřit formou matice. Více informací o Markovových řetězcích lze nalézt v knize „Stochastic processes“ (ROSS, 1996).

Příklad využití modelu diskrétního dvourozměrného Markovova řetězce při řízení přístupu k médiu je zobrazen na následujícím diagramu. Model zobrazuje snižování náhodné doby čekání před pokusem o odeslání rámce. Stav $(-1, 0)$ symbolizuje odesílání rámce.



Obrázek 1 – Model diskrétního dvourozměrného Markovova řetězce

Zdroj: (XIONG, 2008)

kde stav $(r, 0)$ reprezentuje zbývající počet slotů před novým pokusem o odeslání, $(r, -1)$ reprezentuje aktivitu média způsobenou vysíláním jiné stanice, a přičemž hodnota r je určena intervalem: $0 \leq r \leq CW_{max} - 1$.

Více informací o využití Markovových řetězců v bezdrátových sítích lze nalézt v disertační práci „A Markov Chain Approach to IEEE 802.11 WLAN Performance Analysis“ (XIONG,

2008) nebo v článku „*A Markov-Based Channel Model Algorithm for Wireless Networks*“ (KONRAD, a další, 2003).

Dalšími příklady využití dvoustavového diskrétního Markovova modelu (tzv. Gilbertův model) je v experimentu, který provedli Konrad a další (2003) pro výpočet bitové chybovosti sítě (*bit-error rates*) nebo Bianchi (2000 cit. podle WANG a REFAI, s. 1), který použil Markovův model pro výpočet propustnosti MAC vrstvy standardu 802.11.

Nevýhodou těchto modelů je neschopnost modelovat dynamické parametry například chybovost sítě, což je proměnná, která se u bezdrátových sítí rychle mění. Tyto změny jsou způsobeny měnící se úrovní signálu, vlivem různého šíření signálu (útlum, více cestné šíření). (KONRAD, a další, 2003, s. 1)

Některé práce se nicméně snaží metody modelování parametrů bezdrátových sítí zdokonalit. Jedním příkladem může být nahrazení Gilbertova modelu Markovovým řetězcem třetího řádu. Ještě vyšší zpřesnění provedli Konrad a další (2003), kteří navrhli nový algoritmus nazvaný *Markov-based Trace Analysis* (MTA) pro dynamické modelování chybové konstanty. Ta pak lépe odpovídá realitě a přináší oproti tradičnímu Gilbertovu modelu snížení standardní odchylky chyby na hodnotu 8 oproti 22 pro Gilbertův model, respektive 10 pro Markovův model třetího řádu (čím nižší je hodnota odchylky, tím věrněji odpovídá realitě).

I přes zmíněné vylepšení analytického modelování je pro potřeby analýzy současných sítí s jejich složitou architekturou a topologií vhodnější použít některý ze simulačních nástrojů (CHANG, 1999, s. 307).

1.2.2 Počítačová simulace

Počítačovou simulací měření propustnosti je myšleno využití některého ze softwarových nástrojů schopných implementovat kompletní síťový protokol standardu 802.11 a tedy simulovat jeho chování. Jak uvádí Šlinz (2012, s. 33), za takové nástroje lze považovat NetSim, OPNET, Matlab, nebo některý z nekomerčních jako je OMNET++, či ns2. Tyto simulační nástroje poskytují určitou míru abstrakce a uživatel se tak nemusí zabývat podrobnými detaily fungování síťových protokolů.

Počítačová simulace má oproti analytickému modelování výhodu ve schopnosti simulovat dynamické proměnné včetně diskrétních událostí, a to díky schopnosti implementovat kompletní síťový protokol. Výsledky počítačové simulace jsou tak mnohem přesnější než výsledky z analytického modelování. (PELLETTA a VELAYOS, 2005, s. 1)

Počítačové simulaci propustnosti v závislosti na velikosti paketu a odstupu signál/šum se věnovali Ekpenyong a Isabona (2010). Ve své práci také zmínili závislost bitové chybovosti (*bit error rate*) na odstupu signál/šum. Simulace však byla prováděna pouze v ideálních podmínkách. Nebylo tedy přítomno žádné rušení ani jiná degradace signálu vlivem jeho šíření v dynamickém prostředí, což jsou parametry v reálném prostředí všudypřítomné a významně ovlivňující výkonost sítě.

Počítačové simulační modely jsou vhodné pro měření propustnosti v ideálních podmínkách, ovšem v realitě často selhávají. Může za to dynamická a komplikovaná fyzická vrstva bezdrátových sítí, kde je třeba brát v úvahu různé zdroje interferencí a hlavně způsob šíření signálu (JOHNSON a další, 2006 cit. podle LO, 2007, s. 33). Způsob šíření signálu je ovlivněn mnoha faktory od slábnutí signálu vlivem více cestného šíření signálu (*multi-path*), teploty a vlhkosti až po přesun různých objektů (nábytek, otevírání a zavírání dveří) či pohyb osob (LIM, a další, 2006, s. 1). Dalším problémem je nereálnost vytvoření dokonalého modelu prostředí, který by naprosto odpovídal realitě – bylo by nutné vymodelovat dokonale věrně celý interiér budovy včetně všech objektů a jejich vlastností (hustota, reflektivita), a stejně by nebyly brány v úvahu dynamické objekty jako například pohybující se lidé, atd. Hu (2006, s. 31) udává, že i přes zmíněné nedostatky je hlavní výhoda simulace možnost studovat složité síťové topologie, které by v reálném světě bylo nemožné, nebo velice složité realizovat.

Zmíněné vlastnosti analytického modelování a počítačové simulace předurčují tyto metody převážně pro navrhování nových síťových protokolů a pro designéry počítačových sítí, kteří díky nim mohou svou síť nejprve otestovat a teprve poté přejít k implementaci. Tímto postupem jsou sníženy celkové náklady na hardware, který by se bez provedené simulace mohl projevit jako zbytečná investice. (CHANG, 1999, s. 307)

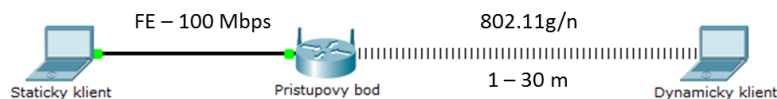
Pelletta a Velayos (2005, s. 1) shrnují faktory, ve kterých simulace nedosahuje parametrů reálného měření, jsou to: výkon hardwaru, propagace signálu a vymodelování okolí. Pro získání exaktních výsledků je proto nutné přistoupit k experimentálnímu měření.

1.2.3 Experimentální měření

Experimentální měření je jediný způsob poskytující přesný vhled do šíření a úrovně signálu v dynamickém a složitém prostředí (LO, 2007, s. 3).

Jedním z nejpoužívanějších způsobů experimentálního měření provedeného v různých pracích (NA, CHEN A RAPPAPORT, 2006; ITO a KAWAGUCHI, 2006) je pevné umístění přístupového bodu, ke kterému je Ethernetovým kabelem připojen jeden z koncových klientů (server, statický klient). K přístupovému bodu je potom bezdrátově připojen druhý klient, jehož vzdálenost se s postupujícím měřením mění (dynamický klient). Klienti jsou nejčastěji reprezentováni notebookem, ale může se jednat i o tablet (vhodné pro mobilního klienta) či stolní PC (statický klient). Cílem měření mohou být různé parametry, nejčastěji se jedná o propustnost, sílu signálu nebo zpoždění. Pokud je měřeným parametrem síla signálu (RSS), v experimentu se vyskytuje pouze přístupový bod a dynamický klient (ITO a KAWAGUCHI, 2006).

Vhodné vzdálenosti pro měření parametrů bezdrátových sítí se pohybují od 2 do 20 metrů (ITO a KAWAGUCHI, 2006 s. 1) či 1–30 metrů (LO, 2007 s. 63).



Obrázek 2 – Obecné schéma experimentálního měření

Zdroj: vlastní

Lo (2007, s. 34) také zmiňuje nevýhody experimentálního měření, je to především časová náročnost, a to kvůli nutnosti opakování měření vlivem dynamických a neovlivnitelných faktorů. Finanční náročnost na koupi určitého hardwaru není dnes natolik podstatná kvůli stále se snižující ceně komponent. Podobně je na tom absence aplikací pro měření propustnosti, kterých je dnes již dostatek, a to i pro různé operační systémy.

Mezi největší úskalí experimentálního měření patří vyvození realistického závěru z provedených měření z důvodu obtížné kontroly externích proměnných, jako jsou odrazy od pohybujících se objektů a rušení od zařízení pracujících na přilehlých frekvencích. (JAMIESON, 2005 cit. podle LO, 2007, s. 34)

Vybrané metody experimentálního měření budou popsány v následující podkapitole.

1.3 Vybrané metody experimentálního měření

Následuje stručný přehled jednotlivých metod experimentálního měření propustnosti a dalších výkonnostních parametrů. Tyto metody budou podrobněji popsány ve třetí kapitole. Všechny tyto metody mohou být prováděny i simulační metodou či analytickým modelováním, nicméně přesnost a vypovídající hodnota takového měření nebude obvykle tak vysoká jako v případě reálného experimentu.

Uvedené metody pro měření propustnosti vycházejí z měření mezi koncovými body (jedná se o tzv. *end-to-end measurement technique*) a mohou být prováděny i uživateli sítě, kteří nemají jakýkoliv administrátorský přístup k síťovým prvkům, přes které přenos dat probíhá. Zejména u klasických počítačových sítí s administrátorským přístupem k síťovým prvkům lze určité výkonnostní parametry spoje zjistit přímo z rozhraní směrovače či přepínače. Jedná se zejména o nominální přenosovou rychlost, průměrné využití spoje a počet bitů/paketů odeslaných za určitý časový interval. Některé tyto parametry zobrazují i přístupové body. (PRASAD, a další, 2003, s. 27)

Měření lze provádět v ideálních podmínkách (uzavřená komora) nebo v reálných podmínkách, kde může být přítomno rušení od ostatních sítí či jiných zdrojů.

1.3.1 Metoda šíření signálu

Eric Lo (2007) se v jeho disertační práci nazvané „*An Investigation of the Impact of Signal Strength on Wi-Fi Link Throughput through Propagation Measurement*“ věnoval praktickému měření propustnosti v závislosti na kvalitě signálu metodou šíření signálu (*propagation measurement*). V této metodě je měřena propustnost sítě a kvalita signálu

v různých vzdálenostech dvou zařízení, tvořených notebookem a přístupovým bodem (AP), ke kterému je bezdrátově připojen druhý notebook v pevné vzdálenosti dvou metrů.

Pro měření kvality signálu byl použit program *WirelessMon*, který je vydáván firmou PassMark a je dostupný pouze pro platformu Windows (LO, 2007, s. 37, 39).

Měření propustnosti bylo vypočítáno podle následujícího vzorce (LO, 2007, s. 37):

$$\text{Propustnost (Mbps)} = \frac{\text{velikost souboru (Mbits)}}{\text{čas přenosu (s)}}$$

Čas pro přenos určitého množství dat byl změřen pomocí stopek a mezi zařízeními byly přenášeny různě velké soubory (vždy o velikosti okolo 200 MB) rozdílných typů (data, audio, video).

1.3.2 Měření propustnosti metodou „packet-by-packet“

Na, Chen a Rappaport (2006) provedli rozsáhlé měření propustnosti na veřejně dostupných hotspotech ve čtyřech restauracích patřící značce „Schlotzsky’s restaurants“. V každé restauraci byl umístěn jeden AP fungující na standardu 802.11b a poskytující otevřený přístup všem zákazníkům restaurace. Propustnost byla měřena třemi nástroji: *LANFielder* 7.0.2, *Iperf* 1.7.0 a *Wget* (FTP klient). Všechny tyto nástroje lze využít k měření propustnosti, ale každý ji měří jiným způsobem a výsledky se proto značně liší. Kvůli minimalizaci faktorů, které by mohly přispět ke zkreslení výsledků (pohybující se zákazníci, vozidla parkující poblíž restaurace) bylo měření propustnosti provedeno pozdě v noci nebo brzo ráno mimo normální otevírací hodiny. Měření probíhalo v jedenácti různých vzdálenostech pro každou restauraci s tím, že některá umístění byla venku (zákazníci se mohou připojit z parkoviště). Měřicí laptop byl vždy postupně umístěn ve všech čtyřech světových stranách a každé měření bylo vypočítáno jako průměr ze tří desetisekundových měření. Kromě propustnosti byly zaznamenávány i hodnoty RSSI a úroveň šumu (*noise level*). Klient byl reprezentován notebookem Dell s dvěma různými síťovými kartami – Cisco Aironet 350 a ORiNOCO Gold. Druhý notebook značky Compaq byl připojen Ethernetovou sítí k AP přes rozbočovač (hub).

Měření potvrdilo velké rozdíly mezi použitými nástroji: *Iperf* ukázal maximální hodnotu propustnosti v první restauraci okolo 5,1 Mbps, *Wget* 4 Mbps a *LANFielder* 1,6 Mbps. Toto měření dokládá, jak důležitá je správná definice propustnosti. Zatímco *Iperf* měří propustnost jako maximální rychlost přenosu TCP (*TCP bandwidth*), *Wget* hlásí rychlost, jakou byl soubor přenesen z FTP serveru. *LANFielder* byl záměrně nastaven pro přenos protokolem UDP (na rozdíl od TCP které využívají *Iperf* i *Wget*) a navíc s volbou dvousměrného přenosu dat (stejná data se přenesou tam a zpět). Toto nastavení v podstatě snižuje propustnost alespoň o polovinu. Naproti tomu rozdíly mezi stejnými nástroji v různých restauracích byly poměrně malé (obvykle jednotky, maximálně desítky procent).

Změřené výsledky byly dále porovnávány s empirickými modely, které dokáží na základě hodnoty SNR odhadnout propustnost. Použity byly dva druhy modelů – *piecewise* a

exponenciální (pomocí funkce *nlinfit* v softwaru MATLAB). Korelační koeficienty křivek získaných z těchto modelů vykazovaly spolehlivost vyšší než 80% pro dvě restaurace a vyšší než 70% pro třetí restauraci.

Druhá část práce se zabývala analýzou dat. Byla prováděna po dobu jednoho týdne, kdy byly dvacet čtyři hodin denně zaznamenány statistiky provozu. Toto zaznamenávání bylo umožněno připojením notebooku zachytávající veškerý provoz přes rozbočovač. Ten každý přijatý paket pošle na všechny své porty (v praxi je toto zařízení nahrazeno bezpečnějším přepínačem – switchem). Celkem bylo takto zachyceno přes 13 miliard paketů, jejichž analýza prokázala, že suverénně nejpoužívanější protokol je HTTP na aplikační vrstvě, respektive TCP (96,8%) na transportní vrstvě. Toto měření potvrzuje vhodnost měření propustnosti právě protokolem TCP.

1.3.3 Metody měření dostupné kapacity

Jak uvádějí Jain a Dovrolis (2003), další velkou oblastí měření výkonu sítě je zjištění dostupné či nevyužité kapacity tzv. *available-bandwidth*, respektive zjištění celkové kapacity spoje (*link capacity*).

Je důležité zmínit, že kapacita podle její definice nerozlišuje užitečnost dat (pokud se nejedná o kapacitu IP vrstvy) a není tedy to samé jako propustnost. Uvedené nástroje však měří dostupnou kapacitu na třetí (například nástroj *Pathload*) nebo vyšší vrstvě, a tak za předpokladu, že v bezdrátové síti neprobíhá jiný provoz, mohou ukazovat podobné hodnoty jako při měření propustnosti. Tímto způsobem lze měřit propustnost.

Tento předpoklad potvrzuje experiment „*End-to-End Available Bandwidth: Measurement Methodology, Dynamics, and Relation with TCP Throughput*“, který provedli Jain a Dovrolis (2003). Autoři v něm zkoumali rozdíl mezi dostupnou kapacitou a propustností u kabelových sítí s probíhajícím provozem. Při dostupné kapacitě okolo 3,5 Mbps dokázal TCP protokol dosáhnout propustnosti až 4,2 Mbps na úkor ostatních TCP spojení, která na spoji probíhala. V případě nulového provozu však lze předpokládat podobné výsledky mezi naměřenou propustností a dostupnou kapacitou.

Zjištění nevyužité kapacity mezi dvěma vzdálenými hosty se v klasických sítích využívá již od protokolu TCP a jeho mechanismu pomalého startu (*slow start*). V něm zařízení pomalu navyšuje rychlost přenosu, dokud není detekováno zahlcení, které je obslouženo mechanismem správy toku (*congestion avoidance*) – přijímací zařízení pomocí ACK paketů signalizuje dosažení maximální možné přenosové rychlosti, na které odesílající zařízení reaguje. (ALLMAN, PAXSON a STEVENS, 1999, s. 2–4)

Další využití je pro management sítě, diagnostiku chyb, *overlay routing*, což je technika dynamického směrování, kdy se směrovací tabulky automaticky upravují v závislosti na využití kapacity různých cest (PRASAD, a další, 2003, s. 27) a ovládání provozu. Způsobů, jak měřit nevyužitou kapacitu v klasických kabelových sítích, existuje celá řada (například HU a STEENKISTE, 2003; JAIN a DOVROLIS, 2003; STRAUSS, KATABI a KAASHOEK, 2003), stejně tak jako teoretických modelů, nicméně u bezdrátových sítí je

situace opačná. Breidel a Fidler (2008, s. 314) shrnují několik zdrojů, ve kterých autoři prakticky ověřili, že díky specifikům bezdrátových sítí i jinak ověřené metody selhávají. Opět za to může již zmiňovaná charakteristika sdíleného média silně ovlivňující všechny parametry bezdrátového přenosu. Specifickou vlastností nevyužití kapacity je její proměnlivost, díky které se měření musí provést co nejrychleji (PRASAD, a další, 2003, s. 29). Johnsson, Melander a Björkman (2006, s. 6) dokázali vliv velikosti paketu na změřenou dostupnou kapacitu – pokud je měřící paket malý, režie datové vrstvy (ACK pakety) je větší, než pokud by byl paket větší. To znamená, že při použití větších měřících paketů experiment změří větší dostupnou kapacitu.

Breidel a Fidler (2008, s. 316–317) uvádějí dva typy metod měření nevyužití kapacity spoje bezdrátových sítí:

Pasivní metody

Pasivní metody jsou založeny na faktu, že médium bezdrátových sítí je sdílené a každý tak může naslouchat aktivnímu přenosu. Metoda počítá čas, kdy žádná stanice nevysílá a zjišťuje tak, kolik kapacity zůstalo nevyužito. Zásadní nedostatek této metody je v případě problému skrytého uzlu. Při tomto problému jsou od sebe dva klienti natolik vzdáleni, že neslyší vysílání toho druhého. Oba však mají dosah k přístupovému bodu. Problém nastává, pokud jeden klient začne vysílat. Druhý klient neslyší žádný přenos, považuje médium za volné a začne také vysílat, což způsobí kolizi. Pokud by tento problém nastal při měření, stanice provádějící analýzu přenosu by nezapočítala vysílání vzdáleného bodu a měření by ukazovalo podstatně nižší využití sítě, než jaké bylo ve skutečnosti.

Aktivní metody

Aktivní metody fungují na principu odesílání tzv. dotazovacích paketů (*probe packets*) mezi dvěma body sítě. Koncový bod ke každému přijatému paketu přiřadí časové razítko a data jsou následně vyhodnocována. Způsob odesílání, struktura paketů a algoritmus vyhodnocení se liší podle použité techniky. (JOHNSON, MELANDER a BJÖRKMAN, 2006, s. 1)

Jiná rozšířená technika je pomocí párových paketů (*the packet pair technique*), kde odesílatel odesílá páry paketů s definovanou časovou mezerou, které jsou koncovým bodem vráceny zpět. Původní odesílatel měří změny mezi dobou přijetí paketů a na jejich základě dokáže určit nevyužitou kapacitu spoje. (HU a STEENKISTE, 2003, s. 879)

Modifikací předchozí metody je metoda paketových vláčků (*packet trains*), kde jsou odesílány vysoké počty paketů konstantní rychlostí. Pokud jsou paketové vláčky posílány s geometricky rostoucí rychlostí přenosu, je tato metoda nazývána paketové potvrzování (*packet chirps*). (BREIDEL a FIDLER, 2008, s. 316)

Výhodou aktivních metod je eliminace problému skrytého uzlu (pokud je zapnut mechanismus RTS/CTS), nevýhodou je určitá režie provozu. Některé z měřících nástrojů

jsou však založeny na určitých předpokladech, které u bezdrátových sítí neplatí, a proto je jejich měření nepoužitelné. Jsou to dva následující předpoklady:

a) Velikost paketu nemá vliv na propustnost / dostupnou kapacitu

Zatímco toto tvrzení je platné u klasických sítí, u bezdrátových sítí platí opak: vzhledem k odlišné fyzické vrstvě velikost paketu značně ovlivňuje dostupnou kapacitu i propustnost. (BREDEL a FIDLER, 2008, s. 315; JOHNSON, MELANDER a BJÖRKMAN, 2006, s. 1)

Poznámka: Breidel a Fidler (2008, s. 315) ve své práci shrnují několik zdrojů, které tvrdí, že velikost paketu má vliv na rychlost přenosu (*bandwidth*): „*Contrary to wired networks a strong impact of packet sizes on bandwidth estimates has been observed for wireless links [15,16,21,19,6]*“ (Na rozdíl od kabelových sítí byl v bezdrátových spojích pozorován silný vliv velikosti paketu na odhad přenosové rychlosti¹). V tomto případě je však zřejmě myšlena dostupná kapacita, protože fyzicky není možné, aby velikost paketu ovlivnila rychlost přenosu dat. Johnson, Melander a Björkman (2006, s. 1) toto tvrzení potvrzují: „*Our experiments show that the measured available bandwidth is dependent on the probe packet size (contrary to what is observed in wired networks)*.“ (Naše experimenty ukázaly, že měřená dostupná kapacita je závislá na velikosti dotazovacího paketu [na rozdíl od kabelových sítí]²).

b) Obsluha paketů stylem „první přijde, první je obsloužen“ (FCFS)

Pakety v klasických kabelových sítích jsou většinou obslouženy stylem FIFO fronty (pokud není aktivní QoS řadící pakety do několika front s různými prioritami). Toto však není u bezdrátových sítí zaručeno, protože přístup klientů k médiu je řízen funkcí DCF (*Distributed Coordination Function*), která počítá s náhodně zvolenými intervaly čekání (BREDEL a FIDLER, 2008, s. 315). Čas, který klient musí před odesláním paketu čekat, je vypočítán podle následujícího vzorce:

$$T_B = random() * T_S$$

Zdroj: vlastní

Kde T_B je celkový čas čekání před pokusem o odeslání (*backoff*), T_S je časová délka jednoho slotu (*slot time*) a *random()* je funkce vybírající náhodné číslo z intervalu. Obě tyto veličiny jsou závislé na fyzické vrstvě a náhodné číslo se zvyšuje s počtem neúspěšných pokusů. Pro DSSS je číslo vybrané z intervalu 1–31 při prvním pokusu o odeslání, při neúspěchu je další pokus zvolen z intervalu 1–63 a tak dále až do hodnoty 1023 (zvyšuje se vždy o mocninu dvou – 1). (GAST, 2005, s. 66–67)

V DCF se může klidně stát, že klient, který chce odeslat paket jako první, bude mít vygenerováno vyšší náhodně zvolené číslo než klient, který chce odeslat data o něco málo

¹ Vlastní překlad.

² Vlastní překlad.

později. To znamená, že schéma FCFS zde není dodrženo a některé měřicí nástroje mohou ukazovat značně zkreslené hodnoty dostupné kapacity.

Jain a Dovrolis (cit. podle BREDEL a FIDLER, 2008, s. 316) uvádějí druhý typ dělení metod pro měření nevyužité kapacity spoje bezdrátových sítí:

Přímé dotazování

Přímé dotazování předpokládá znalost kapacity spoje dopředu (a priori). Měřicí nástroje přímého dotazování jsou: *Spruce*, *WBest* a *IGI*.

Iterativní dotazování

Iterativní dotazování nevyžaduje znalost kapacity. Funguje na principu postupného dotazování s vyššími rychlostmi, dokud nenajde bod zlomu, ve kterém rychlost odezvy začne klesat. Mezi iterativní způsoby měření patří *TOPP*, *DietTOPP*, *PTR*, *Pathload*, *Pathchirp*.

1.3.4 Měření vlivu rádiového rušení na propustnost

Park a další (2003) se zabývali měřením rušení mezi WLAN a třemi zařízeními pracujícími na stejném ISM pásmu (2,4 GHz): mikrovlnné troubě, systém ovládání osvětlení – PLS (plasma lighting system) a bezdrátový robot pro detekci výbušnin používaný na letištích (bezdrátově přenáší obraz z kamer). Autoři prováděli měření s jednotlivými zařízeními postupně při různých vzdálenostech mezi zařízením, AP a klientem. Z testovaných zařízení měla na propustnost největší vliv mikrovlnná trouba. V případě jejího umístění do pěti metrů způsobila podstatné snížení propustnosti celého 2,4 GHz pásma a téměř kompletní zarušení 7. – 10. kanálu (propustnost 0–0,5 Mbps). Propustnost byla ovlivněna lineárně se středem na 8. – 9. kanálu, 1. kanál tak zůstal téměř bez rušení. PLS a bezdrátový robot využívají pouze určité frekvence, které se překrývají pouze s některými kanály WLAN. PLS systém blokuje frekvence 3. – 8. kanálu a na frekvencích prvního, druhého a devátého kanálu způsobuje snížení propustnosti na hraně použitelnosti. Od 10. kanálu lze však WLAN provozovat. Bezdrátový robot využívá frekvenci překrývající se s 11. kanálem a zasahující do sousedních kanálů (9. a 10.). Vzhledem k faktu, že výzkum byl proveden ve Spojených státech, nejsou v experimentu zahrnuty kanály 12, 13 a 14. Lze však předpokládat podobné rušení jako na kanálech 9 a 10 pouze symetricky otočené.

1.3.5 Měření propustnosti více toků

Bredel a Fidler (2008, s. 319–320) se v části své práce dále věnovali měření propustnosti více toků, kdy několik klientů odesílá data najednou a soutěží o dostupnou kapacitu sítě. Tento experiment prověřuje vlastnost DCF (*Distributed Coordination Function*), která by měla zajišťovat rovnoměrné rozprostření kapacity pro všechny klienty.

Měření dvou a čtyř klientů soutěžících o dostupnou kapacitu potvrdilo férovost DCF v případě použití jednotné velikosti všech paketů.

1.3.6 Měření dalších parametrů sítě

Následuje stručný výčet některých dalších provedených experimentálních měření týkajících se dalších dosud nezmiňovaných parametrů. Tyto metody nebudou ve třetí kapitole podrobněji popisovány.

Měření úrovně přijímaného signálu (RSS)

Experimentální měření zkoumající úroveň přijímaného signálu provedl Ito a Kawaguchi (2006). Autoři zkoumali, jak se úroveň přijímaného signálu různých adaptérů liší. V práci došli k závěru, že ukazatel úrovně signálu ukazuje značné rozdíly i mezi stejným výrobcem a v případě návrhu lokalizačního systému je potřeba využít některou upřesňující techniku.

Měření zpoždění

Wang a Refai (2005) provedli jako první měření zpoždění v závislosti na odstupu signál/šum (SNR) pro bezdrátové sítě standardu 802.11g. Tento výzkum je důležitý zejména s nárůstem aplikací vyžadujících rychlou odezvu jako je telefonování (VoIP), videokonference (Skype) či online hraní. Autoři pro generování dat využili skriptu *RealVideo* pro aplikaci *IxChariot*, který mezi dvěma zařízeními přenášel 10 Mbps provoz. Klientská zařízení byla reprezentována notebooky Dell, z nichž jeden byl k AP připojen Ethernetovým kabelem (FE) a druhý přes WLAN 802.11g. Pro zvýšení přesnosti měření byl experiment prováděn o víkendech nebo v pozdních hodinách. Experimentální síť nebyla připojena k internetu a v dosahu nebyla žádná zařízení pracující na podobných frekvencích (ověřeno frekvenčním analyzátozem Tektronix WCA280A).

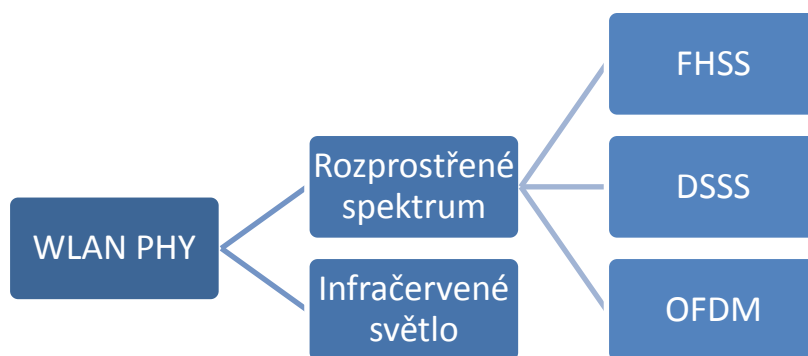
Výsledky ukázaly exponenciální závislost mezi odstupem signál / šum a zpožděním. Zatímco pro SNR 10 dBm bylo zpoždění vyšší než 350 ms, pro 20–60 dBm už to bylo méně než 50 ms (často okolo 10 ms). Výzkum dále prokázal souvislost mezi SNR a počtem ztracených paketů, které vysvětlují dlouhou dobu odezvy při nízkém odstupě signál/šum, vlivem nutnosti znovu ztracené pakety odeslat.

2 Úvod do bezdrátových sítí

Tato kapitola se věnuje vysvětlení základních pojmů bezdrátových sítí a je rozdělena na čtyři podkapitoly. V první podkapitole je vysvětlena historie a základní typy rozprostřeného spektra, což je přenosová technologie, která umožňuje fungování bezdrátových sítí. Následující podkapitola shrnuje IEEE standardy rodiny 802.11 a uvádí jejich základní vlastnosti. Ve třetí podkapitole jsou vysvětleny základní pojmy spojené s bezdrátovými sítěmi. Následuje popis prvků a architektur bezdrátových sítí. Poslední podkapitola pak rozebírá faktory ovlivňující propustnost bezdrátových sítí.

2.1 Rozprostřené spektrum

Bezdrátové sítě na fyzické vrstvě využívají technologii rozprostřeného spektra (*spread spectrum*), za jejímž masovějším rozšířením stojí systém rádiové komunikace americké armády, která potřebovala přenášet data bezpečně, jednoduše a spolehlivě (Planet3 Wireless, Inc., 2002, s. 2). V této podkapitole bude stručně shrnuta historie vzniku rozprostřeného spektra, budou uvedeny jeho základní vlastnosti a následně budou popsány jednotlivé typy rozprostřeného spektra.



Obrázek 3 – Technologie fyzické vrstvy standardu IEEE 802.11

Zdroj: vlastní

2.1.1 Historie vzniku rozprostřeného spektra

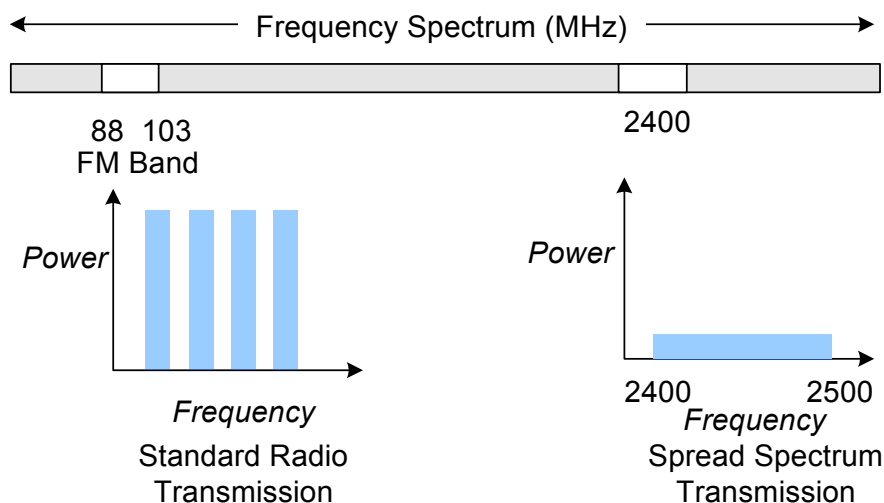
Bezdrátové sítě jsou založeny na technologii rozprostřeného spektra, jejímž prvním představitelem je technika frekvenčních proskoků (*frequency hopping*) podrobněji popsána níže. První výzkum v této oblasti je připisován Nicolovi Teslovi, který v roce 1903 vyplnil patent na systém nazvaný „*Method of Signaling*“. Tento systém je definován vysílačem a přijímačem, které jsou synchronizovány a přeskakují mezi dvěma kanály (frekvencemi) za účelem dosažení vyšší odolnosti proti rušení. V patentu bylo zmíněno, že systém lze modifikovat pro n kanálů, což poprvé zrealizovala německá armáda během první světové války a britským jednotkám tak znemožnila odposlech jejich komunikace. (Nordic Semiconductor, 2012)

Vynález techniky FHSS je připisován herečce Hedy Lamarr (vlastním jménem Eva Maria Kiesler), která v roce 1942 zapsala pod manžellovým jménem patent nazvaný „*Secret*

Communication System“. Jednalo se o systém rádiového řízení torpéda, na kterém pracovala společně s Georgem Antheilem. Systém obsahoval 88 různých kanálů, mezi kterými přijímač a vysílač přeskakovaly v předem dané sekvenci. Armáda však o systém řízení torpéda zájem neměla, a tak bylo FHSS na dalších dvacet let zapomenuto. V šedesátých letech dvacátého století se k němu Armáda spojených států vrátila a poprvé ho využila pro zabezpečenou komunikaci lodí během blokády Kuby. (Nordic Semiconductor, 2012; GAST, 2005, s. 269–270)

2.1.2 Popis rozprostřeného spektra

Rozprostřené spektrum definuje způsob přenášení rádiového či infračerveného signálu v bezdrátové síti na fyzické vrstvě ISO/OSI modelu. Rozprostřené spektrum záměrně přenáší informaci matematickou funkcí rozloženou do širokého frekvenčního intervalu. Tím se liší od klasického rádiového přenosu informace, kde je signál přenášen na jedné frekvenci maximálním výkonem. Porovnání obou druhů komunikace je vyjádřeno následujícím obrázkem. (ZANDL, 2003)



Obrázek 4 – Porovnání standardního a rozprostřeného signálu

Zdroj: (SEXTON, 2012)

Rozprostření signálu přináší oproti klasické rádiové metodě dvě hlavní výhody:

- 1) Odolnost signálu proti rušení

Díky rozprostření signálu do mnohem širšího frekvenčního pásma je nižší šance přerušení přenosu způsobeného rušením. Signál je odolný proti úzkopásmovému rušení, které způsobí pouze snížení rychlosti přenosu dat.

- 2) Nižší vysílaný výkon

Vysílaný výkon je pouze lehce nad úrovní šumu. Tato vlastnost byla výhodná hlavně při prvním používání rozprostřeného spektra v armádě. Šance detekce přenosu nepřátelskou armádou byla mnohem nižší.

Standard 802.11 a jeho dodatky používají tři hlavní typy rozprostřeného spektra:

2.1.3 FHSS

Frekvenční proskoky využívají frekvenční pásmo široké 83,5 MHz rozdělené na 79 nebo 75 kanálů o šířce 1 MHz (zbytek slouží jako ochranné pásmo proti interferencím ze sousedního pásma). Přijímač a vysílač pseudonáhodně střídají kanály, přičemž na každém mohou vysílat maximálně 400 ms a všechny kanály musí vystřídat každých 30 vteřin. (ZANDL, s. 14)

Výhodou FHSS je možnost současného umístění poměrně velkého počtu přístupových bodů. V případě synchronizovaného systému je takto možné umístit až 79 AP (v praxi se nepoužívalo více než 12), u nesynchronizovaného systému až 15 AP. (Planet3 Wireless, Inc., 2002, s. 52)

Nevýhodou jsou poměrně nízké přenosové rychlosti (802.11 dosahuje maximálně 2 Mbps), díky kterým se dnes adaptace tohoto způsobu přenosu používá hlavně u technologie Bluetooth.

2.1.4 DSSS

DSSS neboli přímá sekvence používá oproti FHSS kanály o šíři 22 MHz umožňující dosáhnout vyšších přenosových rychlostí, a to až 11 Mbps v případě standardu 802.11b. V době vydání knihy *Certified Wireless Network Administrator* (2002, s. 55) bylo DSSS nejrozšířenějším typem rozprostřeného spektra zejména kvůli poměrně vysokým přenosovým rychlostem.

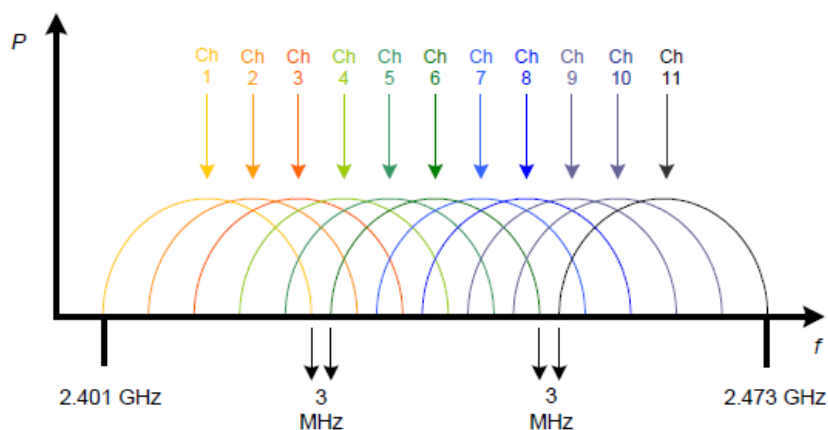
Každý přenášený bit technologií DSSS je převeden na sekvenci bitů tzv. kód (*spreading code*) o délce 10–20 znaků (obvykle 11). Například:

- Bit s hodnotou 1 je převeden na sekvenci 01100100110,
- bit s hodnotou 0 je převeden na sekvenci 10011011001.

Čím větší je délka každého kódu, tím vyšší je odolnost proti úzkopásmovému rušení. Při příjmu signálu lze rozpoznat původní informaci, i pokud je několik bitů ztraceno. (Planet3 Wireless, Inc., 2002, s. 55; SEXTON, 2012)

Dostupné kanály jsou závislé na standardech vydaných pověřenými autoritami v konkrétních zemích. Evropa má oproti Americe navíc kanál 12 (2,467 MHz) a 13 (2,472 MHz), Japonsko smí používat pouze kanál číslo 14 (2,484 MHz). Zatímco kanály 1–13 jsou mezi sebou vzdáleny pouze 5 MHz a tedy se značně překrývají, 14. kanál je od 13. vzdálen 12 MHz. (LESKAROSKI, a další)

Následující obrázek znázorňuje rozložení kanálů pro Severní Ameriku.

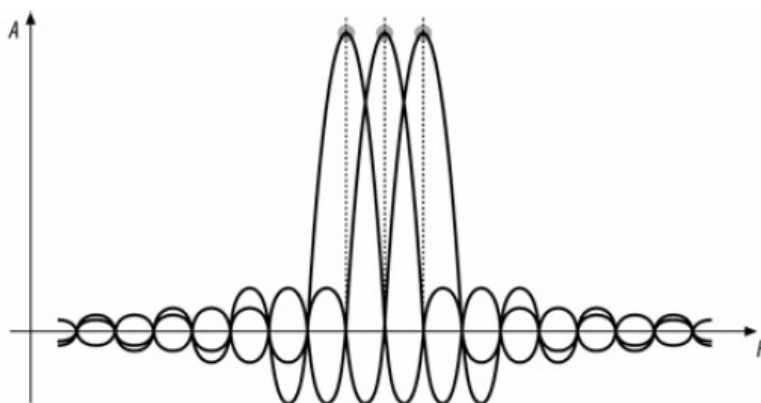


Obrázek 5 – Rozložení kanálů DSSS

Zdroj: (Planet3 Wireless, Inc., 2002, s. 56)

2.1.5 OFDM

OFDM není technologií rozprostřeného pásma, i když se do nich často uvádí, a to kvůli podobným vlastnostem (odolnost proti úzkopásmovému rušení). OFDM je založeno na principu rozdělení jednoho široko-pásmového kanálu na několik sub-kanálů, které pak přenášejí jednotlivá data. Jednotlivé sub-kanály se překrývají, ale jsou uspořádány ortogonálně – data jsou kódována vždy na frekvenci odpovídající maximální amplitudě sub-kanálu (na obrázku vyznačené tečkami), kde jsou amplitudy sousedních signálů nulové. Více informací o detailech OFDM lze nalézt v knize *802.11® Wireless Networks The Definitive Guide* (GAST, 2005).



Obrázek 6 – Ortogonální uspořádání sub-kanálů OFDM

Zdroj: (GAST, 2005, s. 325)

OFDM je používané v technologiích telefonního přenosu internetu – ADSL, HDSL, VDSL a u bezdrátových sítí standardu 802.11a a 802.11g (lehce modifikováno), kde dosahuje přenosových rychlostí až 54 Mbps, respektive 72 Mbps u sítí standardu 802.11n (GAST, 2005).

2.2 Přehled standardů IEEE 802.11

Vznik bezdrátových sítí v podobě, jaké je dnes známe, je datován k roku 1989, kdy začaly práce na standardu 802.11, jehož hlavní parametry (MAC vrstva, fyzická vrstva) byly popsány o pět let později (History of Wireless Local Area Networks (WLANs) in the Unlicensed Bands, 2008). Tato podkapitola poskytuje shrnutí nejdůležitějších standardů rodiny 802.11.

2.2.1 IEEE 802.11

802.11 je prvním standardem bezdrátových sítí přijatým v roce 1997 (ZANDL, 2003, s. 2). V jeho specifikaci je definována jednotná MAC vrstva pro tři různé fyzické vrstvy – DSSS a FHSS pro technologii rozprostřeného spektra (rádiový přenos na frekvencích 2,4–2,4835 GHz) a technologie pro infračervený přenos. (Planet3 Wireless, Inc., 2002; VALADAS, a další, 1998 str. 107)

Přenos v infračerveném pásmu nebude v této práci dále rozebírán, více informací lze nalézt v článku *The Infrared Physical Layer of the IEEE 802.11 Standard for WLAN* (VALADAS, a další, 1998) a *Infrared WLAN* (GEIER, 2003 str. 666).

802.11 definuje dvě přenosové rychlosti 1 a 2 Mbps s tím, že první je povinná a všechna kompatibilní zařízení ji musí podporovat, druhá je pouze volitelná. (SEXTON, 2012).

2.2.2 IEEE 802.11b

802.11b z roku 1999, označován také jako „High-rate“ či WiFi™ je rozšíření původního standardu, které navíc přináší přenosové rychlosti 5,5 a 11 Mbps. Naopak opouští technologii FHSS a zařízení pracující na tomto standardu tak využívají pouze DSSS. (Planet3 Wireless, Inc., 2002)

2.2.3 IEEE 802.11a

Tento standard byl schválen ve stejném roce jako 802.11b (ZANDL, 2003), ale oproti němu přináší výraznou změnu v použitém frekvenčním pásmu, kterým je 5 GHz. Vyšší frekvence přináší lepší přenosovou rychlost a často i menší rušení (pokud jsou v oblasti sítě pracující na frekvenci 2,4 GHz), na druhou stranu má však nižší dosah a horší prostupnost případnými překážkami. Přenosová rychlost 802.11a je až 54 Mbps (Planet3 Wireless, Inc., 2002).

802.11a byl standard původně navržený pouze pro bezdrátová pásma U-NII ve spojených státech. Legislativní úpravy standardu pro Evropu a Japonsko byly definovány ve standardech 802.11h, respektive 802.11j. (GAST, 2005, s. 322)

2.2.4 IEEE 802.11g

Standard 802.11g schválený v roce 2003 je v podstatě pouhým vylepšením a zkombinováním předchozích standardů, s kterými je zpětně kompatibilní (pouze na frekvenci 2,4 GHz). Tato kompatibilita je zaručena použitím ERP (*Extended Rate PHY*) fyzické vrstvy, která obsahuje následující typy:

- a) ERP-DSSS, ERP-CCK – zpětně kompatibilní s 802.11 a 802.11b,
- b) ERP-OFDM – OFDM přejaté z 802.11a implementované na frekvenci 2,4 GHz,
- c) ERP-PBCC – volitelné rozšíření z 802.11b (22 / 33 Mbps), které se prakticky nepoužívá,
- d) DSSS-OFDM – hybridní schéma využívající DSSS pro kódování záhlaví paketu a OFDM pro jeho náklad z důvodu zpětné kompatibility se systémy DSSS. V praxi se také moc nepoužívá. (GAST, 2005, s. 347)

Tento standard je tedy zpětně kompatibilní s 802.11b i klasickým 802.11, ovšem za cenu snížení propustnosti viz podkapitola 2.4.3. V klasickém režimu (OFDM, bez kompatibility) dosahuje přenosových rychlostí standardu 802.11a, tedy 54 Mbps.

2.2.5 IEEE 802.11n

Standard 802.11n byl schválen v roce 2009 a je zpětně kompatibilní se standardem 802.11g, ze kterého vychází (využívá stejnou modulaci OFDM s několika modifikacemi zvyšující propustnost). 802.11n podporuje obě frekvenční pásma (2,4 a 5 GHz), v režimu kompatibility s 802.11g pouze 2,4 GHz. Oproti starším standardům přináší několik zásadních vylepšení: zvýšení základní maximální přenosové rychlosti na 72,2 Mbps (oproti 54 Mbps u 802.11g), volitelnou dvojnásobnou šířku přenosu dat (40 MHz místo 20 MHz) zdvojnásobující propustnost dat (až 150 Mbps) a technologii MIMO. Ta umožňuje využít více antén pro více proudových dat mezi AP a klientem, který musí mít stejný počet antén. Možné konfigurace jsou 2 antény (2 proudy), 3 antény (2 nebo 3 proudy) a 4 antény (4 proudy). Teoretická maximální přenosová rychlost 802.11n tak může dosahovat až 600 Mbps. (SEXTON, 2012)

Pokud má přístupový bod více antén, než je počet proudů, přebytečné antény slouží pro odeslání redundantní informace zvyšující SNR, a tím pádem šanci úspěšného přijetí rámce. Tato technika se označuje jako STBC (*Space-Time Block Coding*) a v podstatě využívá vícecestného šíření signálu, které pro předchozí standardy znamenalo nebezpečí v podobě nižší kvality signálu. (FLUKE NETWORKS, 2008)

2.2.6 IEEE 802.11ac

Jedná se o nový standard, který byl vytvářen v letech 2011–2013 a jeho finální schválení by mělo proběhnout v únoru roku 2014 (Stephen MCCAN, 2013). Tento standard si klade za cíl dosáhnout podobné propustnosti, jako má gigabitový Ethernet. Předpokládaná maximální přenosová rychlost by mohla být až 1,3 Gbps (při použití zařízení podporující simultánní přenos třech datových proudů při šířce pásma 80 MHz), což by odpovídalo propustnosti okolo 910 Mbps (CISCO, 2012, s. 6–7). Reálné testy s prvními zařízeními v domácích podmínkách ukazují reálnou propustnost okolo 600 Mbps při přenosu dat mezi dvěma stejnými přístupovými body, či okolo 400 Mbps při přenosu dat mezi klientem a přístupovým bodem³.

³ <http://www.pcworld.com/article/2050761/netgear-nighthawk-review-this-802-11ac-router-sets-lan-speed-records.html>

802.11ac pracuje pouze na frekvenci 5 GHz, ale současně vyráběné AP podporují smíšený režim, ve kterém dokáže obsluhovat i klienty pracující se standardy 802.11a/b/g/n. Významným vylepšením je tzv. multiuser MIMO (multiple input-multiple output), který AP umožňuje komunikovat s několika klienty najednou za využití více antén a přenosu na různých frekvencích. Díky tomuto systému se bezdrátové sítě přibližují k přepínačům pracujících jako *full-duplex* místo dosavadním rozbočovačům. Maximální počet MIMO antén je navýšen na osm. (CISCO, 2012)

K dosažení vyšších rychlostí je použito širší pásmo, a to 80, respektive 160 MHz, což je čtyřnásobek oproti, 20 respektive 40 MHz u 802.11n. Cisco (2012, s. 5) udává, že zdvojnásobení šířky ze 40 na 80 MHz pásma přináší 2,16 násobné zvýšení přenosové rychlosti. Pro zachování zpětné kompatibility je možné využít 20 a 40 MHz pásma. Dále je použita modulace 256QAM, která podle Cisco (2012, s. 5) při stejných nárocích na frekvenční spektrum přispívá ke zrychlení o 33% oproti standardu 802.11n.

2.2.7 Shrnutí základních vlastností standardů 802.11

Následující tabulka shrnuje nejdůležitější parametry všech zmíněných standardů. U standardů 802.11n/ac jsou uvedeny přenosové rychlosti při použití jednoho datového přenosu. Při použití více datových přenosů pomocí technologie MIMO lze přenosovou rychlost zčtyřnásobit (n), respektive zosminásobit (ac).

Tabulka 1 – Přehled základních parametrů standardů 802.11

Standard	Datum schválení	Frekvence	Technologie SS (modulace)	Max. počet MIMO	Šířka pásma	Přenosová rychlost (Mbps)
802.11	1997	2,4 GHz	DHSS, FHSS	1	20 MHz	1,2
802.11a	1999	5 GHz	OFDM	1	20 MHz	6,9,12,18, 24,36,48,54
802.11b	1999	2,4 GHz	DSSS	1	20 MHz	5,5,11
802.11g	2003	2,4 GHz	OFDM, DSSS	1	20 MHz	6,9,12,18, 24,36,48,54
802.11n	2009	2,4 / 5 GHz	OFDM (64QAM)	4	20 MHz	7.2,14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2
					40 MHz	15, 30, 45, 60, 90, 120, 135, 150
802.11ac	2014?	5 GHz	OFDM (256QAM)	8	80 MHz	až 433*
					160 MHz	až 867*

* podporované rychlosti jsou závislé na konkrétní implementaci, zde uvedeny jen maximální hodnoty

Zdroj: zpracováno dle (SEXTON, 2012; CISCO 2012)

2.3 Základní pojmy bezdrátových sítí

Následující podkapitola je věnovaná stručnému vysvětlení základních pojmů zmiňovaných v souvislosti s bezdrátovými sítěmi a měřením jejich parametrů. V závorce u každého pojmu jsou vždy uvedené anglické výrazy, pod kterými se označuje.

2.3.1 Základní fyzikální pojmy rádiového přenosu

Bezdrátové sítě standardu 802.11 jsou založeny na rádiovém přenosu (mikrovlny, nebo infračervené záření). V této podkapitole budou proto vysvětleny nejpoužívanější pojmy související s rádiovým přenosem dat.

Frekvence (*frequency*)

Frekvence je definována jako počet oscilací signálu za jednu vteřinu. Označuje se f a udává se v hertzech (Hz) (SEXTON, 2012).

Vlnová délka (*wavelength*)

Vlnová délka je délka jednoho oscilačního cyklu signálu. Označuje se λ a u bezdrátových sítí se obvykle označuje v centimetrech. Vlnová délka a frekvence jsou odvoditelné podle následujících vzorců:

$$f = \frac{c}{\lambda} [Hz] \quad \lambda = \frac{c}{f} [m]$$

Zdroj: (SEXTON, 2012)

Kde c je rychlost světla v metrech za sekundu. Vlnová délka signálu bezdrátových sítí o frekvenci 2,4 GHz je tak okolo 12,5 cm, na frekvenci 5 GHz je to okolo 6 cm.

Amplituda (*amplitude, power level*)

Amplituda je úroveň signálu a značí jeho výkon. Udává se ve wattech (W) nebo v decibelech (dB). Zvýšení amplitudy se nazývá zisk (*gain*), snížení pak ztráta (*loss*). (Planet3 Wireless, Inc., 2002, s. 19–20)

Fáze (*phase*)

Fáze je určena časovým posunem mezi dvěma signály a tak se udává ve stupních (°) (SEXTON, 2012).

Frekvenční pásmo (*frequency band*)

Frekvenční pásmo lze definovat stejně jako šířku pásma:

Šířka pásma (*bandwidth*)

Bandwidth v kontextu fyzické vrstvy značí spektrální šířku elektromagnetických signálů (PRASAD, a další, 2003), neboli rozdíl mezi maximální a minimální frekvencí v určitém frekvenčním pásmu (OUELLET, a další, 2002, s. 40–41).

2.3.2 Parametry výkonu sítě

Tato podkapitola se věnuje vysvětlení pojmů spojenými s měřením výkonu bezdrátových sítí.

Přenosová rychlost (*bandwidth, data rate, transmission rate, headline rate, radio data rate, nominal transmission speed*)

Přenosová rychlost udává rychlost, kterou je spoj schopen konstantně přenášet na fyzické vrstvě, tím pádem nerozlišuje, o jaká data se jedná. Přenosová rychlost je limitována fyzickými vlastnostmi média, po kterém jsou informace přenášeny a odesílající / přijímací elektronikou. Příkladem může být 10BaseT Ethernet, který má přenosovou rychlost 10 Mbps, nebo bezdrátová síť standardu 802.11g s přenosovou rychlostí 54 Mbps. (PRASAD a další, 2003, s. 28)

Bandwidth v kontextu datových sítí vyčísľuje rychlost přenosu dat, které je daný spoj schopen dosáhnout (PRASAD, a další, 2003; GAST, 2005, s. 625). Aktuální rychlost přenosu dat bezdrátové sítě se však může měnit a je určena funkcí DRS zmíněnou v kapitole 2.4.1.

Kapacita spoje (*capacity, bandwidth, maximum possible bandwidth*)

Obvykle se udává v bitech za sekundu (bps) a nebere v úvahu povahu dat, a tedy nerozlišuje, zda se jedná o užitečná data, či nikoliv. Kapacita spoje a rychlost přenosu dat vyjadřují stejnou věc a často jsou v literatuře zaměňovány (STRAUSS, a další, 2003) (PRASAD, a další, 2003).

Kapacita může být vyjádřena vzhledem k určité vrstvě ISO/OSI modelu. Kapacita IP vrstvy tak závisí na poměru velikosti paketu k velikosti režie druhé vrstvy (záhlaví a zápatí rámce). Příkladem může být opět 10BaseT Ethernet s kapacitou 10 Mbps, kde režie druhé vrstvy tvoří 38 bajtů. Pokud je velikost paketu 1500 bajtů, kapacita IP vrstvy bude rovna 9,75 Mbps, což ilustruje následující vzorec (PRASAD a další, 2003, s. 28):

$$C_{L3} = C_{L2} \frac{1}{1 + \frac{H_{L2}}{L_{L3}}} = 10^6 \frac{1}{1 + \frac{38}{1500}} = 9,75 * 10^6 bps$$

kde C_{L2} – je kapacita spoje druhé vrstvy ISO/OSI modelu v bajtech za sekundu,
 H_{L2} – je velikost záhlaví a zápatí rámce v bajtech,
 L_{L3} – je celková velikost paketu v bajtech.

Pokud je spojení tvořeno více spoji, je celková kapacita spojení C rovna kapacitě nejpomalejšího spoje:

$$C = \min_{i=1...H} C_i$$

Zdroj: (JAIN a DOVROLIS, 2003)

kde C_i – je rychlost v bitech za sekundu jednotlivých spojů.

Dostupná kapacita spoje (*available bandwidth, unused capacity / bandwidth*)

Je rovna kapacitě spoje minus provoz na spoji, který je nazýván *cross-traffic*. Udává volnou (nevyužitou) kapacitu spoje v časovém intervalu. Strauss, Katabi a Kaashoek (2003) poukazují na zřejmý poznatek, kterým je fakt, že v daném čase je spoj buď nevyužitý, nebo maximálně využitý (nelze data odesílat poloviční rychlostí). Proto musí být dostupná kapacita spoje měřena jako průměr nevyužité kapacity spoje po dobu trvání určitého časového intervalu T.

Metody využívající zjednodušený síťový model, vyjádřen následujícím vzorcem (BREDEL a FIDLER, 2008, s.316) :

$$AB = C(1 - u)$$

kde C – je kapacita spoje,
u – je aktuální provoz na spoji (*cross-traffic*).

Dostupná kapacita spoje je dále ovlivněna kvalitou signálu. Vzorec pro výpočet ovlivnění kapacity definoval Claude Shannon jako:

$$C = BW * \log_2\left(1 + \frac{S}{N}\right)$$

Zdroj: (OUELLET, a další, 2002, s. 43–44)

kde C – je výsledná dostupná kapacita spoje,
BW – je dostupná kapacita,
S/N – je poměr odstupu signál/šum.

Propustnost (*throughput, payload throughput, bulk transfer capacity*)

Propustnost udává, kolik bitů je možné za jednu sekundu přenést mezi aplikační vrstvou. Data nižších vrstev jsou brána jako režie a nejsou v propustnosti brány v potaz. Měří se v bitech za sekundu. (GAST, 2005; PRASAD, a další, 2003)

U propustnosti se někdy uvádí, jaký protokol transportní vrstvy je použit – TCP nebo UDP (například *TCP throughput*). Prasad a další (2003, s. 29) uvádějí, že 90% provozu dat na internetu je zrealizováno protokolem TCP. Jednotlivé parametry TCP jako je počet současných spojení, velikost bufferů na obou stranách spojení a na zařízeních podél cesty významně ovlivňují celkovou propustnost. RFC 2581, které definuje protokol TCP, však neuvádí všechny jeho parametry, a proto se některé implementační detaily mohou u různých výrobců HW lišit. (PRASAD a další, 2003)

V knize *Certified Wireless Network Administrator* (Planet3 Wireless, Inc., 2002, s. 235) je zmíněno, že propustnost sítě 802.11 je rovna zhruba polovině rychlosti přenosu dat, která je tím pádem veličinou nejvíce ovlivňující celkovou propustnost.

BTC (*Bulk Transfer Capacity*) je definována jako maximální propustnost dosažitelná jedním TCP spojením (PRASAD a další, 2003, s. 29). Jain a Dovrolis (2003, s. 10) však BTC definují odlišně, a to jako TCP spojení, které je limitováno pouze výkonem sítě a ne výkonem koncových zařízení. V této práci bude dále používána pouze základní definice propustnosti, a tak žádná z definic BTC dále používaná nebude.

Celková propustnost oblasti (*total area throughput*)

Gast (2005, s. 577) definoval pojem celkové propustnosti oblasti (jinak také nazývané *throughput per unit of area*), která odpovídá součtu propustností všech přístupových bodů v jedné buňce. Přístupové body tedy musejí pokrývat stejnou oblast a pro dosažení nejvyšší možné propustnosti musí být zaručeno, že se navzájem neruší (v případě DSSS lze využít kanály 1, 6, 11).

2.3.3 Parametry úrovně signálu

V této části budou vysvětleny parametry určující úroveň signálu.

Bitová chybovost (*bit-error rate, BER*)

Bitová chybovost je určena poměrem mezi počtem přijatých chybných bitů a celkovým počtem odeslaných bitů za určitý časový interval. Čím vyšší je hodnota BER, tím nižší je propustnost, a naopak vyšší latence sítě a šance, že paket nebude doručen. Vyšší hodnota BER je často zapříčiněna nízkými hodnotami SNR nebo SIR vysvětlenými dále. (LO, 2007, s. 27–28).

Odstup signál šum (*signal-to-noise ratio, SNR*)

Odstup signál šum vyjadřuje poměr mezi silou signálu a okolním šumem a měří se v decibelech. Na rozdíl od úzkopásmového vysílání, kde je SNR v řádu desítek – pro FM rádio okolo 70 dBm (Dirac Delta, 2005), jsou bezdrátové sítě vzhledem k principům rozprostřeného pásma uzpůsobené pro práci s mnohonásobně nižším SNR typicky okolo hodnoty –50 dBm.

Na, Chen a Rappaport (2006, s. 3298) uvádějí, že odstup signál šum je jedním z nejdůležitějších, ne-li nejdůležitější jednotkou charakterizující radiové podmínky kanálu (RF). Wang a Refai (2005 cit. podle LO, 2007, s. 27) provedli studii, která dokázala exponenciální vztah mezi SNR a odezvou sítě.

Odstup signál interference (*signal-to-interference ratio, SIR*)

SIR měří poměr mezi silou signálu a interferencemi způsobenými jinými systémy. Vyšší hodnota SIR znamená lepší kvalitu signálu a menší počet interferencí. Čím vyšší je signál ostatních sítí vysílajících na stejných či sousedních kanálech, tím je hodnota SIR nižší. (LO, 2007, s. 28) Pokud ve stejné oblasti vysílá více bezdrátových sítí na stejných kanálech, snižuje se hodnota SIR tím více, čím aktivněji jednotlivé sítě vysílají (pokud by vysílala jen jedna síť, nebude přítomno žádné rušení).

Na, Chen a Rappaport (2006, s. 3298–3299) zmiňují, že v případě buňkového systému (ESS) je SIR hlavním limitujícím faktorem ovlivňující dosažitelnou propustnost.

Ukazatel přijímané úrovně signálu (*RSS a RSSI*)

RSS a RSSI (*Received Signal Strength Indicator*) jsou dvě používané hodnoty pro určování síly přijímaného signálu. Nevyjadřují však tu samou věc. RSS je reálná hodnota udávající přijímanou úroveň signálu v mW nebo dBm (LO, 2007, s. 30). Naproti tomu RSSI je bezrozměrná veličina udávající sílu signálu v určitém intervalu nezáporných hodnot. Konkrétní škála a přiřazení RSS na RSSI závisí na výrobci, většinou se jedná o interval 0–255. (MYCLE, 2011)

Provedené výzkumy ukazují téměř lineární závislost mezi RSS a propustností. Při použití standardu 802.11b lze dosáhnout propustnosti 4,8 Mbps při RSS nad hodnotou –85 dBm. Od této hodnoty propustnost lineárně klesá se snižujícím se RSS až do hodnoty okolo –97 dBm, kdy je propustnost nulová. (PRASAD, 2000 cit podle WANG a REFAI, 2005, s. 1)

2.3.4 Prvky bezdrátových sítí

Tento článek popisuje základní stavební prvky bezdrátových sítí, z kterých se WLAN skládají.

Přístupový bod (*Access Point*)

AP je nejdůležitějším prvkem bezdrátové sítě. Zprostředkovává komunikaci mezi klienty sítě a tvoří rozhraní mezi kabelovou a bezdrátovou sítí (ZANDL, 2003, s. 6). Jedná se o zařízení s podobnými vlastnostmi jako přepínač (*switch*) v kabelových sítích, jen je třeba připomenout, že vzhledem ke sdílenému médiu bezdrátových sítí je jejich komunikace pouze *half-duplex* (komunikace nemůže probíhat oběma směry ve stejné chvíli). Přístupový bod může pracovat v několika režimech: *root mode* (nejběžnější), *repeater mode* (jeden AP v *root* módu, druhý k němu připojen jako opakovač pro zvýšení pokrytí sítě) a *bridge mode* – P2P (spojení typu bod-bod, například mezi budovami). Přístupové body mohou být vybaveny interními či externími anténami, které mohou být vyměnitelné. AP jsou často napájeny přes Ethernetový kabel (PoE), což usnadňuje jejich montáž. (Planet3 Wireless, Inc., 2002, s. 72–75)

Klient (*client, host*)

Klient, někdy také označovaný host, koncové zařízení či stanice je reprezentován koncovými uzly sítě, kterými jsou zařízení, jako je PC, notebook, PDA, chytrý telefon či jiné zařízení podporující připojení k bezdrátové síti. (Planet3 Wireless, Inc., 2002, s. 86)

Klient může komunikovat s ostatními klienty či s kabelovou sítí včetně internetu, ke které je přístupový bod připojen (pokud je tak přístupový bod nastaven). Je důležité zmínit, že komunikace mezi klienty probíhá vždy přes přístupový bod, což může zejména při přenosu větších objemů dat značně zvýšit dobu odezvy a snížit propustnost sítě.

Bezdrátové médium

Je médiem, které zprostředkovává přenos informace. U klasických kabelových sítí se jedná o kabel (ať už metalický či optický), u bezdrátových sítí je to pak rádiová frekvence. Jak poznamenává Zandl (2003), vzduch není považován za médium, bezdrátové sítě totiž mohou fungovat i ve vzduchoprázdnu.

2.3.5 Architektury bezdrátových sítí

Bezdrátové sítě mohou tvořit tři typy architektur – ad-hoc, infrastrukturní síť a rozšířenou oblast služeb. Všechny tyto architektury vyžadují konfiguraci SSID (*Service Set Identifier*), což je alfanumerický řetězec o maximální délce 32 znaků rozlišující malá a velká písmena, který slouží klientům k jednoduché identifikaci sítě (klient připojující se k WLAN obvykle konfiguruje dva parametry: SSID a heslo). V počátcích bezdrátových sítí byl SSID brán jako primitivní způsob zabezpečení vzhledem k tomu, že je přístupovým bodem periodicky vysílán všem zařízením v dosahu (případně se dá snadno zachytit, jelikož je posílán nezašifrovaně), nejedná se dnes v žádném případě o zabezpečovací prvek. (Planet3 Wireless, Inc., 2002, s. 168; SEXTON, 2012)

Ad-hoc síť

Ad-hoc síť také označovaná jako IBSS (*Independent Basic Service Set*) či P2P síť (*peer-to-peer*) je komunikací klientů bez přístupového bodu. Často se používá pro rychlé sdílení souborů mezi klienty bez přístupu k internetu či jiné kabelové síti. Jeden z klientů však může zajišťovat směrování do jiných sítí, pokud má druhé rozhraní a je správně nastaven. Jediný rozdíl mezi ad-hoc sítí a infrastrukturní sítí pak je použití jednoho klienta místo přístupového bodu a fakt, že klienti mohou komunikovat přímo mezi sebou. (Planet3 Wireless, Inc., 2002, s. 182–183)

Infrastrukturní síť – BSS

Infrastrukturní síť, neboli BSS (*Basic Service Set*) je základní stavební blok bezdrátových sítí. BSS obsahuje klienty a přístupový bod, který může být připojen ke kabelové síti. Pokrytí přístupového bodu se nazývá buňka (*cell*). Každá buňka je identifikována 48 bitovou MAC adresou přístupového bodu, označovanou jako BSSID (*Basic Service Set Identifier*). (SEXTON, 2012)

Druhý identifikátor, který je vysíláný přístupovým bodem v pravidelných intervalech (*beacon*) je SSID (*Service Set Identifier*). Jedná se o alfanumerický řetězec o maximální délce 32 znaků, rozlišující malá a velká písmena, který slouží klientům k jednoduché identifikaci sítě (klient připojující se k WLAN obvykle konfiguruje dva parametry: SSID a heslo). (Planet3 Wireless, Inc., 2002, s. 168)

Rozšířená oblast služeb – ESS

ESS (*Extended Service Set*) umožňuje propojit několik BSS do jedné fungující sítě, ve které se mohou klienti libovolně pohybovat bez ztráty konektivity. ESS je identifikován

síťovým jménem ESSID (*Extended Service Set ID*), což je pouze jiný název pro SSID použitým u ostatních typů sítí. U rozšířené oblasti služeb musí být na všech přístupových bodech tvořících tuto architekturu nastaveny stejné SSID. ESS zajišťuje *roaming* klientů – plynulé přecházení mezi buňkami bez ztráty konektivity a bez nutnosti nějak měnit nastavení na klientských zařízeních. Předání klienta (*handoff*) mezi buňkami je řízeno přístupovými body, které spolu komunikují přes distribuční systém obvykle tvořený kabelovou sítí. (SEXTON, 2012; Planet3 Wireless, Inc., 2002, s. 182–184)

2.4 Faktory ovlivňující propustnost bezdrátové sítě

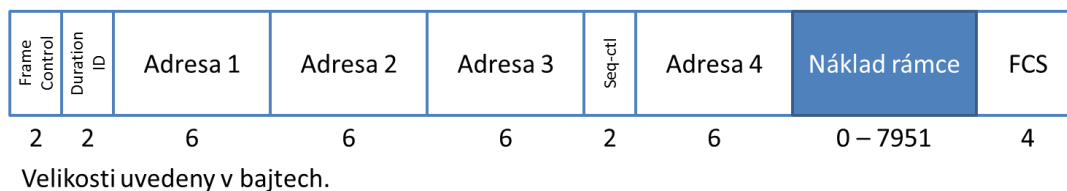
Tato kapitola shrnuje a vysvětluje faktory ovlivňující propustnost bezdrátové sítě. Uvedené faktory jsou specifické pro bezdrátové sítě a týkají se linkové a nižší vrstvy. Obecné faktory ovlivňující propustnost jako je režie síťové a transportní vrstvy nejsou brány v potaz. Faktory bezdrátových sítí ovlivňující propustnost lze rozdělit na tři hlavní skupiny, faktory způsobené MAC vrstvou, šířením signálu a ostatní.

2.4.1 Režie MAC protokolu – velikost paketu

MAC protokol standardu 802.11 má oproti kabelovým sítím svá specifika. Je navržen pro fungování na nespolehlivém médiu s dynamicky se měnícími parametry, což ovšem stojí určitou režii.

Struktura rámce – režie záhlaví a zápatí

Následující obrázek zobrazuje základní strukturu rámce standardu 802.11. Rámec může být menší či větší v závislosti na přítomných parametrech. Povinné pole jsou: *Frame Control*, *Duration/ID*, adresa 1 a *FCS*. Rámec může obsahovat i další neuvedená volitelná pole jako například *QoS* nebo *HT Control*. Jeho velikost bude potom ještě větší.



Obrázek 7 – Struktura typického rámce 802.11

Zdroj: zpracováno dle (IEEE Std 802.11™, 2012, s. 381–382; ROZHAN a LEARY, 2003, s. 73)

Z uvedené struktury rámce je patrné, že záhlaví a zápatí zvyšuje jeho velikost o 34 bajtů (podle nastavených parametrů to může být 14–40 bajtů). Z experimentu, který provedli Na, Chen a Rappaport (2006) vyplynulo, že v bezdrátových sítích se nejčastěji vyskytují pakety o velikosti větší než 1470 bajtů (hlavně příchozí provoz), nebo naopak menší než 100 bajtů (odchozí provoz). V případě paketů o velikosti 1470 bajtů tvoří režie záhlaví a zápatí MAC protokolu pouhé 2,3%, nicméně při paketech o velikosti 100 bajtů je to rovných 34%.

Větší velikost paketu však nemusí vždy znamenat lepší propustnost. Větší pakety potřebují na jejich odeslání delší čas, čímž se zvyšuje riziko ztráty paketu vlivem proměnlivého stavu média. Navíc se také zvyšuje odezva sítě. Pokud je kvalita spoje nízká a dochází k častým ztrátám paketů, které potom vyžadují jejich znovu odeslání, je menší velikost paketu výhodou. Šance, že bude malý paket ztracen je nižší, a proto může být celková propustnost vyšší. Tohoto faktu využívá fragmentace paketů. Velikost paketu je tedy vždy kompromisem mezi propustností a dobou odezvy, přičemž je třeba brát ohled na kvalitu bezdrátového média.

Časové intervaly mezi rámci (mezirámcové mezery)

Časové intervaly mezi rámci (IFS) definují dobu trvání různých časových mezer před odesláním rámců. Tyto intervaly určují prioritu různým typům zpráv. Pokud zařízení chce odeslat zprávu a neslyší žádné probíhající vysílání, musí nejprve počkat daný interval, než se může pokusit zprávu odeslat. Celkem existuje šest typů intervalů, ale nejpoužívanější jsou tři. SIFS, DIFS a PIFS.

SIFS je nejkratším intervalem a nejčastěji je používán před odesláním ACK, RTS a CTS zpráv. Tyto rámce slouží pro řízení toku provozu (*control frames*), a proto mají nejvyšší prioritu a jsou odeslány před jakýmkoliv jinými rámci.

DIFS je nejdelším intervalem a je používán klienty před odesláním obvyklého provozu. Tyto rámce tak mají nejnižší prioritu. Aby se nestalo, že po vypršení DIFS intervalu začnou vysílat všichni klienti naráz, každý klient navíc čeká náhodně zvolenou dobu (*random backoff*).

PIFS svoji délkou patří mezi SIFS a DIFS intervaly. Používá se pouze, pokud je aktivní PCF a slouží jako interval před odesláním řídicích rámců PCF přístupovým bodem. Řídící mechanismus má tak vyšší prioritu než provoz klientů sítě.

Délky uvedených intervalů systému DSSS jsou 10 mikrosekund pro SIFS, 30 PIFS a 50 pro DIFS. Další typy intervalů slouží zejména pro systém QoS (AIFS) a pro zotavení z chyby při přenosu (EIFS).

(IEEE Std 802.11™, 2012, s. 826–828) (Planet3 Wireless, Inc., 2002, s. 207–209)

Automatické ovládání rychlosti toku (DRS)

S rostoucí vzdáleností klienta od přístupového bodu či s rostoucím rušením se snižuje kvalita signálu určená přijímaným RSS. Aby byl přenos dat možný, klient může použít nižší rychlost přenosu dat, což zabezpečuje systém DRS (*Dynamic Rate Shifting*), někdy také nazýván ARS (*Adaptive Rate Selection*). Pokud systém zjistí, že při současné přenosové rychlosti dochází ke ztrátám paketů, provede skok na nejbližší z nižších diskrétně definovaných hodnot přenosových rychlostí. U standardu 802.11g při OFDM modulaci tak může provést skok z 54 Mbps na 48 Mbps. (Planet3 Wireless, Inc., 2002, s. 205–206)

Algoritmus detekce kvality signálu není standardem definována a závisí tak na implementaci výrobce. Obecně však závisí na kvalitě rádiového prostředí (RF), jež je určena několika parametry, jako je RSS, SNR nebo SIR. Jednoduchou implementaci závislé pouze na přijatých ACK paketech uvádí Sexton (2012): systém začíná vysílat na maximální možné rychlosti, pokud však dojde ke ztrátě dvou po sobě jdoucích zpráv, rychlost přenosu se sníží o jednu úroveň. K opětovnému zvýšení o jednu úroveň dojde, pokud je deset po sobě jdoucích zpráv přijato v pořádku.

Zvolená rychlost přenosu přímo ovlivňuje propustnost, jež odpovídá zhruba její polovině.

Potvrzovací pakety ACK

Potvrzovací pakety slouží pro oznámení přijetí paketu odesílajícímu zařízení. Každý odeslaný paket musí být potvrzen, jinak je považován za ztracený a vysílající zařízení se pravděpodobně pokusí paket odeslat znovu. Velikost ACK je pouhých 14 bajtů, protože oproti standardnímu rámci má pouze první tři pole a zápatí. K režii potvrzovacích paketů je také třeba připočíst SIFS interval před jeho odesláním a režii zpracování vysílačem a přijímačem. (GAST, 2005)

Je důležité zmínit, že management a kontrolní rámce standardu 802.11 nejsou přenášeny maximální přenosovou rychlostí, ani aktuální rychlostí přenosu. Většinou mají pevně definovanou přenosovou rychlost, která je kompromisem mezi rychlostí a spolehlivostí. Gast (2005, s. 626) uvádí jako příklad přenosovou rychlost ACK paketů 24 Mbps pro standard 802.11a.

Režii potvrzovacích paketů snižuje mechanismus blokových potvrzovacích paketů implementovaný ve standardech 802.11n a 802.11ac. V tomto případě není nutné potvrzovat každý odeslaný rámec, ale potvrdí se až blok přijatých rámců, který může být složen z maximálně 64 rámců. Blokový potvrzovací paket (BA) obsahuje bitmapu umožňující potvrzení jednotlivých rámců a v případě potřeby dojde k přeposlání pouze ztracených rámců. (LEUTERT, 2009)

Fragmentace

Maximální velikost rámce odeslaného v síti standardu 802.11 je 1518 bajtů. Pokud je rámec větší, nebo je nastaven nižší limit fragmentace než je velikost rámce, musí být rámec fragmentován na více částí. Nastavení nižší maximální velikosti rámce je vhodné při zhoršených přenosových podmínkách. Tato velikost může být nastavena na přenosovém bodu ručně, případně lze využít funkci automatické snížení velikosti při detekci vysokého počtu ztracených rámců. (Planet3 Wireless, Inc., 2002, s. 204–205)

RTS/CTS

RTS/CTS je rozšíření mechanismu CSMA/CA a jedná se o systém alokace času na médiu pro přenos dat. Pokud chce klient odeslat nějaká data, nejprve požádá cílovou stanici. Ta všem klientům v síti nastaví NAV (*Network Allocation Vector*) sloužící jako časovač (na

délku přenosu včetně paketu ACK). Všichni klienti sítě tak ví, na jakou dobu bude médium obsazené. RTS/CTS představuje pro síť značnou režii ústící ve významné snížení propustnosti. Tento systém se tak používá pouze v nezbytných případech, kterými může být problém skrytého uzlu nebo režim koexistence více standardů. (Planet3 Wireless, Inc., 2002, s. 212)

DCF/PCF

DCF a PCF jsou metody řízení přístupu, umožňující klientům sítě soupeřit o dostupné médium. DCF využívá CSMA/CA protokol, což odpovídá standardu 802.3 v případě použití rozbočovačů. Tento mód se používá ve všech třech architekturách bezdrátových sítí. PCF využívá systém dotazování (*polling*), které provádí přístupový bod (PCF nemůže být použit v architektuře ad-hoc). Jedná se o jakousi nadstavbu módu DCF a využívá některé jeho funkce. Výhodou tohoto módu je předem známá doba latence, přesto se však v praxi moc nepoužívá. (Planet3 Wireless, Inc., 2002, s. 206)

2.4.2 Úroveň rádiového signálu

Výkon bezdrátových sítí je úzce svázán s kvalitou rádiového signálu. Jeho úroveň, respektive jeho degradace je závislá na několika faktorech, jsou to:

Útlum (*free path loss*)

S rostoucí vzdáleností od vysílače se snižuje síla signálu vlivem jeho rozšiřování. Největší ztráta signálu nastává, pokud je vysílač izotropní, a tedy vysílá signál všemi směry.

Úroveň signálu v dané vzdálenosti r je určena vzorcem (SEXTON, 2012):

$$\rho = \frac{PG}{4\pi r^2} [\text{wattů}/\text{m}^2]$$

Kde P je vysílaný výkon ve wattech a G je zisk antény (v případě izotropního zářiče je roven jedné). Z prostého dosazení hodnot do vzorce lze spočítat, že při zdvojnásobení vzdálenosti mezi vysílačem a přijímačem bude přijímaný signál roven jedné čtvrtině signálu původního.

Absorpce (*absortion*)

Pokud signál narazí na objekt, kterým nemůže proniknout ani se od něj odrazit, nastává absorpce. V tom případě je signál kompletně, či částečně eliminován přeměnou na teplo. (SEXTON, 2012)

Odraz (*reflection*)

Odraz nastává od objektů s mnohem větší velikostí, než jsou rozměry elektromagnetické vlny. Pokud je povrch objektu hladký, může se signál odrazit téměř ve stejné podobě (určitá minimální ztráta a rozptyl nastává vždy). Odraz je jednou z hlavních příčin vzniku vícecestného šíření signálu. (Planet3 Wireless, Inc., 2002, s. 20–21)

Lom (*refraction*)

Lom signálu nastává při jeho průchodu médii s odlišnou hustotou (voda, studený vzduch). Efektem lomu signálu bývá změna směru šíření signálu a zároveň odrazení části signálu zpět. (Planet3 Wireless, Inc., 2002, s. 21)

Difrakce (*diffraction*)

Difrakce bývá někdy zaměňována s lomem signálu, ale jedná se o rozdílnou věc. Difrakce popisuje ohyb signálu okolo nějakého objektu (objektem na rozdíl od lomu neprochází). V závislosti na velikosti a parametrech objektu se může změnit směr šíření signálu, jeho intenzita a za objektem může vzniknout tzv. rádiový stín (místo s nulovou hodnotou signálu). (Planet3 Wireless, Inc., 2002, s. 22)

Rozptyl (*scattering*)

Rozptyl nastává, pokud signál dopadne na objekt, jehož rozměry jsou několikanásobně menší než rozměry vlny signálu. Příkladem takových objektů mohou být různé zubaté povrchy, jako je písek, kamení nebo předměty jako lampy, dopravní značení či městská zeleň. Rozptyl způsobuje mnohonásobný odraz signálu s malými amplitudami jednotlivých odražených signálů. Ty mají na hlavní signál ničivý vliv a mohou způsobit jeho úplnou eliminaci. (Planet3 Wireless, Inc., 2002, s. 23)

Vícecestné šíření signálu (*multipath*)

Vícecestné šíření signálu je definováno jako součet hlavního signálu a všech odražených dílčích signálů způsobenými odrazem, rozptylem nebo lomem signálu. Tyto dílčí signály vznikají tím, jak se signál během svého šíření rozpíná do všech směrů a naráží na různé překážky. Rozdíl mezi dobou přijetí hlavního signálu a posledního odraženého signálu je definován jako zpoždění šíření (*delay spread*).

Vícecestné šíření signálu může mít na výsledný signál čtyři efekty či jejich kombinace. Je to snížení nebo zvýšení amplitudy (v závislosti na tom, jestli je odražený signál mimo nebo ve fázi), poškození signálu nebo jeho úplné vynulování (pokud odražený signál dorazí v opačné fázi). (Planet3 Wireless, Inc., 2002, s. 224–230)

Vícecestné šíření signálu je závislé na prostředí mezi vysílačem a přijímačem. Jejich posunutí byť o pár centimetrů může způsobit drastickou změnu přijímaného signálu. Tohoto efektu využívají zařízení s více anténami (systém tzv. *antenna diversity*).

Parametry použitých antén

Úroveň přijímaného signálu záleží také na typu, orientaci, umístění a polarizaci antén obou účastníků přenosu – vysílače i přijímače (Planet3 Wireless, Inc., 2002, s. 111).

Rušení

Rušení může být způsobeno jinými bezdrátovými sítěmi nebo ostatními zdroji. V zásadě se rozlišují dva typy rušení – úzkopásmové a širokopásmové. Úzkopásmové rušení obvykle pro systémy rozprostřeného spektra nepředstavuje výrazný problém, zařízení si s ním poradí samo, případně stačí změnit kanál, na kterém bezdrátová síť pracuje. Širokopásmové rušení je schopné zarušit celé frekvenční pásmo (například 2,4 GHz) a pro bezdrátovou síť může znamenat velký problém, který nelze snadno vyřešit. V podstatě je možné pouze odstranit zdroj rušení, nebo přejít na bezdrátovou síť na odlišné frekvenci (2,4 / 5 GHz). Vzhledem k faktu, že bezdrátové sítě pracují v nelicencovaném pásmu, se v něm může nacházet poměrně velké množství zdrojů způsobujících rušení. V pásmu 2,4 GHz to může být technologie Bluetooth (bezdrátové myši, klávesnice, telefony), bezdrátová sluchátka nebo i mikrovlnné trouby. Pokud není mikrovlnná trouba dokonale utěsněná, i malý únik signálu bývá v řádech wattů (normální výkon mikrovlnné trouby je okolo 1000 W), což je násobně více než úroveň výkonu bezdrátových sítí.

Pokud je rušení způsobeno přilehlými bezdrátovými sítěmi pracujícími na stejném frekvenčním pásmu 2,4 GHz a používajícími stejnou modulaci OFDM, je možné použít systém opakovaného použití kanálů (*channel reuse*). V něm jsou použity kanály 1, 6 a 11 tak, že shodné kanály spolu nikdy nesousedí, takže spolu neinterferují. (Planet3 Wireless, Inc., 2002, s. 246–248)

Provoz na síti (zahlcení)

Bezdrátové sítě fungují na principu sdíleného média, tedy v jednu chvíli lze data odesílat nebo přijímat. Čím více klientů je připojeno k jedné síti, a čím více se jich snaží komunikovat, tím větší je režie sítě, a tím nižší propustnost.

Cisco (2009) při testování standardu 802.11n naměřilo maximální propustnost 185 Mbps. Pokud však přes síť zkoušeli přenést co nejvyšší počet video streamů, došlo ke snížení propustnosti na 140 Mbps.

2.4.3 Další faktory

Tyto faktory nezapadají do výše uvedených skupin.

Koexistence více standardů (802.11b + 802.11g)

Gast (2005, s. 628) tvrdí, že koexistence standardů 802.11b a g – tzv. *protection mode* způsobí snížení propustnosti i o více než 50%. V provedeném experimentu z roku 2003 porovnával Gast (2003) normální režim s dvěma typy koexistence – ochrana CTS-to-self a ochrana RTS/CTS. Při normálním režimu byla propustnost 27,3 Mbps, při režimu CTS-to-self klesla na 13 Mbps a při RTS/CTS na pouhých 8,8 Mbps. Takto drastické snížení propustnosti je zapříčiněno způsobem fungování ochrany, kdy před odesláním paketu rychlostí standardu g je nutné nejprve odeslat kontrolní rámce (CTS, respektive RTS+CTS), které musejí být odeslány rychlostí srozumitelnou pro všechny klienty (pro 802.11b je to maximálně 11 Mbps). (GAST, 2003)

Velikost vyrovnávací paměti

Lo (2007, s. 23) zmiňuje určitý vliv velikosti vyrovnávací paměti (*buffer*) zařízení na propustnost. Pokud je tato paměť malá a dojde k jejímu zaplnění, další pakety budou zahozeny, což sníží propustnost. Vhodná velikost vyrovnávací paměti u sítí typu 802.11b by měla být mezi 64–128 KB (JIN Z. a další, 2003 cit. podle LO, 2007, s. 23).

Šifrování

Leutert (2009) uvádí, že použitím WPA2 šifrování ve standardu 802.11n s propustností okolo 100 Mbps dojde k jejímu snížení o 5–15 %.

3 Experimentální metody měření propustnosti bezdrátových sítí

V této kapitole budou podrobněji rozebrány existující experimentální metody měření propustnosti bezdrátových sítí, které byly stručně představeny v první kapitole. Autoři těchto metod byli popsáni v první kapitole, a proto zde nebudou dále uváděni.

3.1 Metoda šíření signálu

Metodika měření byla rozdělena na dvě hlavní části – úvodní měření a hlavní měření.

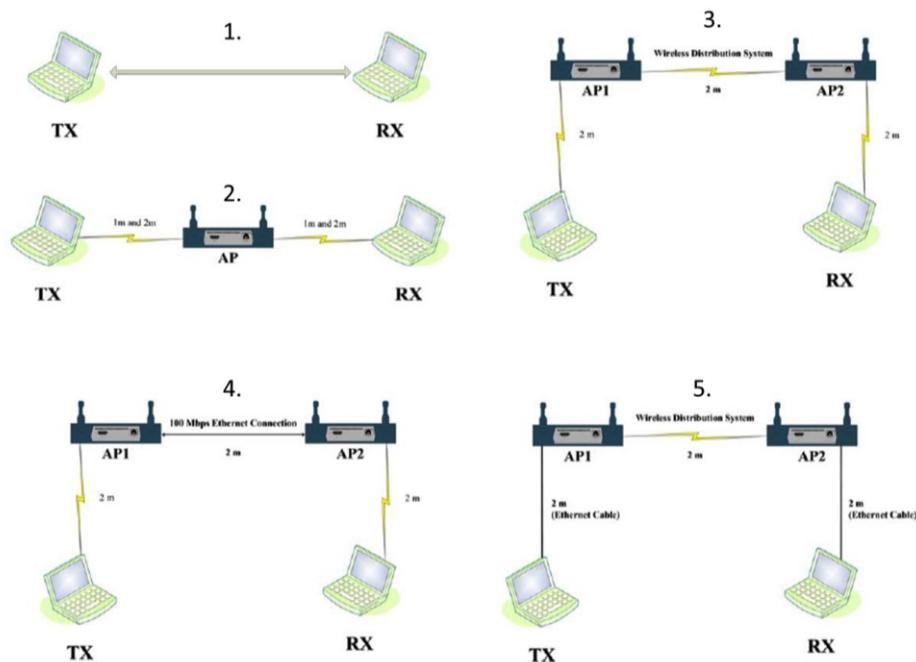
Úvodní měření

Při úvodním měření byla pomocí šesti různých scénářů získána vzorová data pro porovnání s hlavním měřením. Toto měření probíhalo v relativně kontrolovaném prostředí (zasedací místnost) při minimálních vzdálenostech mezi klientem a přístupovým bodem. Antény zařízení uvedených v experimentech byly vždy umístěny metr nad zemí pro zabránění efektů spojených s Fresnelovou zónou⁴. Měření bylo provedeno při následujících scénářích:

- 1) Ad-hoc měření mezi dvěma notebooky, při vzdálenostech 1, 2 a 3 metrů,
- 2) AP a k němu bezdrátově připojeny dva notebooky ve vzdálenostech 1 a 2 metrů,
- 3) dva bezdrátově spojené AP a ke každému navíc bezdrátově připojen jeden klient, všechny vzdálenosti 2 metry,
- 4) stejný scénář jako 3. jen AP jsou propojeny Ethernetovým kabelem (100Mbps, 2 metry),
- 5) stejný scénář jako 3. jen klienti jsou k přístupovým bodům připojeni kabelem.

Grafické znázornění jednotlivých scénářů je na následujícím obrázku.

⁴ Fresnelova zóna je elipsovitá oblast mezi vysílačem a přijímačem. Pokud se v ní nacházejí objekty blokuji komunikaci, dochází ke snižování úrovně signálu. (Planet3 Wireless, Inc., 2002, s. 26) Při výšce umístění antén 1 metr nad zemí, se Fresnelova zóna dotkne země až při vzdálenosti antén mezi sebou 33 metrů, což je pro experiment dostatečné.



Obrázek 8 – Schémata jednotlivých scénářů

Zdroj: (LO, 2007)

Lo zmiňuje, že stěžejní experimenty pro pochopení vztahu mezi velikostí a formátem souboru, vzdáleností, kvalitě signálu a propustností byly experimenty 2–5. Měření probíhala pro různé typy souborů a velikostí.

Následující tabulka zobrazuje naměřené hodnoty z uvedených scénářů (označeny číslem 1–5) pro různé typy souborů.

Tabulka 2 – Porovnání propustností v závislosti na měřeném scénáři

Experiment č.	1. (Mbps)	2. (Mbps)	3. (Mbps)	4. (Mbps)	5. (Mbps)
RSS (dBm)	–47	–43	–43	–43	N/A
Data 109 MB	8,149	10,461	5,793	11,152	18,794
Data 274 MB	8,079	10,306	5,733	12,036	19,264
Audio 263 MB	8,150	10,425	5,717	12,507	19,465
Video 256 MB	8,252	10,236	5,778	11,755	19,603
Průměr	8,157	10,357	5,755	11,863	19,281

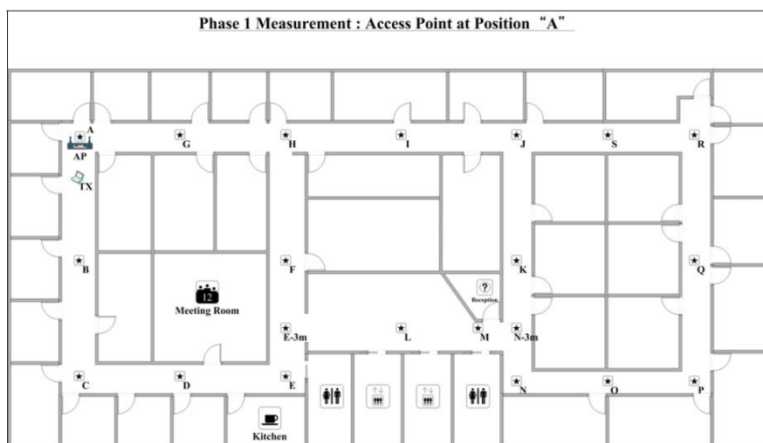
Zdroj: (LO, 2007)

Z uvedených dat je patrné, že propustnost je nejvíce ovlivněna počtem přenosů (skoků) přes bezdrátový přenos. Při jednom bezdrátovém přenosu je tak propustnost téměř 20 Mbps, pokud je však do cesty přidán další bezdrátový spoj, propustnost klesne o polovinu na 10 Mbps. S dalšími spoji propustnost dále klesá. Experiment číslo čtyři vykazuje oproti druhému o něco vyšší propustnost způsobenou využitím jiného kanálu na jednom z AP, takže se bezdrátové spoje neruší. První scénář vykazuje velice nízkou propustnost kvůli faktu, že zvolené WLAN adaptéry v noteboocích podporovaly v režimu ad-hoc pouze standard 802.11b, který má maximální rychlost přenosu dat 11 Mbps.

Hlavní měření

Při hlavním měření bylo zkoumáno pokrytí signálu reálného prostředí při různých umístěních přístupových bodů a jejich konfigurací (někdy byl přítomný pouze jeden AP). Notebook, který měřil kvalitu signálu, byl přesouván na vozíku na předem definovaná místa v různých vzdálenostech. Druhý notebook byl umístěn v pevné vzdálenosti dvou metrů od přístupového bodu a byl také připojen bezdrátově. To odpovídá druhému scénáři v úvodním měření, pouze je prováděno v jiných vzdálenostech a v reálném prostředí. Toto řešení se podstatně liší od ostatních metodologií, které jsou většinou založené jen na jednom bezdrátovém přenosu. Naměřená propustnost v této metodologii tak bude méně než poloviční, tedy podobná jako by v ostatních metodologiích o médium soupeřili dva klienti.

Schéma budovy, kde bylo měření prováděno a rozvržení jednotlivých měřených bodů je znázorněno na následujícím obrázku (jedná se o první scénář hlavního měření, kde byl umístěn pouze jeden AP na lokaci A).



Obrázek 9 – Měření propustnosti v experimentálním prostředí

Zdroj: (LO, 2007)

Výsledky hlavního měření jsou kompletně závislé na prostředí, ve kterém se odehrává, a proto nejsou vhodné pro jakékoliv porovnávání metod. Maximální propustnost při minimální vzdálenosti dosahovala hodnoty okolo 10 Mbps.

Způsob měření

Jak již bylo zmíněno v první kapitole, propustnost je prostě vypočítána jako velikost souboru dělená časem nutným pro přenos dat, který byl změřen stopkami. Tento způsob není úplně přesný, a lze tak předpokládat určitou chybu měření.

Pro zpřesnění výsledků byla provedena tři následující opatření. Pro minimalizaci vlivu pohybujících se osob na kvalitu signálu bylo měření prováděno o víkendech, kdy v kancelářích nikdo nebyl (během pracovních dnů se v prostorech pohybuje více než třicet zaměstnanců). Vliv rušení ostatními sítěmi byl vyloučen použitím techniky skenování vždy

před provedením experimentu (v dosahu bylo možné nalézt 3–5 vysílajících AP). Posledním opatřením bylo nastavení parametrů AP tak, aby byl minimalizován jeho vliv na měření. Tedy veškeré funkce ovlivňující výkon (např. šifrování) byly vypnuty.

Implementační detaily metodiky

Použitý hardware:

- AP: D-link, DWL-2100AP, 802.11g,
- notebook 1: IBM, X31, 1,7 GHz CPU, 1GB RAM,
- notebook 2: Toshiba, Celeron 2,4 GHz CPU, 512MB RAM,
- USB Wireless Adapter: D-link, DWL-G132, 802.11 b/g,
- 2,4GHz Antenna: D-link, ANT24-0700, 802.11 b/g, 2,4–2,5 GHz.

Použitý software:

- Microsoft Windows XP, Service Pack 2,
- Colligo Workgroup Edition v. 4.0,
- WirelessMon Profession Edition v. 2.0 (1010).

Nastavení AP:

- Šifrování: zakázáno, autentifikace: otevřený systém,
- QoS (WMM): zakázán, SSID broadcast: povoleno,
- kanál: 1 (V případě dvou AP je druhé AP nastaveno na odlišný kanál, bohužel Lo nezmiňuje, který přesně je použit. Pro minimalizování vzájemného rušení lze však předpokládat například jedenáctý).

Závěry

Maximální naměřená propustnost 802.11g sítě byla okolo 19,6 Mbps při jednom bezdrátovém spoji. Přičemž zvolený formát ani velikost souboru neměly na propustnost téměř žádný vliv. Je však nutno podotknout, že toto tvrzení platí v případě volby dostatečně velkých souborů, pokud by byly přenášeny malé soubory, propustnost by to značně snížilo. Metodika měření propustnosti využívá pro měření času přenosu stopky ovládané uživatelem. Tento způsob měření obsahuje určitou nepřesnost způsobenou zpožděnou reakcí člověka i odezvou OS – ten může začít přenášet soubor dříve, než zobrazí grafickou animaci ukazující úroveň přenosu. Dalším problémem je nevyužití specializovaného nástroje pro měření propustnosti, který by zaručoval maximální možné využití všech dostupných prostředků. V tomto případě je tak možné, že OS nepřihradí přenosu maximální prioritu a může tak docházet ke zkreslení výsledků.

V práci byl dále zkoumán vliv RSS na propustnost, který byl potvrzen. Dostatečná hodnota RSS však negarantuje dostatečnou propustnost. Ta totiž závisí i na dalších faktorech, jako je vzdálenost, počet zdí či jiných překážek mezi klientem a AP nebo pozicí AP. (LO, 2007, s. 78,92)

SWOT analýza metodiky

<p>Silné stránky</p> <ul style="list-style-type: none"> • Velký počet provedených scénářů. • Nenáročnost na software (v případě měření propustnosti postačí služba poskytovaná téměř jakýmkoliv operačním systémem). • Uvažování vlivu Fresnelovy zóny na propustnost a její eliminace. • Měření přenášením více druhů souborů různých velikostí. 	<p>Slabé stránky</p> <ul style="list-style-type: none"> • Nepřesnost měření vzniklá použitím stopek. • Nepřesnost měření vzniklá nepoužitím specializovaného SW nástroje pro měření propustnosti. • V metodice chybí klasický scénář, kde je jeden notebook připojen k AP pomocí kabelu.
<p>Příležitosti</p> <ul style="list-style-type: none"> • SWOT analýza neodhalila žádné zvláštní příležitosti metodiky. 	<p>Hrozby</p> <ul style="list-style-type: none"> • Vysoká možnost ovlivnění měření externími faktory (rušení pocházející z ostatních bezdrátových sítí).

3.2 Měření propustnosti metodou „packet-by-packet“

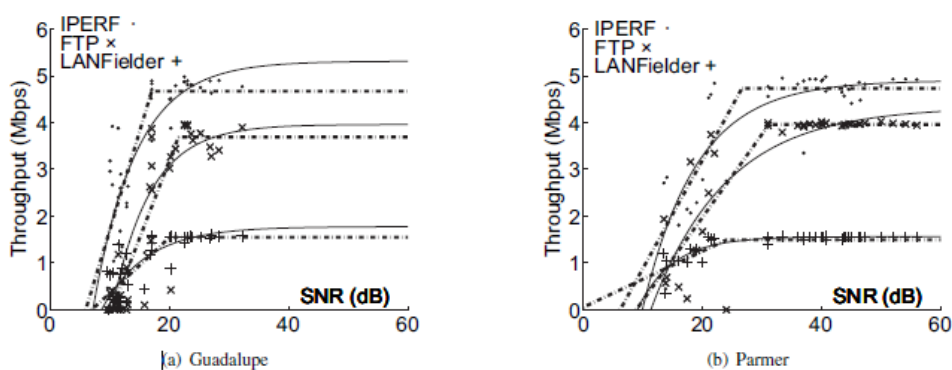
Způsob měření a výsledky

Měření bylo rozděleno na dvě části. Část zabývající se analýzou uživatelských dat zde dále nebude popisována. Část měřící propustnost reprezentuje téměř typické zapojení experimentálního měření, kde je jeden klient připojen k AP bezdrátově a druhý kabelem. V tomto případě je však mezi statickým klientem a AP přítomný ještě rozbočovač, což by v určitých případech mohlo vést k určitému zkreslení výsledků. Naproti tomu pro zvýšení přesnosti měření propustnosti byly použity tři různé softwarové nástroje.

Aplikace přenášely soubory o velikosti 300 KB v podmínkách s malým SNR a 3 MB v podmínkách s velkým SNR. Velikosti byly voleny tak, aby přenos souboru trval přibližně deset sekund. V každé restauraci bylo naměřeno 264 datových souborů (11 lokací, 2 WNIC, 3 aplikace pro měření propustnosti a umístění na 4 světové strany).

Jak autoři zmiňují, experiment byl zaměřen na zkoumání vztahu mezi propustností na aplikační vrstvě a hodnotě SNR. Následná analýza provedená empirickými modely (zmíněná v první kapitole) zde nebude dále rozebírána, protože se netýká experimentálního měření propustnosti.

Naměřené hodnoty ze dvou restaurací zobrazují následující grafy.



Obrázek 10 – Naměřené propustnosti v závislosti na hodnotě SNR

Zdroj: (NA, CHEN A RAPPAPORT, 2006)

Implementační detaily metodiky

Použitý hardware:

- AP: Colubris Networks CN-3000, 802.11b,
- notebook 1: Compaq Evo N600c, Debian Linux 3.0,
- notebook 2: Dell Latitude C640,
- rozbočovač: Netgear DS-104 Ethernet,
- PCMCIA WNIC 1: Cisco Aironet 350,
- PCMCIA WNIC 2: ORiNOCO Gold.

Použitý software:

- LANFielder 7.0.2,
- Iperf 1.7.0,
- Wget (FTP klient),
- Netstumbler 0.3.30.

Závěry

V této metodě jsou na rozdíl od metody šíření signálu využity sofistikované nástroje pro měření propustnosti. Propustnost je vypočítána průměrem z velkého počtu měření a možnost ovlivnění výsledků externími faktory je tak mnohem menší. Měření bylo také prováděno mimo normální provozní hodiny, takže by nemělo být přítomno zkreslení měření vlivem uživatelů. Vzhledem k použití staršího standardu 802.11b, který má mnohem nižší přenosové rychlosti, nemá smysl porovnávat výsledky s předchozí metodou.

Největší hrozbou této metodiky jsou malé velikosti přenášených souborů. Jain a Dovrolis (2003, s. 11) se v jejich experimentu věnovali vlivu krátkého přenosu dat TCP protokolem a došli k závěru, že pouze několika sekundový přenos dat způsobuje v propustnosti výrazné rozdíly, a to od stovek Kbps až po 6 Mbps. Pro získání přesných výsledků použili Jain a Dovrolis pěti minutové intervaly měření, které poskytují dostatek prostoru pro ustálení TCP protokolu. Druhé riziko zkreslení výsledků představuje připojení experimentální sítě k internetu, které může způsobit přenos nechtěných dat (například stahování automatických aktualizací).

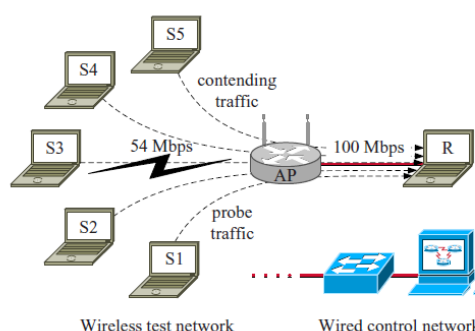
SWOT analýza metodiky

<p>Silné stránky</p> <ul style="list-style-type: none"> • Vysoká přesnost metody daná velkým množstvím prověřovaných parametrů (4x orientace klienta, 2x WNIC, 3x použité softwarové nástroje s odlišným nastavením). • Rychlé provedení jednoho experimentu (malá velikost přenášených souborů). 	<p>Slabé stránky</p> <ul style="list-style-type: none"> • Připojení statického klienta přes rozbočovač místo přímého připojení k AP. • Přístupový bod byl během měření připojen k internetu.
<p>Příležitosti</p> <ul style="list-style-type: none"> • Nízká možnost ovlivnění experimentu externími faktory. 	<p>Hrozby</p> <ul style="list-style-type: none"> • Riziko zkreslení výsledků náhodným přenosem dat z internetu způsobeným určitým procesem. • Možná nepřesnost měření vlivem malé velikosti přenášených souborů vedoucí k neustálení TCP protokolu.

3.3 Metody měření dostupné kapacity

Způsob měření

Experimentální měření bylo prováděno ve stíněné komoře, pokryté materiálem absorbujícím odrazy. V komoře bylo umístěno několik notebooků (v závislosti na prováděném experimentu) a AP podle následujícího schématu.



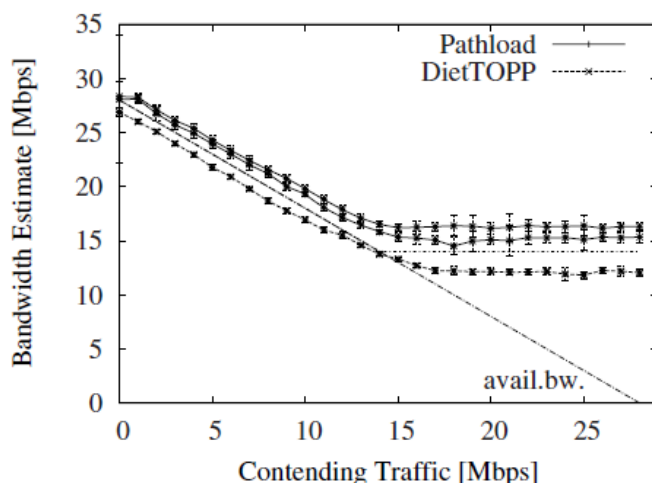
Obrázek 11 – Schéma měření dostupné kapacity

Zdroj: (BREDEL a FIDLER, 2008, s. 319)

Vzdálenost mezi klienty a přístupovým bodem se pohybovala mezi 0,5 a 1,5 metru. Každý experiment byl spuštěn 25x a byl vypočítán průměr ze všech naměřených hodnot (interval spolehlivosti 0,95). Měření bylo provedeno sedmi nástroji pro měření dostupné kapacity. Vzhledem k problémům pasivních metod byly vybrány pouze nástroje měřící aktivní metodou měření. Čtyři nástroje dále měřily iterativním způsobem a tři přímým.

1) Iterativní metody

Experiment byl proveden s následujícími nástroji měřícími iterativním způsobem: *Pathload*, *Pathchirp*, *PTR*, *DietTOPP*. Při defaultním nastavení však tyto metody selhávají. Tento úkaz lze opravit nastavením pevné velikosti paketů na hodnotu 1500 bajtů. I přes toto opatření však *PTR* ani *Patchirp* nepodávají přesné výsledky a nejsou proto příliš vhodné pro měření dostupné kapacity bezdrátových sítí. Naopak *Pathload* a *DietTOPP* vykazují přesné výsledky, dokud provoz na spoji nepřesáhne polovinu celkové kapacity. Dostupná kapacita je pak totiž funkcí DCF rozdělena symetricky a nástroje tak zobrazují dostupnou kapacitu rovnou zhruba polovině kapacity celkové, což zobrazuje následující graf.



Obrázek 12 – Dostupná kapacita naměřená iterativními metodami

Zdroj: (BREDEL a FIDLER, 2008, s. 322)

2) Přímé metody

Z nepřímých metod byly prověřeny tyto nástroje: *Spruce*, *IGI* a *WBest*. Protože tyto metody vyžadují počáteční znalost kapacity, byly nastaveny pro kapacitu spoje $C = 28$ Mbps (zvoleno s ohledem na naměřenou propustnost pro velikost paketu 1500 bajtů). Z provedených experimentů se však nepodařilo určit trend. Tyto metody byly nepřesné, a proto jejich výsledky nejsou vypovídající.

Implementační detaily metodiky

Použitý hardware:

- Notebooky: Lenovo ThinkPad R61, 1,6 GHz CPU, 2 GB RAM,
- WLAN adapter (interní): Intel PRO/Wireless 4965 AG, 802.11g.

Použitý software:

- OS: Ubuntu Linux 7.10, kernel version 2.6.22.

Nastavení AP:

- RTS/CTS: vypnuto, Fragmentace: vypnuta,
- Medium Access: DCF.

Závěry

Měření propustnosti bezdrátové sítě lze provést technikou měření dostupné kapacity při dodržení následujících podmínek. K měření musí být použity nástroje využívající aktivní a iterativní metody, přičemž nej přesnějších výsledků lze dosáhnout použitím nástrojů *Pathload* nebo *DietTOPP*. Tyto metody musí být nastaveny s pevnou velikostí paketů na hodnotu 1500 bajtů. Posledním požadavkem je nulový provoz dat na bezdrátové síti, tzn. všechna volná kapacita bude dostupná pro měřicí nástroje.

SWOT analýza metodiky

Silné stránky	Slabé stránky
<ul style="list-style-type: none">• Přesné výsledky metody, zaručené:<ul style="list-style-type: none">○ použitím sedmi sw nástrojů z nichž dva poskytují přesné výsledky,○ průměrem z 25 měření,○ měřením ve stíněné komoře.	<ul style="list-style-type: none">• Komplexnost měření a nižší přesnost v porovnání s metodami měření propustnosti.• Nutné správné nastavení měřicích nástrojů a dodržení přesných požadavků metodiky.• Měření pouze uvnitř stíněné komory nereflextuje reálné prostředí.
Příležitosti	Hrozby
<ul style="list-style-type: none">• Měření uvnitř stíněné komory zaručuje přesné výsledky bez jakéhokoliv zkreslení vlivem rušení.• Možnost provedení experimentu vně stíněné komory.	<ul style="list-style-type: none">• Nezminěna přítomnost generátoru šumu ve stíněné komoře.

Další způsoby měření dostupné kapacity

Uvedený způsob měření popisuje experiment, který provedli Bredel a Fidler. Existují i další způsoby měření, jedním z nich je první testování nástroje *DietTOPP* provedený jeho

tvůrci: Johnsson, Melander a Björkman (2006). Experiment byl prováděn v mnohem komplikovanější síťové topologii (6 počítačů a 3 směrovače) a na síti 802.11b. Experiment porovnával výsledky naměřené nástrojem *DietTOPP* s prověřeným a oblíbeným *Pathload* a dokázal, že jejich výsledky jsou porovnatelné. Dále byl zkoumán vliv velikosti dotazovacích paketů na dostupnou kapacitu. Při snížení velikosti paketu z 1500 na 250 bajtů došlo ke snížení dostupné kapacity zhruba o dvě třetiny (z 6 Mbps na 2 Mbps, respektive z 2,3 Mbps na méně než 1 Mbps při přítomném provozu). Na dostupnou kapacitu měl v neposlední řadě vliv rozložení paketů simulujících probíhající provoz (exponenciální a Paretovo rozložení přineslo větší rozptyl v dostupné propustnosti než rovnoměrné rozložení).

3.4 Měření vlivu rádiového rušení na propustnost

Způsob měření

Celkem byly provedeny tři různé experimenty pro ověření vlivu rušení zařízení pracujících na stejné frekvenci jako WLAN (2,4 GHz).

1) Mikrovlnná trouba

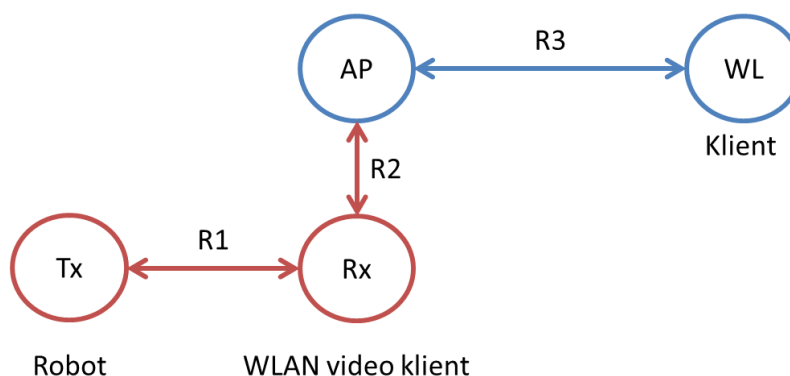
Mikrovlnná trouba byla umístěna v pevné vzdálenosti pěti metrů od přístupového bodu. Klient byl od přístupového bodu vzdálen 35 metrů.

2) PLS systém

Jednotlivé komponenty komunikující na frekvenci 2,4 GHz PLS systému byly umístěny ve vzdálenosti 5–30 metrů od AP. Klient byl od přístupového bodu vzdálen 15 metrů. Pro měření frekvenčního spektra byl navíc ve vzdálenosti pěti metrů od AP umístěn spektrální analyzátor.

3) Robot

Experiment s bezdrátovým robotem byl zkoumán pro různé vzdálenosti mezi všemi zařízeními. Tyto vzdálenosti jsou označeny R1–R3 na následujícím diagramu.



Obrázek 13 – Experiment měření vlivu rušení bezdrátového robota na WLAN

Zdroj: zpracováno dle (PARK a další, 2003)

Vzdálenosti, při kterých nedošlo k úplnému zarušení přenosového pásma, byly shrnuty ve dvou experimentech:

- Experiment 1: R1 = 100 m, R2 = 5 m, R3 = 57 m,
- experiment 2: R1 = 100 m, R2 = 5 m, R3 = 17 m.

Propustnost však nebyla měřena na všech kanálech, ale pouze na kanálech 7–11 pro první experiment, respektive 9–11 pro druhý.

Naměřené hodnoty propustnosti z jednotlivých experimentů jsou zobrazeny v následující tabulce. U kanálů, které nebyly pro daný experiment měřeny, je uvedena pomlčka.

Tabulka 3 – Naměřené výsledky propustnosti

Všechny hodnoty propustnosti uvedeny v Mbps

Číslo kanálu	Bez rušení	Mikrovlnná trouba*	PLS systém	Robot experiment 1	Robot experiment 2
1	4,692	4,2	0,117	-	-
2	4,703	3,6	0,029	-	-
3	4,541	2,8	0	-	-
4	2,286	2,75	0	-	-
5	2,798	2,1	0	-	-
6	4,708	2,6	0	-	-
7	4,577	0,4	0	3,283	-
8	4,669	0	0	3,087	-
9	3,453	0	0,042	0	4,479
10	4,627	0,75	2,221	0	3,905
11	4,635	1	4,076	0	4,166
12	-	1,8	-	-	-
13	-	2,7	-	-	-

* Tyto hodnoty jsou přibližné, jelikož byly odečteny z grafu.

Zdroj: zpracováno dle (PARK a další, 2003)

Implementační detaily metodiky

Autoři této metodiky bohužel nezmiňují konkrétní detaily o použitém hardwaru ani softwaru. Z naměřených hodnot propustnosti lze odhadovat použití standardu 802.11b. Zajímavé jsou vzdálenosti, při kterých byla propustnost měřena (až 57 metrů). To zřejmě odpovídá letištní hale s přímou viditelností mezi AP a klientem.

Závěry

Zařízení pracující na stejných frekvencích, na kterých pracují bezdrátové sítě, významně ovlivňují jejich výkon, a při návrhu sítě je tak potřeba s tímto zjištěním počítat.

SWOT analýza metodiky

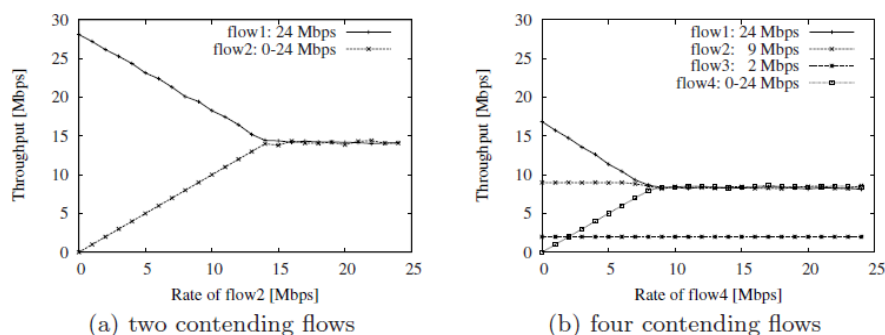
<p>Silné stránky</p> <ul style="list-style-type: none"> Uvedení všech kanálů při měření rušení způsobeném mikrovlnnou troubou. 	<p>Slabé stránky</p> <ul style="list-style-type: none"> Metodika vyžaduje použití specifického hardware. Měření nebylo provedeno na všech kanálech. Neznámá detailní metodika měření propustnosti.
<p>Příležitosti</p> <ul style="list-style-type: none"> SWOT analýza neodhalila žádné zvláštní příležitosti metodiky. 	<p>Hrozby</p> <ul style="list-style-type: none"> Značná závislost změřené propustnosti na použitém HW způsobujícím rušení.

3.5 Měření propustnosti více toků

Způsob měření a výsledky

Jedná se o modifikaci metody pro měření dostupné kapacity. Tento experiment byl proveden stejnými autory za použití stejných iterativních metod popsanych v podkapitole 3.3. Měření bylo provedeno na síti standardu 802.11g, kde klienti generovali datové toky různých rychlostí. Pro toto generování byl použit nástroj *Rude/Crude*. Všechny pakety měly stejnou velikost 1500 bajtů. Propustnost byla vypočítána jako průměr z měření trvajícího jednu minutu.

Následující grafy dokazují rovnoměrné rozprostření propustnosti pro všechny toky. V prvním grafu jsou dva toky, kdy druhému je postupně zvyšován tok dat až do hodnoty 28 Mbps. V tom případě dojde k rovnoměrnému rozdělení propustnosti pro oba toky (14 Mbps). Druhý příklad zkoumá 4 klienty, každý s jiným datovým tokem. Opět je dosaženo férového rozdělení (klient 3 posílá data pouze rychlostí 2 Mbps a nevyžaduje vyšší propustnost).



Obrázek 14 – Grafy rozložení propustnosti pro více klientů

Zdroj: (BREDEL a FIDLER, 2008, s. 320)

Implementační detaily metodiky

Metodika používá stejné zapojení, hardware a software jako metodika popsaná v podkapitole 3.3.

Závěry

Mechanismus DCF systému CSMA/CA by měl zaručovat rovnoměrné rozprostření kapacity sdíleného média všem klientům. Bredel a Fidler (2008) však také uvádějí zdroj⁵ ukazující na určitou krátkodobou neférovost DCF, nicméně tato chyba by se měla týkat jen některých starých WaveLAN karet.

SWOT analýza metodiky

Silné stránky <ul style="list-style-type: none">• Přesné výsledky (minutový přenos dat).• Měření uvnitř stíněné komory zaručuje přesné výsledky bez jakéhokoliv zkreslení vlivem rušení.	Slabé stránky <ul style="list-style-type: none">• Při nastavení nekonstantní velikosti paketů se metoda stává nepoužitelnou.• Při nastavení nižší velikosti paketu než 1500 bajtů může metoda ukazovat zkreslené výsledky.• Měření pouze uvnitř stíněné komory nereflektuje reálné prostředí.
Příležitosti <ul style="list-style-type: none">• Měření uvnitř stíněné komory zaručuje přesné výsledky bez jakéhokoliv zkreslení vlivem rušení.• Možnost provedení experimentu vně stíněné komory.	Hrozby <ul style="list-style-type: none">• Při použití starých WaveLAN karet může metoda vlivem neférovosti implementované DCF selhat.• Nezminěna přítomnost generátoru šumu ve stíněné komoře.

⁵ Berger-Sabbatel, G., Duda, A., Heusse, M., Rousseau, F.: Short-term fairness of 802.11 networks with several hosts. In: Proc. of IFIP MWCN, Říjen 2004, s. 263–274 (2004)

3.6 Přehled nástrojů pro měření výkonnostních parametrů WLAN

Následující tabulka uvádí existující nástroje pro měření výkonnostních parametrů bezdrátových sítí. Dále jsou uvedeny podporované platformy, jakou veličinu daný nástroj měří a jakým způsobem.

Tabulka 4 – Přehled nástrojů pro měření výkonnostních parametrů WLAN

Nástroj	Platforma	Co měří	Způsob měření
Patchar	Unix	Kapacitu	Proměnná velikost paketu
Clink	Linux	Kapacitu	Proměnná velikost paketu
Pchar	Unix	Kapacitu	Proměnná velikost paketu
Bprobe	IRIX	Kapacitu (E2E)	Párové pakety
Pathrate	Linux	Kapacitu (E2E)	Párové a vláčkové pakety
Sprobe	Linux	Kapacitu (E2E)	Párové pakety
Cprobe	IRIX	Dostupnou kapacitu	Vláčkové pakety
DietTOPP	Unix	Dostupnou kapacitu	Vláčkové pakety, iterativní
Pathload	Linux	Dostupnou kapacitu	Samovyvažovací periodické streamy
IGI	Linux	Dostupnou kapacitu	Samovyvažovací periodické streamy, přímá
Pathchirp	Unix	Dostupnou kapacitu	Packet chirps, iterativní
PTR	Linux	Dostupnou kapacitu	Vláčkové pakety, iterativní
Spruce	Linux	Dostupnou kapacitu	Párové pakety, přímá
WBest	Linux	Dostupnou kapacitu	Vláčkové pakety, přímá
Ttcp	Win, Unix	Propustnost	TCP spojení
Iperf	Win, Unix	Propustnost	Paralelní TCP spojení
Netperf	Win, Unix	Propustnost	Paralelní TCP spojení

Zdroj: zpracováno dle (PRASAD a další, 2003, s. 34; CAIDA, 2014)

Pro testování propustnosti je v dnešní době vhodný zejména nástroj *Iperf*, respektive jeho grafická nadstavba *Jperf*. Jedná se o open source nástroj, který je multiplatformní, a lze tak měřit propustnost i napříč různými operačními systémy (Windows, Linux, Android). Mezi jeho další přednosti patří možnost volby transportního protokolu (TCP/UDP), schopnost simulace provozu více klientů (více TCP spojení), duální přenos dat a široké možnosti nastavení parametrů přenosu. *Iperf* kromě propustnosti měří i zpoždění a počet ztracených paketů. (IPERF, 2011)

4 Metodika pro měření propustnosti

Tato kapitola se věnuje návrhu a popisu nové metodiky. Nejprve je popsán postup navržení metodiky následován jejím popisem včetně návodů na zprovoznění vyžadovaného SW vybavení.

4.1 Návrh nové metodiky

Nejprve byl vytvořen teoretický model maximální propustnosti, který později mohl být porovnán s naměřenými hodnotami. Dále byla provedena analýza nedostatků zmíněných metod pro měření propustnosti a dostupné kapacity, na jejímž základě byly určeny stěžejní vlastnosti, které by nová metodika měla obsahovat. Podle určených vlastností byl zvolen vhodný software a hardware, kterým mohly být ověřeny určité zmíněné předpoklady ostatních metod. Ověření těchto předpokladů bylo stěžejní částí práce a detailní popis metodiky byl vytvořen podle jejich výsledků.

4.1.1 Model teoretické maximální propustnosti bezdrátové sítě

Vytvoření matematického modelu maximální teoretické propustnosti sítě bylo důležité pro porovnání s reálně naměřenými hodnotami. Model zobrazuje dosažitelnou propustnost sítě standardu 802.11g v ideálních podmínkách bez přítomnosti rušení, při nulové ztrátě paketů, se zakázanou fragmentací, použití módu DCF a předpokladu, že odesílající stanice má vždy připravena data, která chce odeslat. Jun, Peddabachagari a Sichitiu (2003, s. 2) tuto veličinu za uvedených podmínek označují jako TMT (*theoretical maximum throughput*). Propustnost je uvedena pro jednotlivé velikosti paketů a různé modulace. Podrobná data, ze kterých jsou grafy vytvořeny, lze nalézt v příloze A. Více informací o všech parametrech lze nalézt v příspěvku „*The Theoretical Maximum Throughput Calculation for the IEEE 802.11g Standard*“ (BARBOSA, CAETANO a BORDIM, 2011).

Výpočet teoretické maximální hodnoty propustnosti (*Maximum Throughput*) je proveden podle následujícího vzorce (BARBOSA, CAETANO a BORDIM, 2011):

$$MT = \frac{MS_{Size}}{T_{SIFS} + T_{DIFS} + T_{ACK} + T_{BO} + T_{Data}}$$

Kde T_{Data} je vypočítán jako (BARBOSA, CAETANO a BORDIM, 2011):

$$T_{Data} = T_{PHY_Header} + \left(T_{Sym} \frac{L}{N_{DBPS}} \right)$$

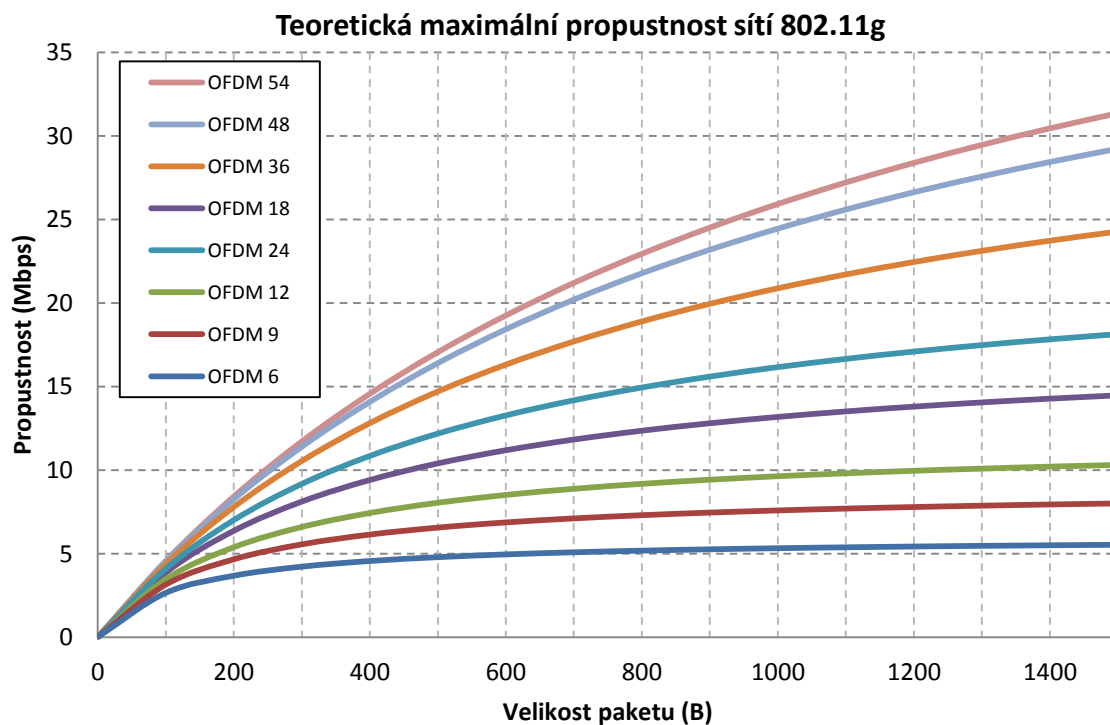
Popis a typické hodnoty jednotlivých parametrů ukazuje následující tabulka.

Tabulka 5 – Parametry pro výpočet teoretické propustnosti

Parametr	Popis	Typická hodnota (OFDM 54)
MS_{Size}	Velikost rámce v bitech	1500*8 bitů
T_{SIFS}	Short interframe space interval	16 μs
T_{DIFS}	DCF interframe space interval	34 μs
T_{ACK}	Doba pro odeslání potvrzovacího rámce (<i>acknowledgement</i>)	22,52 μs
T_{BO}	Hodnota náhodné čekací doby (<i>backoff</i>) zvolena jako polovina z možného intervalu	67,5 μs
T_{DATA}	Čas strávený vysláním rámce	2,024 ms
$T_{PHY\ Header}$	Doba trvání záhlaví fyzické vrstvy dat (<i>preamble+signal</i>)	20 μs
T_{Sym}	OFDM interval symbolu	4 μs
N_{DBPS}	Počet bitů na jeden symbol v OFDM	216 bitů
L	Velikost rámce v bitech včetně záhlaví ($MS_{Size} + 16 + 6$)	1500*8+22 bitů

Zdroj: zpracováno dle (BARBOSA, CAETANO a BORDIM, 2011; IEEE Std 802.11™, 2012)

Následující graf ilustruje teoretickou maximální propustnost sítě 802.11g při velikostech paketů 0–1500 bajtů a při všech modulacích podporovaných standardem 802.11g. Naměřené výsledky ukazují teoretickou maximální propustnost okolo 31 Mbps.



Obrázek 15 – Vliv velikosti paketu na teoretickou propustnost sítě 802.11g

Zdroj: vlastní výpočty

4.1.2 Shrnutí nedostatků zmíněných metod

Následující seznam shrnuje nedostatky uvedených metod, které byly zachyceny SWOT analýzou a podrobněji popsány ve třetí kapitole. Tyto nedostatky mohou způsobit snížení přesnosti měření, případně zanedbávají určité faktory měření propustnosti:

- Použití stopek pro měření času přenosu (zpoždění GUI OS, reakce člověka),
- nepoužití specializovaného SW pro měření propustnosti,
- přenos přes více bezdrátových spojů,
- připojení statického klienta k AP přes rozbočovač,
- připojení experimentální sítě k internetu,
- malá velikost přenášených souborů (TCP zkreslení),
- při měření vlivu rušení neproveden experiment na všech kanálech.

4.1.3 Analýza nedostatků zmíněných metod

Na základě analýzy zjištěných nedostatků uvedených metod pro měření propustnosti byly navrženy následující vlastnosti, které by nová metodika měla mít:

- Použít klasický scénář zapojení klientů, tedy statického klienta připojit kabelem přímo k AP, dynamického pak připojit k AP bezdrátově. Celou síť nechat oddělenou a nepřipojovat ji k internetu.
- Před prováděním experimentu provést skenování okolních sítí na všech kanálech pro analýzu možného rušení a pro provádění experimentu zvolit nejméně zarušený kanál.
- Pro měření propustnosti využít specializovaný SW. Nepoužívat ruční měření času stopkami a dopočítávání propustnosti podle délky přenosu dat.
- Při měření propustnosti použít dostatečně velké soubory, respektive použít dostatečně dlouhý přenos dat, který umožní ustálení protokolu TCP. Na druhou stranu přenos dat by neměl být zbytečně dlouhý, aby experiment netrval příliš dlouho. Při delší době provádění experimentu se zvyšuje šance změny parametrů rádiového pásma a tím pádem negativního ovlivnění měření. Ideální délka přenosu dat se tak jeví kolem jedné minuty.
- Provést testování na současně nejpoužívanějších standardech, tedy 802.11g nebo 802.11n.

Na základě těchto vlastností mohl být zvolen konkrétní SW a HW popsany dále.

4.1.4 Použitý software

Jako nejvhodnější softwarový nástroj pro měření propustnosti byl vybrán dostupný a široce podporovaný *Iperf* verze 2.0.5-2⁶. Ten je dostupný ve verzi pro Windows i pro Linux, a proto mohl být nasazen na obou těchto platformách. Pro testování propustnosti s využitím mobilních zařízení na platformě Android byl použit port softwaru *Iperf*, který je nazván *iPerf for Android*⁷ (verze 2.06) a je zdarma dostupný.

Pro skenování okolních sítí byl použit *Wifi Analyzer*⁸ (verze 3.6.6) dostupný pro operační systém Android. Lze využít i jiný SW, předností *WiFi Analyzeru* však je interaktivní zobrazení přispívající k rychlé analýze. Ukázkový výstup z tohoto programu je zobrazen v příloze B. Jedná se o stav rádiového pásma před prováděním první části ověřování předpokladů metod pro měření propustnosti.

Jako podobné programy lze použít *inSSIDer* (Windows) nebo *WiFi Radar* (Linux), poslední zmiňovaný však data prezentuje pouze v textovém režimu.

4.1.5 Použitý hardware

Pro měření propustnosti byl využit následující HW (příslušný OS je vždy uveden). Tento HW bude dále označován uvedenými zkratkami.

- AP: LinksysWRT54GL (Firmware: 4.30.15 build 2, Dec. 8, 2010).
- PC_D: Dell Optiplex 360 (Windows 7 Enterprise, 64bit) – CPU Dual-Core E5200 2,5 GHz, 4 GB RAM.
- PC_{LW}: Lenovo Z580 (Windows 8.1, 64bit) – CPU Core i7-3632QM 2,2 GHz, 8 GB RAM.
- PC_{LU}: stejné zařízení jako předchozí, jen s OS: Ubuntu 12.04, 64bit.
- NB: Asus A6Vm (Xubuntu 12.04, 32bit) – CPU Pentium M 735 1,7 GHz, 512 MB RAM.
- N7: tablet Nexus 7 2013 (Android 4.4.2) – CPU Snapdragon S4 Pro 1,5 GHz, 2 GB RAM.
- SP: HTC Evo 3D (Android 4.0.3) – CPU Qualcomm MSM8660 1,5 GHz, 1 GB RAM.

4.1.6 Ověření určitých předpokladů zmíněných metod

Zmíněné metody pro měření propustnosti vycházejí z určitých předpokladů, které mohou výsledné měření ovlivnit, ale v určitých podmínkách se projevit nemusí. Proto bylo pro návrh komplexní a kvalitní metodiky potřeba tyto předpoklady prakticky ověřit a určit, zda

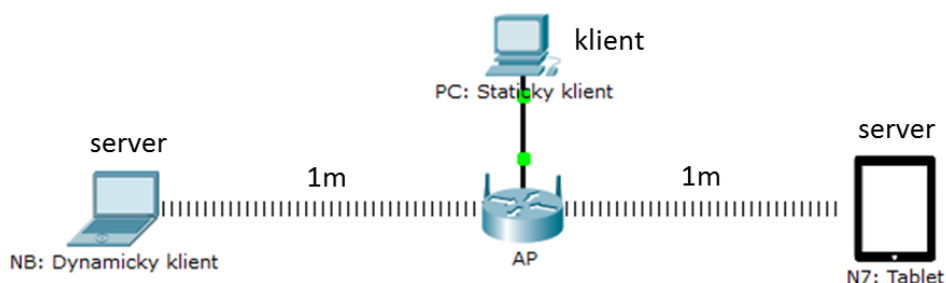
⁶ Dostupný z: <http://iperf.fr/> (cit. 3. 4. 2014)

⁷ Dostupný z: <https://play.google.com/store/apps/details?id=com.magicandroidapps.iperf> (cit. 3. 4. 2014)

⁸ Dostupný z: <https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=cs> (cit. 3. 4. 2014)

se v konkrétních podmínkách projevují a je nutné se jim věnovat, či se neprojevují a mohou se ignorovat.

Měření bylo provedeno podle následujícího schématu v laboratorní místnosti NET101 (kromě posledního experimentu) a jako statický klient byl použit PC_D (pokud neuvedeno jinak), ve výsledcích označován jako PC. Pokud nejsou uvedeny vzdálenosti bezdrátových zařízení, jednalo se o vzdálenost jednoho metru. Experiment byl vždy prováděn na aktuálně nejméně zarušeném kanálu. Evropské kanály (12 a 13) nebyly v této softwaru přístupového bodu dostupné, jednalo se tedy zřejmě o US verzi. Dílčí experimenty mohou ukazovat rozdílné hodnoty propustnosti, to je dáno faktem, že experimenty byly prováděny v různých dnech a v různých časech, což odpovídalo vždy jiným podmínkám rádiového pásma. Důležité je, že v rámci každého experimentu, který byl proveden co nejrychleji, byly podmínky stejné.



Obrázek 16 – Schéma měření ověření předpokladů metod

Zdroj: vlastní

Měření bylo vždy provedeno protokolem TCP po dobu šedesáti sekund. Kvůli proměnlivosti bezdrátového média byly vždy provedeny dva po sobě jdoucí pokusy, a pokud se výsledky lišily o více než o 10%, bylo provedeno nové měření (podrobnosti tohoto opatření budou popsány ve vlastnostech metodiky). Uvedené hodnoty jsou průměrem z těchto dvou měření. Kompletní výsledky lze nalézt v příloze C.

Nastavení klienta (PC) v programu *Iperf*:

```
C:\sw\iperf>iperf -c 192.168.1.102 -i 1 -t 60
-----
Client connecting to 192.168.1.102, TCP port 5001
TCP window size: 64.0 KByte (default)
-----
```

Jako server byl použit NB, respektive N7 a ve dvou experimentech byla tyto zařízení doplněna o SP.

Vliv OS a HW na měření propustnosti

První podmínkou bylo ověřit, zda výkon všech zařízení nemůže ovlivnit měření propustnosti. Proto bylo provedeno měření propustnosti mezi PC_D a třemi zařízeními z různých kategorií – NB v kategorii notebooků, N7 v kategorii tabletů a SP v kategorii chytrých telefonů. Měření bylo provedeno pro dvě vzdálenosti, a to jednoho a osmi metrů. Vzhledem k delšímu časovému rozestupu mezi měřeními pro různé vzdálenosti došlo ke změně rádiového pásma a naměřená propustnost pro delší vzdálenost je tak vyšší.

[3]	0.0-60.1 sec	117 MBytes	16.50 Mbits/sec	-- PC - NB, 1m
[3]	0.0-60.1 sec	121 MBytes	16.95 Mbits/sec	-- PC - N7, 1m
[3]	0.0-60.1 sec	118 MBytes	16.05 Mbits/sec	-- PC - SP, 1m
[3]	0.0-60.1 sec	137 MBytes	19.15 Mbits/sec	-- PC - NB, 8m
[3]	0.0-60.1 sec	139 MBytes	19.55 Mbits/sec	-- PC - N7, 8m
[3]	0.0-60.1 sec	89.2 MBytes	13.10 Mbits/sec	-- PC - SP, 8m

Uvedené výsledky ukazují, že zařízení NB a N7 jsou schopná dosáhnout téměř stejných hodnot propustností, a proto jejich výkon nebude měření negativně ovlivňovat. U SP je patrné, že i když výkon zařízení by měl být dostatečný, což potvrzuje měření při metrové vzdálenosti, v situacích s horším příjmem signálu (větší vzdálenost od AP) dochází k podstatnému snížení propustnosti. Tento jev je pravděpodobně způsoben rozměry integrované antény, které jsou podstatně menší než u ostatních porovnávaných zařízení.

Minimální délka bezdrátového spoje

Experiment potvrdil domněnku, kterou zmiňoval Lo (2007) a sice, že pokud je klient umístěn od AP ve vzdálenosti menší než jeden metr, dojde vlivem špatného šíření signálu k podstatnému snížení propustnosti. Níže uvedené výsledky ukazují snížení propustnosti z původních 18,6 Mbps při vzdálenosti jednoho metru na 11 Mbps při půlmetrové vzdálenosti.

[3]	0.0-60.1 sec	134 MBytes	18.6 Mbits/sec	-- PC - NB (1m)
[3]	0.0-60.1 sec	78.8 MBytes	11.0 Mbits/sec	-- PC - NB (0,5m)

Vliv orientace NB / AP

Autoři metody „packet-by-packet“ (NA, CHEN a RAPPAPORT, 2006) provedli měření pro různé orientace klienta, a to na všechny světové strany. Následující výsledky zobrazují měření pro čtyři různé orientace NB a čtyři orientace AP. Měření bylo provedeno vždy ve stejné vzdálenosti jednoho metru. Z výsledků je patrné, že orientace zařízení může mít na propustnost vliv, tato odchylka je však zřejmě způsobená drobným posunem zařízení, který způsobí odlišné šíření a příjem signálu, což potvrzuje následující experiment.

[3]	0.0-60.1 sec	134 MBytes	18.6 Mbits/sec	-- NB Východ
[3]	0.0-60.1 sec	115 MBytes	16.1 Mbits/sec	-- NB Sever
[3]	0.0-60.1 sec	123 MBytes	17.2 Mbits/sec	-- NB Západ
[3]	0.0-60.1 sec	116 MBytes	16.2 Mbits/sec	-- NB Jih
[3]	0.0-60.1 sec	132 MBytes	18.4 Mbits/sec	-- AP Východ
[3]	0.0-60.2 sec	110 MBytes	15.4 Mbits/sec	-- AP Sever


```
[ 3] 0.0-60.1 sec 111 MBytes 15.5 Mbits/sec -- AP Západ
[ 3] 0.0-60.0 sec 115 MBytes 16.1 Mbits/sec -- AP Jih
```

Vliv minimálního posunutí AP

Tento experiment byl proveden pro určení platnosti tvrzení, že proměnlivá propustnost v předchozím experimentu byla způsobena spíše změnou umístění zařízení, než směrem antény. Obě zařízení byla umístěna orientací na východ se vzdáleností jednoho metru a AP bylo ve čtyřech světových stranách posunuto o 10 cm. Naměřené hodnoty propustnosti odpovídají odchylkám z předchozího experimentu a lze tedy tvrdit, že vliv orientace klienta či AP je vzhledem k jejich posunutí zanedbatelný (za předpokladu, že disponují všesměrovými anténami). Zajímavá je také odchylka při výchozích pozicích ukazující na proměnlivost média.

```
[ 3] 0.0-60.1 sec 126 MBytes 17.5 Mbits/sec -- výchozí pozice
[ 3] 0.0-60.1 sec 125 MBytes 17.4 Mbits/sec -- 10 cm na Východ
[ 3] 0.0-60.1 sec 113 MBytes 15.8 Mbits/sec -- 10 cm na Sever
[ 3] 0.0-60.1 sec 112 MBytes 15.6 Mbits/sec -- 10 cm na Západ
[ 3] 0.0-60.1 sec 135 MBytes 18.8 Mbits/sec -- zpět výchozí pozice
```

Vliv šifrování

Lo (2007) měřil propustnost při vypnutém šifrování z důvodu možného negativního ovlivnění měření vlivem nedostatečného výkonu HW. Proto byla provedena dvě experimentální měření, jedno při zabezpečení WPA2 Personal s šifrováním AES a druhé bez jakéhokoli zabezpečení (*Open System*). Z uvedených výsledků je patrné, že v reálném prostředí obsahujícím několik bezdrátových sítí nemá šifrování na propustnost prakticky žádný vliv. To může být také způsobeno použitím modernějšího HW vybavení, než ke svému experimentu používal Lo.

```
[ 3] 0.0-60.1 sec 120 MBytes 16.8 Mbits/sec -- WPA2 AES, NB
[ 3] 0.0-60.1 sec 127 MBytes 17.7 Mbits/sec -- WPA2 AES, N7
[ 3] 0.0-60.1 sec 112 MBytes 15.6 Mbits/sec -- Open System, NB
[ 3] 0.0-60.1 sec 134 MBytes 18.7 Mbits/sec -- Open System, N7
```

Přenos dat přes dva bezdrátové spoje

Metodika měření propustnosti šířením signálu zobrazovala více než poloviční snížení propustnosti při použití přenosu dat přes dva bezdrátové spoje. Podobných výsledků bylo dosaženo při ověřovacím experimentu. V tomto případě probíhal přenos dat mezi NB nastaveným jako klient a N7 nastaveným jako server. Propustnost byla snížena z původních 18,6 Mbps na 8,88 Mbps.

```
[ 3] 0.0-60.1 sec 134 MBytes 18.6 Mbits/sec -- jeden bezdrátový spoj
[ 3] 0.0-60.1 sec 63.6 MBytes 8.88 Mbits/sec -- dva bezdrátové spoje
```

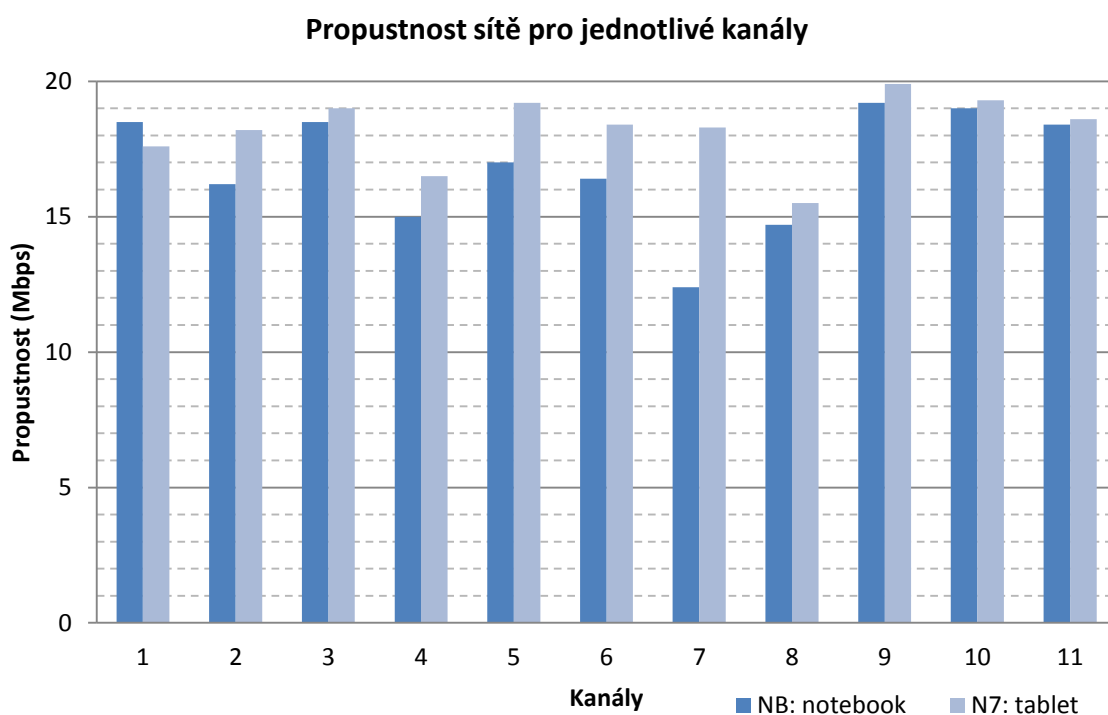
Proměnlivost bezdrátového média

Propustnost bezdrátové sítě se v čase dynamicky mění, což dokládá následující experiment, kde byla měřena propustnost v určitých časových rozestupech.

[3]	0.0–60.1 sec	128 MBytes	17.9 Mbits/sec	-- NB, 17:20, 25.3.2014
[3]	0.0–60.1 sec	125 MBytes	17.5 Mbits/sec	-- N7, 17:21, 25.3.2014
[3]	0.0–60.1 sec	131 MBytes	18.3 Mbits/sec	-- NB, 18:30, 25.3.2014
[3]	0.0–60.2 sec	130 MBytes	18.1 Mbits/sec	-- N7, 18:31, 25.3.2014
[3]	0.0–60.1 sec	117 MBytes	16.3 Mbits/sec	-- NB, 17:30, 1.4.2014
[3]	0.0–60.1 sec	117 MBytes	16.4 Mbits/sec	-- N7, 17:27, 1.4.2014

Vliv ostatních bezdrátových sítí

V tomto experimentu byla postupně ověřována propustnost na všech dostupných kanálech (1–11) pro obě připojená zařízení. Mezi nejzaručenější kanály patřily kanály 1–8, viz příloha B. Pro přehlednost jsou neměřená data zobrazena formou grafu.



Obrázek 17 – Graf naměřené propustnosti v závislosti na rušení od ostatních sítí

Zdroj: vlastní

Z naměřených dat je patrné, že přítomné bezdrátové sítě nezpůsobují velké snížení propustnosti, pokud nejsou výrazněji aktivní. Na druhou stranu jejich aktivní vysílání může způsobit nečekaný propad propustnosti jako v případě sedmého kanálu u měření pomocí NB.

V tomto experimentu nebylo každé měření dvakrát ověřováno kvůli dynamicky se měnícím parametrům v závislosti na aktivitě koexistujících sítí. Stav rádiového pásma byl v průběhu experimentu několikrát ověřován a víceméně odpovídal stavu na začátku experimentu (stejně sítě s podobnými hodnotami RSS).

TCP a UDP propustnost

TCP a UDP jsou rozdílné protokoly, z čehož vyplývá i různá hodnota naměřené propustnosti. Zatímco TCP je spolehlivý protokol se značnou režii, UDP je navrženo pro maximální rychlost bez ohledu na případnou ztrátu paketů. Detaily mezi protokoly TCP a UDP jsou obecně známy a podrobně vysvětleny například v knize *CCENT/CCNA ICND1 640-822* (ODOM, 2012, s. 139–152). Následující tabulka zobrazuje naměřené hodnoty propustnosti pro oba protokoly při měření se třemi různými zařízeními při třech vzdálenostech. SP však při měření UDP propustnosti ukazoval značně kolísavé hodnoty, zřejmě způsobené nedostatečně výkonným HW nebo chybou SW, a zařízení z kategorie chytrých telefonů tak pro měření UDP propustnosti nelze doporučit.

Tabulka 6 – Rozdíl mezi TCP a UDP propustností

TCP / UDP propustnost (Mbps)						
Protokol	TCP			UDP		
Vzdálenost (m)	NB	N7	SP	NB	N7	SP ⁹
1	16,5	17	16,1	23,4	23,9	4,33*
2	16,8	15,9	14,6	22,4	23,3	1,3*
5	17,9	16,7	16,5	22,1	20,4	7,55*

* Nespolehlivé měření – rozdílnost propustnosti překročila 10%.

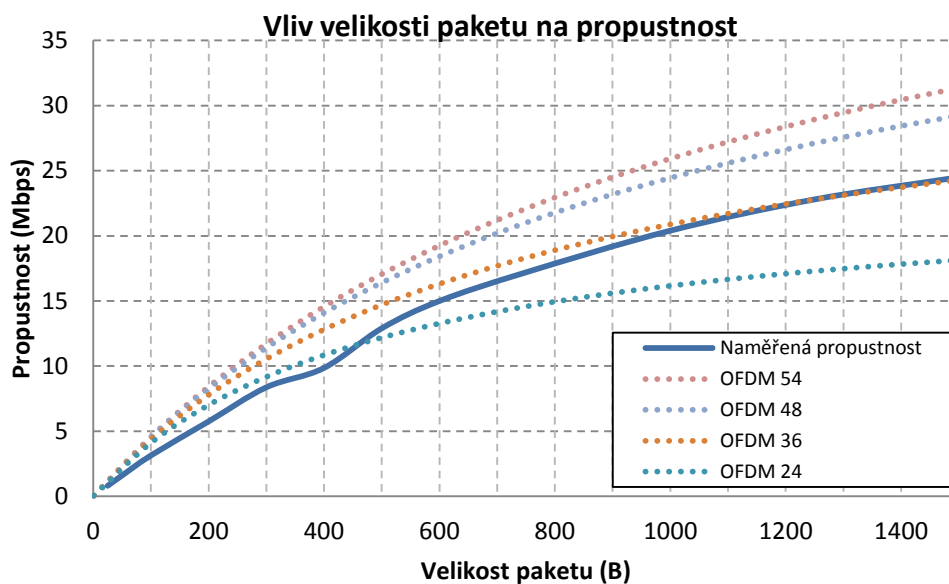
Zdroj: vlastní

Uvedené hodnoty jsou opět průměrem ze dvou měření, které se nelišily o více než 10% a jedná se o průměrné hodnoty potvrzené serverem (*server report*). Naměřené hodnoty u NB a N7 potvrzují vyšší režii TCP protokolu, jehož průměrná propustnost v tomto experimentu byla 16,8 Mbps oproti 22,6 Mbps u UDP, což je téměř o 35% více. Na druhou stranu protokol UDP byl více náchylný na změny v bezdrátovém médiu, a jednotlivá měření tak ukazovala výrazně proměnlivější výsledky, což často znamenalo provádět více měření.

Vliv velikosti paketu

Program *Jperf* umožňuje nastavení velikosti paketu při měření UDP propustnosti. Toho bylo využito při ověření vlivu velikosti paketů, který zmiňoval Bredel a Fidler (2008). Následující graf dokazuje značný vliv velikosti paketu na propustnost. Pro názornost jsou přerušovanými čarami zobrazeny vypočítané teoretické hodnoty propustnosti pro modulace OFDM 24 a vyšší.

⁹ Pro připomenutí: NB = notebook, N7 = tablet (Nexus 7), SP = chytrý telefon (smartphone).



Obrázek 18 – Graf vlivu velikosti paketu na propustnost

Zdroj: vlastní

Dostupná kapacita a propustnost

Poslední experiment byl zaměřen na měření dostupné kapacity a porovnával jeho výsledky s naměřenou propustností. Dostupná kapacita byla měřena nástrojem *Pathload*, který podporuje pouze operační systém Linux, a proto bylo měření provedeno v domácích podmínkách (cihlový dům viz kapitola 5) místo místnosti NET101. Jako klient byl využit PC_{LU} a server reprezentoval NB. Nejprve bylo provedeno měření TCP propustnosti, následované UDP propustností a na závěr bylo provedeno několik měření dostupné kapacity (zde uvedeny K1–K3).

```
[ 3] 0.0-60.1 sec 133 MBytes 18.6 Mbits/sec -- TCP1
[ 3] 0.0-60.1 sec 131 MBytes 18.3 Mbits/sec -- TCP2
[184] 0.0-60.1 sec 164 MBytes 23.0 Mbits/sec 0.656 ms (23%) -- UDP1
[184] 0.0-60.1 sec 171 MBytes 23.9 Mbits/sec 0.597 ms (20%) -- UDP2
Available bandwidth range : 6.33 - 18.42 (Mbps) (15,77 sec) -- K1
Available bandwidth range : 6.25 - 22.24 (Mbps) (15,13 sec) -- K2
Available bandwidth range : 6.36 - 18.61 (Mbps) (83,28 sec) -- K3
```

Nástroj *Pathload* měří kapacitu na třetí vrstvě ISO/OSI modelu a k měření využívá UDP pakety, které vysílá mezi dvěma zařízeními v určitých skupinkách (*fleets*) s různou rychlostí přenosu a na základě jejich zpoždění odhadne dostupnou kapacitu (DOVROLIS, 2003).

I přes několik provedených měření *Pathload* ukazoval vysokou variabilitu v dostupné kapacitě, zřejmě způsobenou proměnlivostí bezdrátového média. Nejvyšší naměřená dostupná kapacita však dosahovala poměrně přesně hodnot naměřené TCP propustnosti a v případě druhého měření (K2) propustnosti UDP. Lze tedy říci, že nástroje pro měření dostupné kapacity lze využít i pro měření propustnosti. Z důvodu vyšší náročnosti měření,

nižší přesnosti a nemožnosti měření mezi různými operačními systémy se však tomuto měření v práci dále nevěnuji.

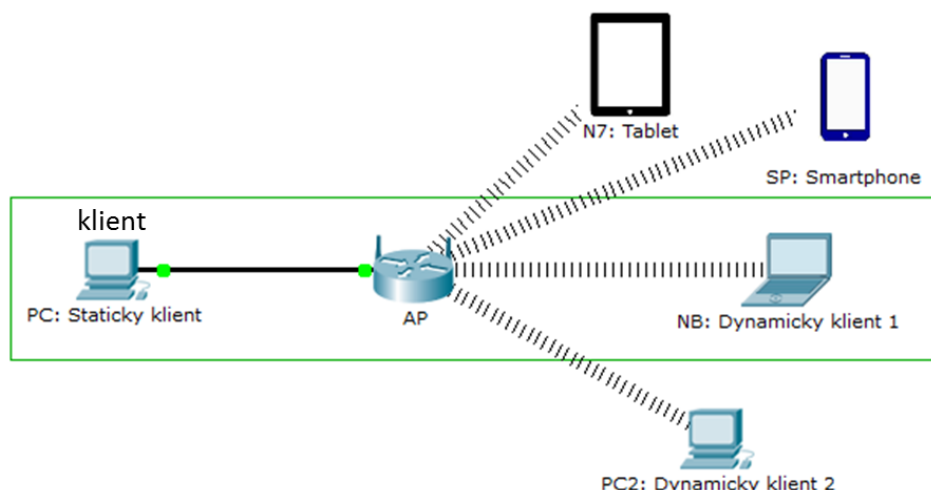
4.2 Metodika komplexního měření propustnosti v reálném prostředí

Na základě vlastností z analýzy nedostatků a na základě praktického ověření některých z předpokladů metodik byla navržena metodika komplexního měření propustnosti v reálném prostředí. Metodika se skládá ze dvou částí, ze základního měření, kde se měří propustnost mezi statickým a dynamickým klientem, a z volitelného upřesňujícího měření mezi více zařízeními. Tato druhá část je zaměřena na zmírnění dopadů proměnlivosti bezdrátového média. Ta může být způsobena měnící se úrovní rušení ostatními sítěmi v okolí (s měnícím se objemem přenášených dat) nebo lokálním úbytkem signálu způsobeným vlivem vícecestného šíření signálu. Tento způsob také odstraňuje potenciální problém v podobě různé orientace klienta, případně specifické implementace anténního modulu klienta.

4.2.1 Schéma metodiky

Následující obrázek znázorňuje schéma měření metodiky. Zařízení, která se nacházejí v zeleném orámování, jsou vyžadována pro základní měření, zařízení mimo rám jsou pak navíc použita pro upřesňující měření. Počet ani typ těchto zařízení není pevně definován, jedinou podmínkou je, že jejich výkon nesmí negativně ovlivnit měření. Pokud experiment vyžaduje použití takového zařízení (například pokud se v síti budou pohybovat uživatelé s těmito zařízeními), toto zařízení se uvede v samostatné kategorii a jeho data nebudou zahrnuta do celkového průměru naměřené propustnosti.

Minimální délka bezdrátového spoje, pro kterou může být propustnost měřena je jeden metr, maximální hodnota naměřené propustnosti je pak typicky ve vzdálenosti okolo dvou metrů. Pokud probíhá měření propustnosti v reálném prostředí, vzdálenost se postupně zvyšuje a provádí se měření na předem určených místech. Pokud je volitelné měření prováděno v otevřeném prostoru, lze zařízení kruhově rozmístit ve stejných vzdálenostech od přístupového bodu. V případě měření v komplikovaném prostředí, kdy mezi zařízeními není přímá viditelnost, je nutné postupně jednotlivé dynamické klienty umísťovat na stejné místo, případně pár centimetrů od sebe, což je vzhledem k vzdálenosti od AP zanedbatelný rozdíl.



Obrázek 19 – Schéma rozložení metodiky měření propustnosti

Zdroj: vlastní

4.2.2 Detaily metodiky

Propustnost je měřena vždy mezi statickým klientem, který je v programu *Iperf* nastaven jako klient a jedním z připojených zařízení (dynamický klient), které je vždy ve funkci serveru, a tedy pouze poslouchá na určitém portu a čeká na připojení klienta. Jednotlivé měření probíhá po dobu jedné minuty a je provedeno dvakrát po sobě. Tyto dvě průměrné hodnoty propustnosti jsou porovnány, a pokud jsou určeny jako spolehlivé, je z nich vypočítána průměrná hodnota propustnosti jako aritmetický průměr. Pokud je prováděno volitelné měření, ze všech hodnot propustností naměřených s jednotlivými klienty (kromě specifických zařízení, které mají svoji vlastní kategorii) včetně hodnot získaných ze základního měření je vypočítán průměr, a ten je potom uveden jako výsledek metodiky.

Měření lze provádět oběma transportními protokoly – TCP i UDP, přičemž je vždy nutné uvést, který protokol byl použit. Vzhledem k dominanci protokolu TCP, která už byla zmiňována (96,8%), se ve všech měřeních věnuji právě tomuto protokolu a UDP používám jen pro ověření ve specifických případech. Tento způsob měření je doporučený také kvůli větší předvídatelnosti protokolu TCP a jednoduššímu způsobu měření.

Pokud je experiment prováděn v otevřeném prostředí, kde se mohou nacházet lidé, je nutné použít šifrování, a to alespoň WPA nebo WPA2. Šifrování WEP je dnes již prolomené a není považováno za adekvátní zabezpečení. Toto opatření vychází z předpokladu, že je použit dostatečně výkonný HW, který nezpůsobuje snížení propustnosti. Vzhledem k tomu, že v reálném prostředí často není možné dosáhnout maximálních hodnot propustnosti, HW nebývá limitujícím faktorem. Naopak nepoužitím šifrování by mohlo dojít k ovlivnění experimentu uživatelem, který by se k síti z nějakého důvodu volně připojil.

Všechna zařízení účastníci se experimentu by měla být umístěna v podobné výšce, přičemž doporučená výška je zhruba jeden metr nad zemí kvůli zmiňovaným problémům s Fresnelovou zónou. Zařízení by ideálně měla být umístěna na okrajích stolů apod. Pokud

mezi zařízeními není přímá viditelnost, je tuto skutečnost nutné uvést. Měřená vzdálenost mezi zařízeními se vždy uvádí jako vzdušná vzdálenost – tedy nejkratší přímá.

4.2.3 Konfigurace HW a SW nástrojů

Cílem této podkapitoly je vysvětlit nastavení přístupového bodu pro provádění experimentu. V druhé části je podrobně popsána instalace a základní parametry programů *Iperf*, respektive *Jperf*, které jsou využity v metodice měření propustnosti.

Nastavení přístupového bodu

Konfigurační soubor nastavení přístupového bodu je umístěn v příloze C. Následující seznam zobrazuje nastavení několika hlavních parametrů přístupového bodu pro provádění experimentálních měření.

1) Basic Wireless Settings

- Network Mode: G only, Network Name (SSID): linksys-dp.
- Wireless Channel: 11 – 2,462 GHz (pokud nenastaven jiný).

2) Wireless Security

- Security Mode: WPA2 Personal, WPA Algorithms: AES.

3) Ostatní

- Vypnuta dodatečná bezpečnostní opatření (FW, IPSec, PPTP, L2TP).
- Vypnuty služby: DMZ, QoS, UPnP, SecureEasySetup.

Instalace a zprovoznění programu Iperf

Stažení programu a podrobné detaily o instalaci jsou dostupné ze stránek iperf.fr. V operačním systému Windows stačí stáhnout a rozbalit příslušný soubor a pak program spustit příkazem „*iperf*“ provedeným v příkazové řádce v adresáři, kde je program rozbalen.

V operačním systému Linux lze program stáhnout a zprovoznit následujícími příkazy (platné pro 32 bitový systém):

```
wget http://iperf.fr/download/iperf_2.0.5/iperf_2.0.5-2_i386
chmod +x iperf_2.0.5-2_i386
sudo mv iperf_2.0.5-2_i386 /usr/bin/iperf
```

Iperf ve verzi pro operační systém Android (*Iperf for Android*) je nutné nainstalovat z obchodu Google Play. Po spuštění programu lze do zobrazené příkazové řádky zadávat příkazy obdobně jako v ostatních operačních systémech s tím, že příkaz je nutné potvrdit kliknutím na tlačítko ON/OFF (týká se současné verze 2.06).

Zobrazení nápovědy programu:

```
iperf -h
```

Přehled parametrů programu Iperf

Následující tabulka shrnuje hlavní parametry používané v experimentálním měření. Úplný výčet všech parametrů lze nalézt v nápovědě programu *Iperf*.

Tabulka 7 – Popis základních parametrů programu Iperf

Parametr	Název	Vysvětlení
Obecné parametry:		
-h	help	Zobrazení nápovědy
-f	format	Formát zobrazování výstupu (Kbits, Mbits, KBytes, MBytes,...)
-i	interval	Interval v sekundách mezi výpisem informací o aktuální propustnosti
-p	port	Číslo portu, na kterém bude nasloucháno/ke kterému se připojí
-u	UDP	Použití UDP místo TCP
Parametry serveru:		
-s	server	Specifikuje mód serveru
Parametry klienta:		
-c	client	Specifikuje mód klienta
-t	time	Délka provádění měření v sekundách (defaultně 10 sekund)
-n	num	Počet bajtů, které budou odeslány (nahrazuje parametr -t).
-b	bandwidth	Nastavení rychlosti odesílání dat pro UDP v bps (defaultně 1 Mbps)
-d	dualtest	Nastavení obousměrného testování
-P	parallel	Počet paralelních spojení, která budou testovat propustnost (simulace více klientů)

Zdroj: zpracováno dle nápovědy programu Iperf

Měření TCP propustnosti programem Iperf

Následující příkazy slouží pro měření TCP propustnosti, které je v metodice využíváno primárně. Vteřinový výpis je nutný pro detekci proměnlivých výpadků přenosu. Ostatní parametry nejsou pro měření propustnosti vyžadovány a postačí použití defaultních hodnot.

Spuštění jako serveru s výpisem propustnosti každou sekundu:

```
iperf -s -i 1
```

Spuštění v módu klienta s vteřinovým výpisem a dobou trvání měření 60 sekund:

```
Iperf -c IP -i 1 -t 60 (kde IP je IP adresa serveru)
```

Měření UDP propustnosti programem Iperf

Měření UDP propustnosti má oproti TCP propustnosti určitá specifika. Protože se jedná o nespolehlivý protokol, vysílající zařízení neobdrží žádné informace o doručení či ztracení odesílajících paketů. V praxi to znamená, že udávaná rychlost odesílání dat na statickém klientu se bude blížit limitu kabelového připojení, kterým je klient připojen k AP (tedy

v případě Fast Ethernetu to bude okolo 95 Mbps). Data je tedy nutné měřit na straně serveru, který musí mít na rozdíl od měření TCP propustnosti nastaven vteřinový výpis dat (parametr -i). Alternativně lze využít sumárních informací, které budou po dokončení měření odeslány zpět klientu a označeny jako „*Server Report*“. I přes to je však nutné na straně serveru ověřit případné výpadky v přenosu dat a nedosažení nastavené maximální přenosové rychlosti, která by snížila výslednou propustnost.

Tato rychlost je druhým specifickým měřením TCP propustnosti a určuje, jako rychlostí budou data z klienta odesílána. Rychlost musí být vždy vyšší než dosažitelná propustnost, jinak by měření bylo negativně ovlivněno. Z tohoto důvodu je nutné kontrolovat výpis aktuální propustnosti na straně serveru (opět parametr -i), a pokud bude propustnost rovna nastavené přenosové rychlosti, je nutné zvolit rychlost vyšší a provést nové měření.

Poslední upozornění se týká výkonu HW, které může způsobovat výkyvy naměřené propustnosti na které je UDP velice náchylné. Z tohoto důvodu je měření vhodné provádět s hlavními zařízeními a nepoužívat experimentální zařízení, jakým je například chytrý telefon.

Spuštění v módu UDP serveru s výpisem propustnosti každou sekundu:

```
iperf -s -i 1 -u
```

Spuštění v módu klienta s vteřinovým výpisem, dobou trvání měření 60 sekund a odesílající rychlostí 20 Mbps:

```
Iperf -c IP -i 1 -t 60 -u -b 20000000 (kde IP je IP adresa serveru)
```

Alternativní měření programem Jperf

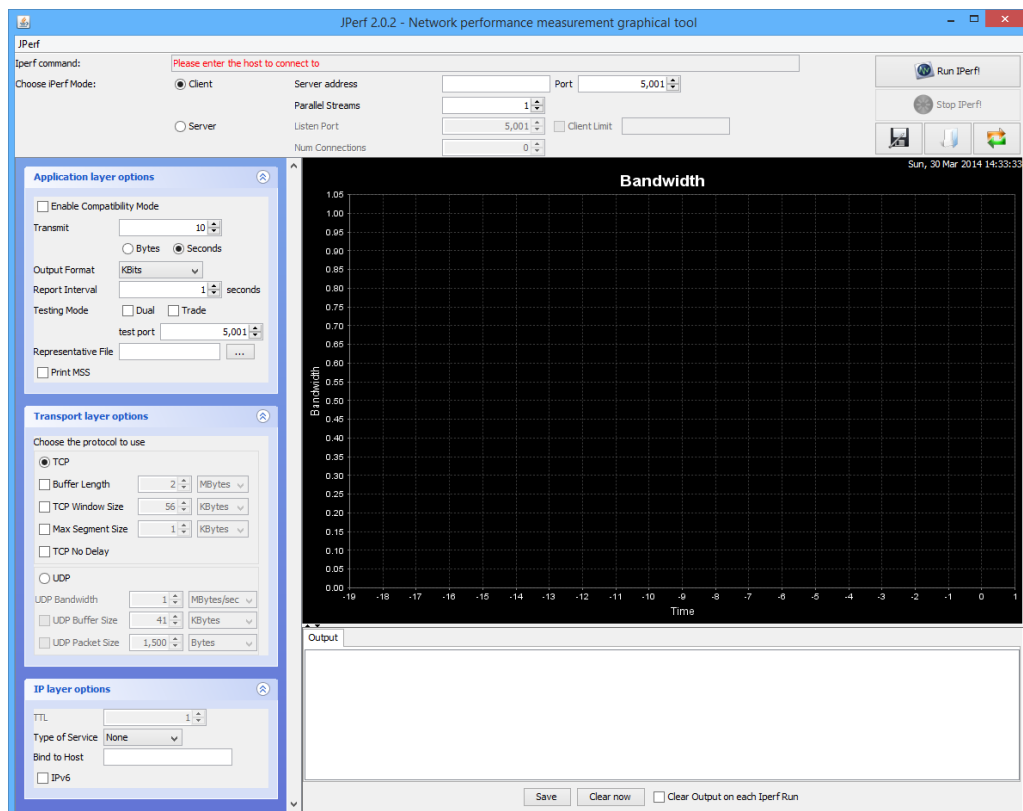
V případě zájmu lze pro měření propustnosti použít program *Jperf*, který slouží jako grafická nadstavba programu *Iperf*. *Jperf* verze 1.7.0 lze opět volně stáhnout ze stránek iperf.fr (odkaz se nachází v sekci „*Projects around Iperf*“). Program stačí pouze rozbalit a spustit souborem *jperf.bat* (Windows), respektive *.jperf.sh* (Linux). Ke spuštění programu je však vyžadována verze Javy alespoň 1.5, jejíž instalaci je možné v Linuxu ověřit a spustit následujícími příkazy:

```
java -version (ověření současné verze)
sudo apt-get install default-jre (instalace Javy)
```

V operačním systému Windows může na novějších systémech dojít k zobrazení hlášky „*Windows cannot find javaw*“. To je způsobeno špatně nastavenou, či chybějící cestou k souboru *javaw.exe*. Tu je nutné ručně upravit v souboru *jperf.bat* (případně použít předpřipravený soubor *jperf.bat* umístěný v příloze C). Příklad správného nastavení současné verze Javy v operačním systému Windows 8.1:

```
Path=C:\Program Files (x86)\Java\jre7\bin;
```

Po úspěšném spuštění programu dojde k zobrazení následujícího rozhraní:



Obrázek 20 – Rozhraní programu Jperf

V horní části programu jsou ovládací prvky pro módy klienta a serveru, v levé části pak specifické prvky detailního nastavení a pod ním volba transportního protokolu a několik základních prvků spojených se sítovým protokolem. Hlavní část pak graficky reprezentuje měřené údaje (výchozí hodnota aktualizace je jedna vteřina) s tím, že klasický výstup programu *Iperf* je zobrazen v okně *Output*.

Program *Jperf* slouží pouze jako grafická nadstavba, a tak je možné ho použít i v kombinaci s programem *Iperf* běžícím na ostatních zařízeních.

4.2.4 Postup provedení experimentálního měření

Vzhledem k proměnlivosti rádiového pásma by experimentální měření mělo být provedeno co nejrychleji. Aby se vyloučilo případné ovlivnění proměnlivými vlivy, je vhodné po skončení experimentu provést ověření naměřené propustnosti popsané v pátém kroku.

Následující postup ilustruje provedení experimentálního měření.

1) Nastavení kanálu pro provádění experimentu

Prvním krokem je využití některého ze SW nástrojů pro určení kvality rádiového prostředí. Nejméně zarušený kanál by měl zajišťovat maximální propustnost a nejmenší odchylky v měřené propustnosti, a proto je třeba ho na AP nastavit pro provedení experimentu. Skenování rádiového pásma by mělo být provedeno v bodě, kde se bude nacházet AP, nebo v jeho přímé blízkosti.

V případě dostatku času lze provést měření propustnosti ve vzdálenosti jednoho metru pro všechny dostupné kanály a určit tak ten s nejvyšší hodnotou propustnosti. Přesto je však nutné přihlédnout k počtu koexistujících sítí, které mohou měření proměnlivě ovlivňovat.

2) Základní měření propustnosti (PC–NB)

Následuje fáze provádění základního experimentu, ve kterém jsou po sobě provedeny dva bezdrátové přenosy, přičemž každý trvá jednu minutu. Data jsou přenášena mezi statickým a dynamickým klientem. Následuje porovnání průměrných hodnot naměřených propustností, a pokud se neliší o více než 10%, lze měření považovat za úspěšné. Porovnání je provedeno podle následujícího vzorce:

$$\Delta = \left(\frac{P_V - P_M}{P_V} \right) * 100$$

Zdroj: vlastní

kde P_V – je vyšší hodnota z průměru minutového měření propustnosti,
 P_M – je nižší hodnota z průměru minutového měření propustnosti.

V případě, že se naměřené hodnoty liší o více než 10%, je vhodné provést další měření. Pokud se některé hodnoty shodují, mohou se uvést do metodiky. Pokud se však nově naměřená hodnota neshoduje s žádnou z předchozích, je vhodné zařízení o pár centimetrů posunout a provést nové měření. Zařízení se totiž může nacházet v bodě, kde vlivem více cestného šíření signálu dochází k lokálnímu úbytku signálu. Pokud ani nové měření neprokáže shodu hodnot, označí se jako nespolehlivé a pokračuje se dále. Kvůli časové proměnlivosti média není možné čekat delší dobu na jednom kroku, protože zbytek měření by to mohlo negativně ovlivnit. Pokud je však naměřená propustnost velice nízká (nižší než 5 Mbps), porovnání se pravděpodobně téměř vždy bude lišit o mnohonásobně více než o 10%. To je v pořádku, pokud se propustnost liší o méně než 1 Mbps a tento jev upozorňuje na fakt, že používání sítě v tomto konkrétním místě může být na hranici použitelnosti. Toto měření se v experimentu také označí jako nespolehlivé.

V případě, že se při měření propustnosti v přenosu vyskytují výpadky (vteřinový výpis ukazuje propustnost 0 bitů za sekundu), naměřené hodnoty se pravděpodobně shodovat nebudou. V tomto případě se přenos označí jako chybový (pokud došlo k ojedinělým výpadkům tvořících méně než 10% přenosového času – v případě minutového měření tedy méně než 6 výpadků, a žádný výpadek nenásleduje dvakrát po sobě), nebo silně chybový (výpadků je více než 10%, či jsou alespoň dva hned po sobě). Chybové přenosy nemusí pro síť znamenat vážnější problém, způsobují pouze snížení propustnosti a dočasné zvýšení zpoždění, které by mělo vliv hlavně na real-time aplikace jako videokonference a IP telefonie. Silně chybové přenosy na druhou stranu prakticky znemožňují síť používat a v realitě například při implementaci bezdrátové sítě by měly být považovány za místa s nulovou propustností.

Příklad chybového přenosu (další výpadek se v měření nevyskytuje):

[3]	0.0– 1.0 sec	128 KBytes	1.05 Mbits/sec
[3]	1.0– 2.0 sec	0.00 Bytes	0.00 bits/sec
[3]	2.0– 3.0 sec	512 KBytes	4.19 Mbits/sec
[3]	3.0– 4.0 sec	512 KBytes	4.19 Mbits/sec
[3]	4.0– 5.0 sec	640 KBytes	5.24 Mbits/sec

Příklad silně chybového přenosu:

[3]	0.0– 1.0 sec	128 KBytes	1.05 Mbits/sec
[3]	1.0– 2.0 sec	0.00 Bytes	0.00 bits/sec
[3]	2.0– 3.0 sec	128 KBytes	1.05 Mbits/sec
[3]	3.0– 4.0 sec	0.00 Bytes	0.00 bits/sec
[3]	4.0– 5.0 sec	0.00 Bytes	0.00 bits/sec
[3]	5.0– 6.0 sec	128 KBytes	1.05 Mbits/sec

3) Volitelné měření propustnosti (PC–všechna klientská zařízení)

V této volitelné fázi je prováděno měření mezi statickým klientem a ostatními zařízeními podle stejného scénáře jako v předchozím kroku. Pokud probíhá měření se zařízením z kategorie, které by pravděpodobně mohlo mít nižší hodnoty propustnosti, než hlavní měření, toto zařízení se nebude uvádět do celkového průměru, ale bude mít svoji vlastní kategorii. Typicky se jedná o zařízení s nižším výkonem či menšími rozměry (telefony, přehrávače, chytré hodinky a podobně). Aritmetické průměry jsou vždy vypočítány podle následujícího vzorce.

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$$

Zdroj: vlastní

4) Měření v různých vzdálenostech

Následuje opakování kroků dva a tři pro různé vzdálenosti mezi dynamickými klienty a přístupovým bodem. Kromě vzdáleností je vhodné uvádět specifické parametry místa jako například rozdílnou výšku oproti AP, či počet překážek mezi AP a zařízením.

5) Ověření naměřené propustnosti

Pokud bylo prováděno měření TCP propustnosti, lze toto měření ověřit dodatečným měřením propustnosti pomocí UDP protokolu. Vzhledem k tomu, že UDP je konstruováno pro maximální rychlost a nebere ohledy na případný provoz na spoji, bude pravděpodobně naměřená propustnost podstatně vyšší. Pokud by došlo k naměření výrazně nižší hodnoty propustnosti, než bylo naměřeno TCP protokolem, zřejmě došlo ke změně stavu rádiového pásma a je vhodné provést znovu základní měření TCP propustnosti.

Vzhledem k časové náročnosti měření UDP propustnosti, vyžadující rekonfiguraci všech klientů pro měření UDP protokolem, je vhodné toto měření provést až po dokončení měření na všech prověřovaných místech.

4.2.5 Shrnutí stěžejních vlastností metodiky

Metodika komplexního měření propustnosti v reálném prostředí má specifické vlastnosti, které shrnuje následující seznam.

- Měření programem *Iperf* / *Jperf* případně jeho portem pro OS Android,
- měření podle typického scénáře zapojení (jeden bezdrátový přenos),
- měření prováděno na nejméně zarušeném kanále, který je určen skenováním okolních sítí před provedením experimentu,
- zvýšení přesnosti měření volitelným měřením mezi více zařízeními,
- možnost měření propustnosti zařízeními patřícími do specifických kategorií (chytré telefony, senzory, přehrávače, hodinky, apod.),
- naměřená propustnost konkrétního zařízení je aritmetickým průměrem ze dvou minutových přenosů, které se neliší o více než 10%,
- celková naměřená propustnost je aritmetickým průměrem dílčích průměrných propustností všech zařízení spadajících do hlavní kategorie,
- označení nespolehlivého měření (měření, kde se liší propustnost o více než 10%),
- označení chybového a silně chybového spojení,
- možnost ověření experimentu měřením UDP propustnosti.

5 Experimentální měření v cihlovém domě

V této kapitole bude proveden experiment v reálném prostředí cihlového domu. Cílem experimentu bude prozkoumat šíření signálu standardu 802.11g a jeho vliv na propustnost. Dále bude zkoumáno, zda jeden AP dostatečně efektivně pokryje oblast dvou sousedících bytů.

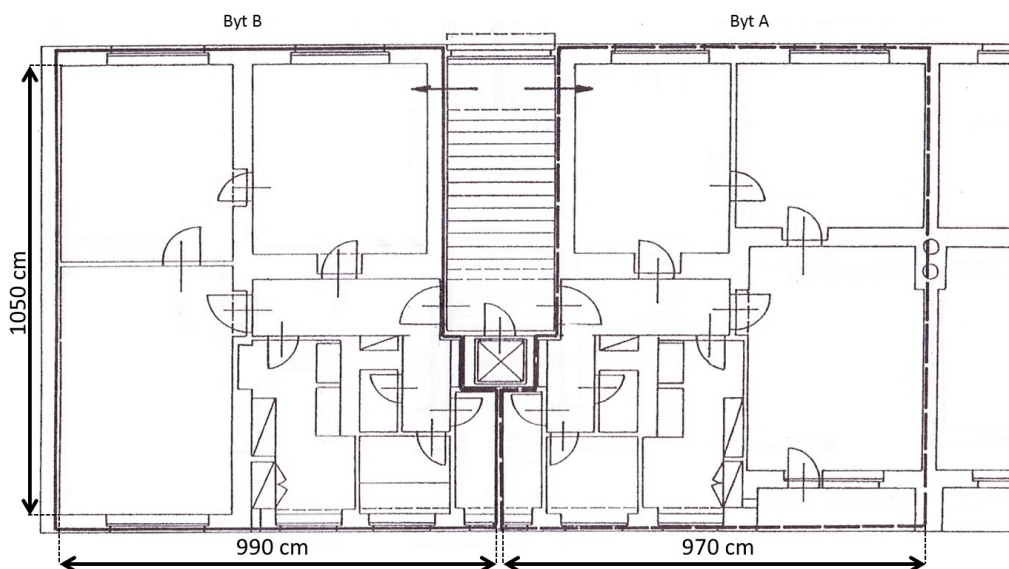
5.1 Úvod do experimentu

Při ověřování metodik v laboratorní místnosti NET101 bylo zjištěno, že tato místnost nebude pro rigorózní měření propustnosti dostatečně rozměrná, a proto bylo experimentální měření provedeno v typickém prostředí cihlového domu. Pro zachování stejných podmínek byl použit stejný AP a stejný HW s tím, že statický klient byl nahrazen PC_{LW} (dále označován jako PC), který disponuje podobným HW jako PC_D.

5.1.1 Popis prostředí

Měření bylo prováděno ve dvou sousedících bytech velikosti 3+1 umístěných ve třetím podlaží čtyřpodlažního cihlového domu. Ten je situován v Pardubické čtvrti Dukla a bezprostředně sousedí s dvěma dalšími domy stejného typu. Toto prostředí poskytlo experimentu dostatečnou reálnost prostředí danou vlivem přítomnosti ostatních bezdrátových sítí, komplexním prostředím pro komplikované šíření signálu a dostatečným prostorem pro provádění experimentu.

Rozložení bytů a jejich rozměry ilustruje následující obrázek. Pro potřeby experimentu budou jednotlivé byty dále značeny jako A a B.



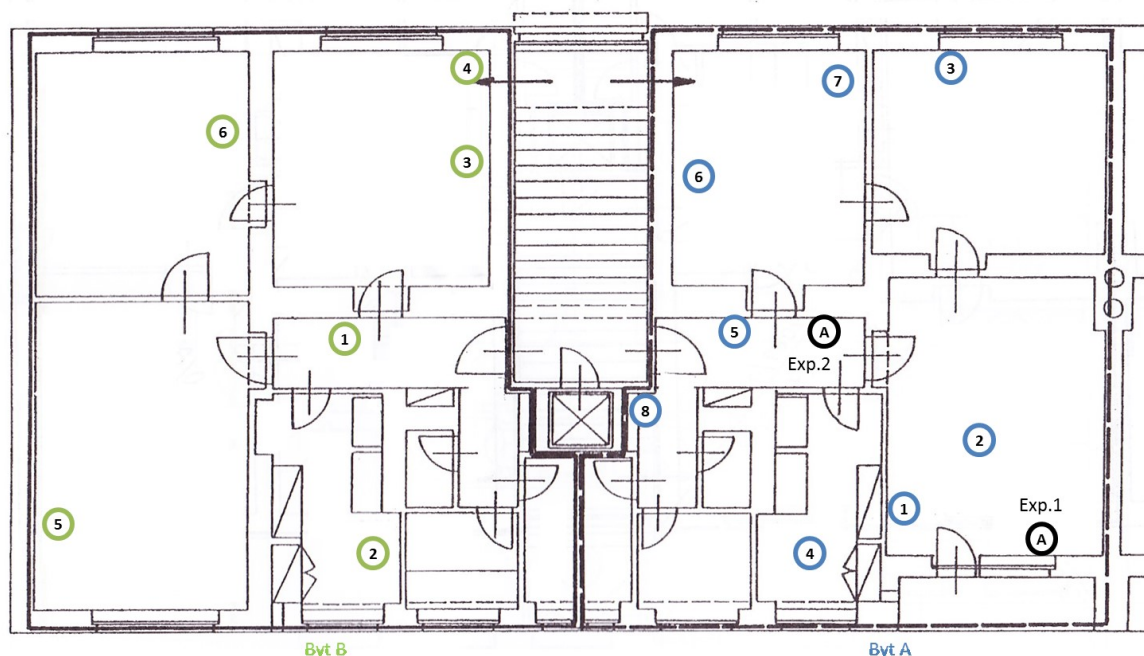
Obrázek 21 – Plán bytů pro provádění experimentálního měření

Zdroj: zpracováno dle materiálů v kupní smlouvě

5.1.2 Popis experimentů

Prověření stanovených cílů vyžaduje rozdělení měření na dva experimenty. První experiment ilustruje nevhodné umístění přístupového bodu a zkoumá dosah šíření signálu. V tomto případě je prověřeno chování metodiky i v lokacích se špatným příjmem signálu. Druhý experiment se věnuje typickému umístění přístupového bodu a opět zkoumá šíření signálu dvěma byty.

Měření propustnosti bylo provedeno na čtrnácti místech, z toho osm z nich bylo v bytě A a šest v bytě B. Tato místa byla stejná pro oba experimenty. V experimentech se lišilo umístění AP, což zobrazuje následující obrázek. Přístupové body jsou označeny černě symbolem A s popisem, o který experiment se jednalo. Jednotlivá místa, na kterých probíhalo měření, jsou pak očíslována v rámci konkrétního bytu. Ve výsledcích jsou pak označeny A1–A8, respektive B1–B6.



Obrázek 22 – Plán bytů pro provádění experimentálního měření

Zdroj: zpracováno dle materiálů v kupní smlouvě

5.1.3 Ukázka z postupu provádění metodiky

Podle postupu, popsaném ve čtvrté kapitole, bylo provedeno experimentální měření propustnosti, což ilustruje následující text. Jedná se o měření prvního experimentu v bodě 1A.

1) Nastavení kanálu pro provádění experimentu

Rádiové pásmo bylo skenováno nástroji *WiFi Analyzer* a *inSSIDer*, které ukázaly velice zarušené 2,4 GHz pásmo, ve kterém bylo prakticky rovnoměrně umístěno zhruba šestnáct sítí. Jako nejvhodnější kanál pro provádění experimentů byl zvolen kanál první, a to z důvodu, že přijímaná úroveň signálu okolních sítí v bytě A byla na tomto kanále nejnižší

(pod -80dBm). V bytě B tato úroveň vzrostla na -70dBm, ale ani ostatní kanály na tom nebyly o moc lépe a jejich hodnoty se pohybovaly kolem -75dBm. Pro provádění experimentů je však stěžejní stav v bezprostřední blízkosti AP, ke kterému byl navíc vzat v úvahu fakt, že tři sítě umístěné na kanálech 1, 4 a 8 měly nastavenou dvojnásobnou šířku pásma (40 MHz), a tedy mohly zasahovat až do frekvencí vyšších kanálů.

2) Základní měření propustnosti (PC–NB)

Základní měření prováděné dvěma minutovými přenosy na umístění 1A. Následující hodnoty jsou průměrem z jednotlivých přenosů.

```
[ 3] 0.0-60.1 sec 133 MBytes 18.6 Mbits/sec
[ 3] 0.0-60.1 sec 139 MBytes 19.4 Mbits/sec
```

Následovalo porovnání průměrných hodnot propustností:

$$\Delta = \left(\frac{19,4 - 18,6}{19,4} \right) * 100 = 4,124\%$$

Protože naměřené hodnoty se neliší o více než 10%, do výsledků je zaznamenána průměrná hodnota 19 Mbps.

3) Volitelné měření propustnosti (PC–N7, PC–SP)

Volitelné měření propustnosti probíhalo obdobně jako základní měření, jen byla využita další zařízení, a to N7 a SP. Měření propustnosti pomocí SP bylo bráno jako doplňkové a do průměrných hodnot nebylo zahrnuto. V prvním experimentu byla propustnost mezi PC a SP měřena pouze na vybraných umístěních. Následující data jsou z naměřené propustnosti pomocí N7.

```
[ 3] 0.0-60.1 sec 145 MBytes 20.2 Mbits/sec
[ 3] 0.0-60.1 sec 142 MBytes 19.8 Mbits/sec
```

Porovnání těchto hodnot přináší rozdíl 1,98% a průměrná hodnota propustnosti 20 Mbps je tedy zahrnuta do výsledků. Celková naměřená hodnota propustnosti pro umístění 1A je aritmetickým průměrem hodnot ze zařízení NB a N7 a je rovna 19,5 Mbps. Hodnota průměrného rozdílu je pak vypočítána jako aritmetický průměr z hodnot 4,12% a 1,98% a odpovídá hodnotě 3,052%.

4) Opakování kroků 2–4 pro ostatní vzdálenosti (2A–6B).

5) Ověření naměřené propustnosti

Propustnost protokolem UDP mezi PC_{LOW} a NB byla ověřena u druhého experimentu, a to na místech 1A a 1B.

5.2 Experiment 1 – nevhodné umístění AP

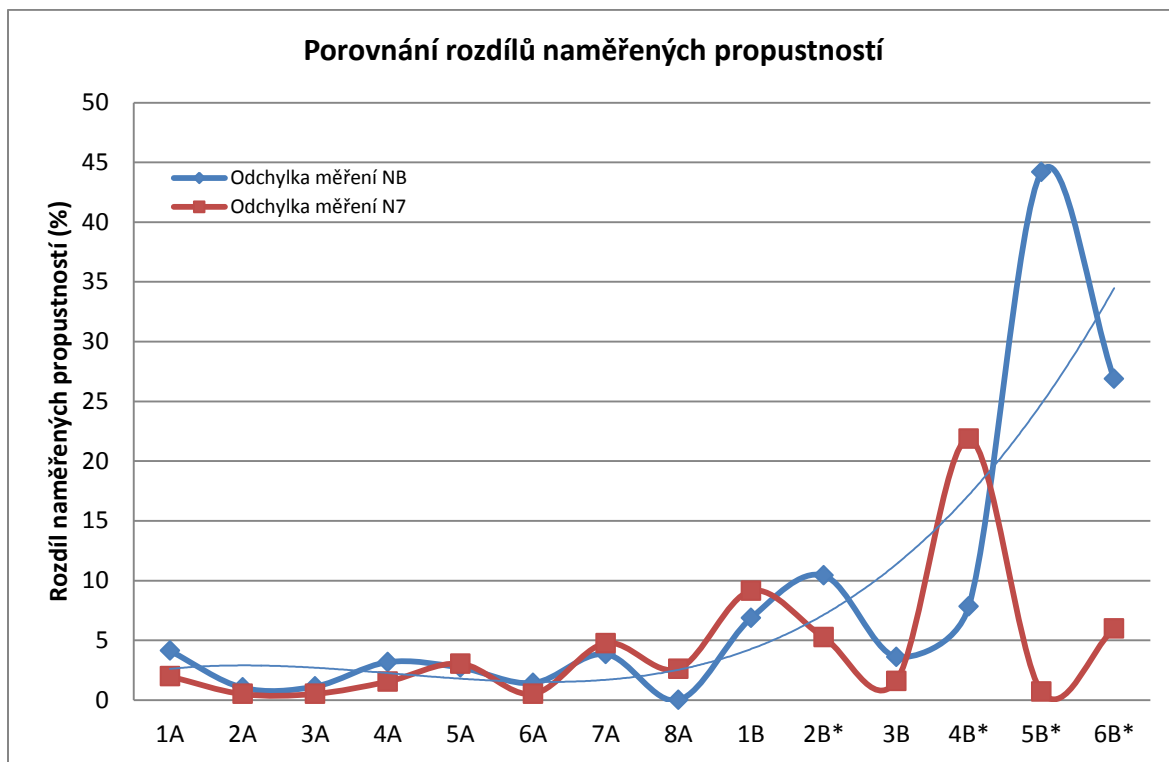
První experiment prokázal, že při nevhodném umístění přístupového bodu byla bezdrátová síť v bytě B použitelná pouze na specifických místech, která ale mohla zaznamenat určité výpadky přenosu dat. Následující tabulka shrnuje naměřené hodnoty propustnosti. Oranžovou barvou jsou znázorněny chybové přenosy a červenou barvou pak silně chybové (podle specifikace popsané v metodice). Měření SP bylo provedeno pouze na vybraných místech jako doplňkové. U každého umístění je uvedena přibližná vzdálenost zařízení od AP a počet překážek.

Tabulka 8 – Naměřené hodnoty propustnosti experimentu 1

Experiment 1 (Mbps)					
Umístění	NB	N7	Průměr	Průměrné rozdíly (%)	SP
1A, 2,5m - 0 zdí	19	20	19,5	3,051955	
2A, 2,5m - 0 zdí	19,1	19,75	19,425	0,773359	16,7
3A, 9m - 1 zeď	17,5	19,15	18,325	0,828598	
4A, 4,5m - 1 zeď	18,6	19,25	18,925	2,360497	
5A, 7m - 2 zdi	18,15	19,4	18,775	2,881538	
6A, 9,5m - 2 zdi	13,9	19,25	16,575	0,973353	15,25
7A, 9,5m - 2 zdi	10,2	14,35	12,275	4,304029	15,25
8A, 7,5m - 2 zdi	18,6	18,85	18,725	1,308901	
1B, 13,5m - 4 zdi	4,79	16,7	10,745	7,998848	
2B, 12,5m - 6 zdi	3,09*	11,1	7,095	7,846303	
3B, 13m - 4 zdi	7,905	12,4	10,1525	2,601242	7,33
4B, 14m - 5 zdi	3,92	1,425*	2,6725	14,85907	2,655
5B, 18,5m - 7 zdi	0,5165*	5,58	3,04825	22,45367	0
6B, 17m - 5 zdi	0,5445*	4,375	2,45975	16,42737	3,805

* Nespolehlivé měření – rozdílnost propustnosti překročila 10%.

Následující graf ukazuje rozptřeni odchylky získané porovnáním naměřených hodnot propustnosti. Z grafu je patrný rostoucí trend zejména u měření získaných z NB (proloženo spojnicí trendu). Procentuální porovnávání dvou naměřených hodnot přináší větší odchylky v případě nižších hodnot naměřené propustnosti, což se ukázalo být vhodným způsobem porovnávání z důvodu přehlednosti. Při měření tak snadno dojde k odhalení místa s nízkou propustností pravděpodobně nedostačující pro reálné používání sítě. Pokud by hodnoty byly porovnávány například střední kvadratickou chybou aritmetického průměru, měření s nižší hodnotou propustnosti by naopak ukazovalo chybu nižší a odhalení takového místa by nebylo možné.



Obrázek 23 – Porovnání rozdílů naměřených propustností

5.3 Experiment 2 – typické umístění AP

Druhý experiment se zabýval typickým umístěním AP zhruba ve středu bytu s tím, že AP bylo umístěno v blízkosti vývodu telefonní zásuvky přivádějící internetové připojení. To je místo, které by z důvodu jednoduchého zapojení pravděpodobně využila většina uživatelů. AP bylo umístěno na polici, která byla oproti stolu asi o 70 cm výše. Protože se jedná o reálné zapojení, ve kterém se pohybují uživatelé s chytrými telefony, je v experimentu provedeno měření propustnosti pomocí SP, a to na všech umístěních. Výsledky SP však nejsou zahrnuty do průměrné hodnoty propustnosti, a je tak umístěn ve zvláštní kategorii. Naměřené výsledky zobrazují následující tabulky.

Tabulka 9 – Naměřené hodnoty propustnosti experimentu 2

Umístění	Experiment 2 (Mbps)				
	NB	N7	Průměr	Průměrné rozdíly (%)	SP
1A, 3,5m - 2 zdi	18,2	19,35	18,775	4,207921	18
2A, 3,5m - 1 zed'	19,25	20,5	19,875	2,215504	19,75
3A, 5,5m - 2 zdi	14,3	19,65	16,975	5,256765	17,4
4A, 4m - 1 zed'	20,05	20,55	20,3	0,985293	19,3
5A, 1,5m - 0 zdí	19,85	20,2	20,025	0,743867	19,7
6A, 3,5m - 1 zed'	19,6	20,95	20,275	1,218515	19,25
7A, 5m - 1 zed'	19,4	20,3	19,85	0,490196	19,45

Umístění	NB	N7	Průměr	Průměrné rozdíly (%)	SP
8A, 3,5m - 0 zdí	19,75	20,2	19,975	0,252525	20,2
1B, 9m - 2 dveře	17,95	20,15	19,05	0,525303	19,95
2B, 9m - 4 zdi	15,6	16,15	15,875	1,557188	9,02
3B, 7m - 3 zdi	13,65	16,05	14,85	3,502048	17,8
4B, 8m - 3 zdi	13,65	12,15	12,9	3,81469	9,65
5B, 14,5m - 4 zdi	9,45	17,45	13,45	0,285714	4,185*
6B, 12m - 4 zdi	8,49	14,75	11,62	1,475645	9,34*

* Nespolehlivé měření – rozdílnost propustnosti překročila 10%.

Měření druhého experimentu nezaznamenalo žádné chybové přenosy, a síť tak byla použitelná na všech místech. Jediný problém nastal při měření propustnosti pomocí N7 na lokaci 3B, kde naměřené propustnosti značně kolísaly (7,42; 5,22; 12,1; 3,38 Mbps). Podle pokynů zmíněných v definici metodiky bylo zařízení o pár centimetrů přesunuto a následující měření už ukázalo shodující se hodnoty 16 a 16,1 Mbps.

Nižší hodnoty propustnosti v místech s horší úrovní signálu zaznamenal především SP, což je vzhledem k rozměrům jeho antény očekávatelný výsledek. V ostatních případech však jeho měření poměrně přesně korespondovalo s hodnotami ostatních zařízení. Experiment byl na závěr ověřen měřením UDP propustnosti na dvou místech.

Tabulka 10 – Naměřené hodnoty propustnosti experimentu 2

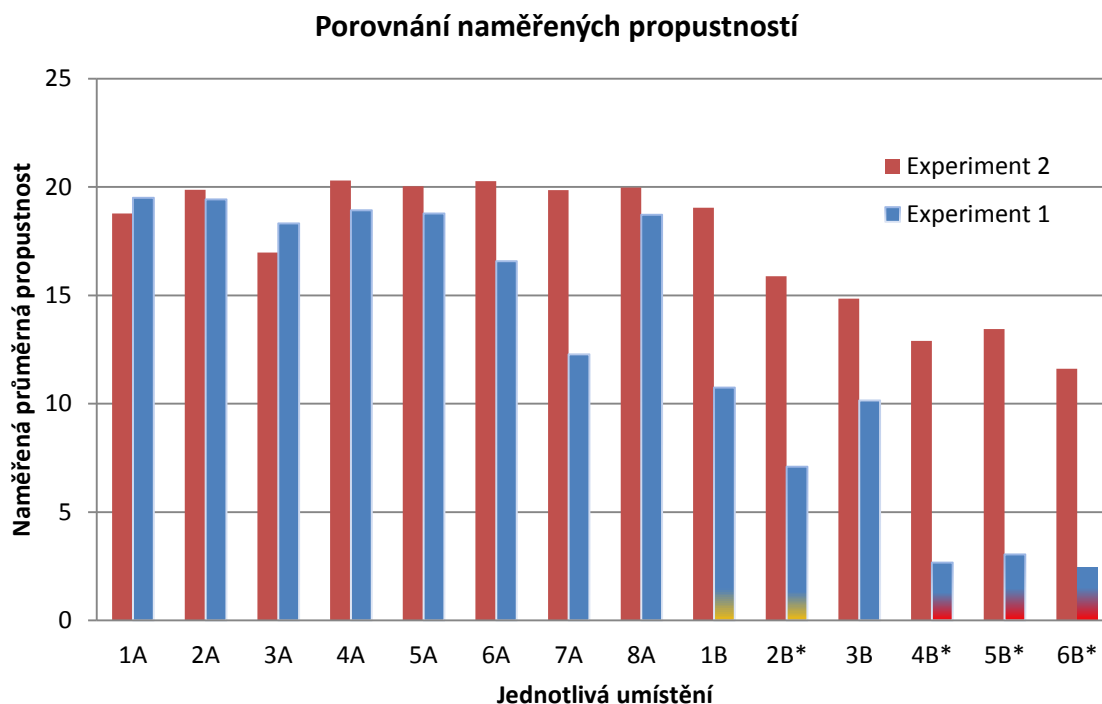
UDP ověření		
	1A	1B
NB_1	22,3	22,9
NB_2	21,9	22,5
Průměr	22,1	22,7
Rozdíl (%)	1,793722	1,746725

UDP ukazuje propustnost větší o 15, respektive 16%, což je sice zhruba o polovinu méně, než ukazovaly výsledky v ověřování metodik, ale stále se jedná o hodnotu potvrzující platnost naměřených hodnot propustností.

5.4 Analýza výsledků

Prezentované výsledky prokazatelně ukazují značný vliv umístění AP na výslednou propustnost v rámci určitého prostředí. Celková průměrná propustnost prvního experimentu byla 11,9 Mbps, zatímco druhého 17 Mbps (bez uvažování SP). V tomto shrnutí však není zahrnut nejdůležitější fakt, kterým je spolehlivost jednotlivých přenosů. V prvním experimentu byl přenos nespolehlivý na pěti místech v bytě B, přičemž tři místa ukazovala tak nízké hodnoty propustnosti, které by v podstatě znemožňovaly používání sítě. Dá se tedy říci, že pohodlné používání sítě v bytě B by až na výjimečná místa možné nebylo. I v bytě A by však při takto nevhodně umístěném AP došlo ke snížení

propustnosti, a to z hodnoty 19,5 na 17,8 Mbps, což však není příliš výrazná změna. Propustnost jednotlivých experimentů shrnuje následující graf. Opět jsou barevně označeny experimenty s chybovostí (oranžová barva), respektive se silnou chybovostí (červená barva).



Obrázek 24 – Graf porovnání naměřených propustností

6 Porovnání metodiky

V této kapitole bude metodika komplexního měření propustnosti v reálném prostředí porovnána s metodikami zmíněnými ve třetí kapitole.

6.1 SWOT analýza metodiky

Provedená SWOT analýza zachycuje vlastnosti metodiky komplexního měření propustnosti v reálném prostředí.

Silné stránky	Slabé stránky
<ul style="list-style-type: none">• Přesné výsledky.• Výsledky odrážející kategorie určitých specifických zařízení (SP, tablet).• Provedení experimentu na nejméně zarušeném kanálu.• Možnost volby měření v textovém režimu (<i>Iperf</i>) či grafickém (<i>Jperf</i>).• Možnost ověření výsledků měřením UDP propustnosti.• Označení nespolehlivého měření, chybového a silně chybového spojení.	<ul style="list-style-type: none">• Delší doba provádění experimentu.• Složitější provádění měření v případě míst s proměnlivou propustností (horší úroveň signálu, rušení jiných sítí).
Příležitosti	Hrozby
<ul style="list-style-type: none">• Možnost měření mezi různými OS.• Detekce potenciálně problémových míst.	<ul style="list-style-type: none">• Možnost ovlivnění výsledků nevhodným HW – nutnost ověření před experimentem.

6.2 Komparativní analýza s ostatními metodami

Tato část porovnává vlastnosti autorovy metodiky se zmíněnými metodami pro měření propustnosti a dostupné kapacity.

Metoda šíření signálu

Lo ve své metodě provedl podrobné měření propustnosti standardu 802.11g v konkrétním prostředí na více než dvaceti místech pro každý experiment. Jeho metoda však měřila propustnost přes dva bezdrátové spoje, což neodpovídá typickému použití bezdrátové sítě. Dva bezdrátové spoje odpovídají přenosu mezi dvěma zařízeními, kde přenos probíhá přes AP. Toto schéma je použitelné pouze v domácích či komerčních sítích, kde může probíhat přenos dat mezi dvěma uživateli, či mezi uživatelem a například tiskárnou. V klasickém schématu sítě jako veřejného hotspotu (například v restauracích, školách, hotelech, ...) mezi sebou zařízení spojení nemají, a jediný přístup tak mají k internetu. I v domácích podmínkách však pravděpodobně bude naprostá většina datového přenosu směřována do nebo z internetu, a tedy bude odpovídat jednomu bezdrátovému spoji, který byl právě z těchto důvodů použit v autorem navržené metodice.

Další výraznou vlastností experimentu je použití pouze nativního softwaru pro měření propustnosti. To sice zjednodušuje provádění experimentu, nicméně přesnost metody

nebude nikdy tak vysoká jako za použití specializovaného softwaru, jakým je například mnou použitý *Iperf*, respektive *Jperf*.

Metoda šíření signálu však jako jediná z popsaných metod uvažovala vliv Fresnelovy zóny na propustnost a Lo vypočítal, že při umístění všech zařízení alespoň metr nad zemí, její účinky nebudou experiment ovlivňovat do vzdálenosti 33 metrů. Toto opatření je v metodice implementováno.

Metoda packet-by-packet

Největší nevýhodou této metody je v použití dnes již zastaralého standardu 802.11b, kvůli kterému byly pro přenos použity pouze malé soubory, které mohly zkreslit výsledky měření TCP propustnosti. Pro eliminaci tohoto problému je v autorově metodice použit minutový přenos dat, který je prováděn vždy minimálně dvakrát pro každé umístění. Zapojení statického klienta přes rozbočovač připojený k internetu mohl výsledky dále ovlivnit. Statický klient zapojený v autorově metodice je připojen přímo k AP, které není připojeno k internetu.

Metoda „packet-by-packet“ však vyniká vysokou přesností danou použitím dvou klientských adaptérů, měřením třemi odlišnými nástroji a uvažováním vlivu orientace klienta. V autorově metodice není nic z toho aplikováno z následujících důvodů. Použití různých adaptérů simuluje využití více zařízení s výhodou snazšího provádění a více vypovídající hodnoty (jiný OS a konstrukce zařízení). Měření třemi nástroji zvyšuje náročnost provádění experimentu a způsobuje delší provádění experimentu, které může způsobit nekonzistentnost výsledků. Nástroj *Iperf* dokáže měřit propustnost obou transportních protokolů, a proto ho lze použít pro měření UDP propustnosti na místo použitého *LANFider*. Vliv orientace klienta je v nově navržené metodice záměrně zanedbán z důvodu, že při ověřování předpokladů metodik se tento vliv neprojevil, respektive jeho vliv je zanedbatelný v porovnání s nepatrným posunutím dynamického klienta či AP.

Metody měření dostupné kapacity

Ověřením předpokladů bylo zjištěno, že tyto metody dokáží změřit podobné hodnoty jako metody pro měření propustnosti. Nevýhodou však je komplexnost, jakou tuto kapacitu měří, což v praxi znamená nutnost provedení většího množství experimentů, při kterých stejně není zaručeno zjištění maximální hodnoty kapacity, protože určitý provoz může měření ovlivnit. Tyto metody mají velký potenciál ve zjišťování dostupné kapacity při přítomném provozu, ale při provozu nulovém je jejich použití zbytečné. Experiment, který provedl Bredel a Fidler (2008), byl navíc proveden ve stíněné komoře, což sice zvyšuje přesnost měření, ale získaná data neodpovídají reálnému prostředí a experiment neumožňuje měření ve větších vzdálenostech.

Vliv rádiového rušení na propustnost

Tato metoda zkoumá pouze vliv ostatních zařízení pracujících na stejných frekvencích jako bezdrátové sítě na propustnost a nejedná se tedy o typickou metodu měření propustnosti. Vliv ostatních zařízení je v autorově metodice zahrnut automaticky z důvodu měření v reálném prostředí. Tato zařízení však nejsou známá a priori, a v případě podezření na silné rušení, například mikrovlnou troubou v blízkosti, by bylo vhodné tento vliv dále prozkoumat právě metodou vlivu rádiového rušení na propustnost.

Měření propustnosti více toků

Měření propustnosti více toků je další specifické měření, které potvrdilo téměř rovnoměrné rozložení dostupné propustnosti mezi připojené klienty. Z tohoto důvodu nebylo v navržené metodice dále zkoumáno. Pokud by v měřené síti byly zvláštní nároky na počet připojených uživatelů či kvalitu jejich spojení, bylo by vhodné provést měření propustnosti více toků pro všechny tyto klienty.

Závěr analýzy

Metodika komplexního měření propustnosti v reálném prostředí je zaměřena na typické měření propustnosti, a to mezi jedním či volitelně více různými zařízeními, a je tedy možné ji srovnávat se třemi prvně zmíněnými metodami měření propustnosti. Z provedené analýzy je zřejmé, že navržená metodika má potenciál se vyrovnat provedeným experimentům ze zmíněných metod a předčit je v mnoha ohledech, jakými je měření různými zařízeními včetně specifických, uvažování míst s potenciálně proměnlivou propustností a velkou variabilitou měření. To lze provádět oběma transportními protokoly, mezi zařízeními s různými OS a také dvěma různými způsoby – textovým a grafickým.

Metodika komplexního měření propustnosti v reálném prostředí si však na druhou stranu neklade za cíl prověřovat specifické aspekty, jakým je rušení ostatních zařízení, či propustnost více toků, a s těmito metodami ji tedy porovnávat nelze.

Závěr

Cílem této práce bylo vytvořit a prakticky ověřit metodiku pro měření propustnosti bezdrátových sítí standardu IEEE 802.11, která by byla vytvořena na základě nedostatků existujících metod pro měření propustnosti bezdrátových sítí. Práce je uspořádána podle postupu, jakým byla metodika navrhována.

V úvodní části práce byl postaven teoretický základ měření výkonnostních parametrů sítě, byla provedena rešerše existujících metod a popsány základní veličiny používané při měření. Byly uvedeny základní typy měření propustnosti: analytické modelování, počítačová simulace a experimentální měření. První dva typy byly pro potřeby práce vyloučeny, protože se ukázaly jako ideální pro měření v ideálních podmínkách, ovšem nevhodné pro měření v reálném prostředí. Experimentální měření bylo určeno jako jediný způsob měření v reálném prostředí, a proto se jím práce dále zabývala. Následně byly popsány metody měření propustnosti experimentálním měřením včetně metod pro měření dostupné kapacity, které mohou být pro měření propustnosti také použity, což později dokázalo experimentální měření. Na základě popsaných metod bylo určeno obecné schéma experimentálního měření, které bylo později rozšířeno a použito v navržené metodice. Popsané metody byly detailně rozebrány ve třetí kapitole, kde byly popsány jejich implementační detaily, schémata měření a SWOT analýzy. Právě SWOT analýza poskytla nástroj pro názorné odhalení nedostatků jednotlivých metod, které mohly být shrnuty v následující kapitole.

Návrh vlastní metodiky byl popsán ve čtvrté kapitole. Nejprve byl vytvořen matematický model teoretické maximální propustnosti bezdrátové sítě, s kterým mohly být porovnávány naměřené hodnoty. Na základě nedostatků zmíněných metod byly provedenou analýzou určeny vlastnosti, které se staly základem pro vytvoření nové metodiky. Té byl určen konkrétní SW, a to *Iperf* (volitelně *Jperf*), a to hlavně z důvodu jeho multiplatformnosti, jednoduchosti použití a spolehlivosti. Pro provádění experimentu byl zvolen konkrétní HW, který byl složen z různých zařízení obsahujících odlišné operační systémy. Těmito nástroji mohly být ověřeny předpoklady zmíněných metod pro měření propustnosti.

Ověření těchto předpokladů bylo posledním krokem před finálním navržením metodiky. Nejprve bylo ověřeno, že výkon použitých zařízení nebude negativně ovlivňovat měření, a že měření propustnosti lze také provádět dnes průměrným tabletem, což práci značně usnadňuje. Další vlastností byla minimální délka bezdrátového spoje, kterou Lo stanovil na jeden metr. Snížení této vzdálenosti o polovinu způsobilo značný pokles propustnosti, a proto je v metodice tato vzdálenost uvedena jako minimální doporučená. Naopak vliv orientace NB nebo AP, který uvažovali Na, Chen a Rappaport (2006) se nijak zásadně neprojevil a dodatečné měření minimálního posunutí AP potvrdilo, že nepatrné změny propustnosti jsou způsobeny spíše změnou umístění než orientací antén. Negativní vliv šifrování na výkon, který uváděl Lo, se v dnešním HW také neprojevil, a metodika tak byla prováděna se zapnutým šifrováním. Další experiment zkoumal propustnost sítě při jednom a dvou bezdrátových spojkách a potvrdil, že při dvou spojkách klesne propustnost o více než

polovinu. Z tohoto důvodu je v metodice používán právě jeden přenos, který je zvolen hlavně kvůli faktu, že většina přenosu dat v bezdrátových sítích je realizována mezi zařízením a internetem, a tedy prochází pouze přes jeden bezdrátový přenos. Další experimenty prokázaly proměnlivost bezdrátového média, kvůli které je nutné provést měření co nejrychleji, vliv ostatních bezdrátových sítí na propustnost, a to zejména v případě aktivního vysílání ostatní sítě a vliv velikosti paketu na propustnost, který odpovídal matematickému modelu. Poslední experiment porovnal propustnost měřenou protokoly TCP a UDP a zjistil, že režie a způsob fungování TCP protokolu způsobuje snížení propustnosti zhruba o třetinu oproti UDP.

Metodika bere v úvahu vliv ostatních sítí, a proto vyžaduje před provedením experimentu skenování okolních sítí a volby nejméně zaručeného kanálu. Samotná metodika je pak složena ze dvou částí. Ze základního měření, které cílí na jednoduché použití a rychlé provedení experimentu, a volitelného měření, kde za pomoci více zařízení dochází k upřesnění výsledků zmírněním dopadů proměnlivosti bezdrátového média způsobené dočasným rušením ostatními sítěmi a vícecestným šířením signálu. Volitelné měření také umožňuje provést měření propustnosti zařízeními spadajícími do specifických kategorií, jako například zařízení s nízkým výkonem. Ty nejsou zahrnuty do celkového průměru, ale mají svoji vlastní kategorii. Typické použití této vlastnosti by mohlo být v implementaci bezdrátové sítě v restauraci, kde si budou hosté objednávat jídlo pomocí chytrých telefonů, a proto je potřeba zjistit hodnoty propustnosti právě pro tato zařízení.

Spolehlivost naměřené propustnosti je zaručena provedením dvojice po sobě jdoucích měření, které jsou označeny jako platné, pouze pokud se jejich průměrné hodnoty propustnosti neliší o více než deset procent. Pokud je navíc v přenosu dat zachycen výpadek spojení, je přenos podle závažnosti výpadku označen jako chybový či silně chybový. Po provedení měření na všech místech je možné měření ověřit doplňkovým měřením UDP propustnosti na vybraných místech. Tím jsou potvrzeny naměřené hodnoty a navíc je prozkoumána i UDP propustnost.

Metodika byla prakticky ověřena na experimentu provedeném ve dvou sousedících bytech v cihlovém domě. Toto prostředí poskytovalo dostatečný prostor pro ověření šíření signálu a věrohodnost reálného prostředí plného ostatních bezdrátových sítí. Experiment byl rozdělen na dvě části, z nichž v jedné byl AP záměrně umístěn nevhodně, tak aby metodika mohla být prověřena i pro hodnoty s nízkou propustností. Ve druhé části experimentu byl pak AP umístěn tak, aby pokryl oba byty. Z výsledků je patrné, že metodika je schopna určit hodnoty propustnosti pro konkrétní místa a spolehlivě určit oblasti se slabým signálem a nízkou hodnotou propustnosti, která je potom názorně zobrazena.

Další prověření metodiky by umožňoval experiment provedený novějším standardem 802.11n, který disponuje komplikovanější technologií fyzické vrstvy a umožňuje využít vícecestného šíření signálu pro dosažení vyšší hodnoty SNR.

Literatura

ALLMAN, M., V. PAXSON a W. STEVENS, 1999. *RFC 2581: TCP Congestion Control*. [Online]. April 1999 [cit. 6. 2. 2014]. Dostupné z: <http://www.ietf.org/rfc/rfc2581.txt>

BANERJI, Sourangsu a Rahul Singha CHOWDHURY, 2013. Wi-Fi & WiMAX: A Comparative Study. In: *Indian Journal of Engineering*. Vol. 2, iss. 5. arXiv: 1302.2247. Dostupné z: <http://arxiv.org/ftp/arxiv/papers/1302/1302.2247.pdf>

BARBOSA, Alex V., Marcos F. CAETANO a Jacir L. BORDIM, 2011. The Theoretical Maximum Throughput Calculation for the IEEE802.11g Standard. In: *IJCSNS International 136 Journal of Computer Science and Network Security*. April 2011, vol. 11, no. 4, pp. 136-143. ISBN 978-0-7695-4277-5.

BREDEL, Michael a Markus FIDLER. A Measurement Study of Bandwidth Estimation in IEEE 802.11g Wireless LANs Using the DCF, 2008. In: *Proceeding NETWORKING'08 Proceedings of the 7th international IFIP-TC6 networking conference on AdHoc and sensor networks, wireless networks, next generation internet*. Berlin, pp. 314-325. ISBN 3-540-79548-0.

CAIDA, 2014. Performance Tools Taxonomy. *The Cooperative Association for Internet Data Analysis*[Online]. 10. 1. 2014 [cit. 23. 2. 2014]. Dostupné z: <http://www.caida.org/tools/taxonomy/perftaxonomy.xml>

CISCO, 2009. Key Performance Benefits of 802.11n. *Cisco*[Online]. [cit. 21. 11. 2013]. Dostupné z: http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_c11-513840.html

CISCO, 2012. 802.11ac: The Fifth Generation of Wi-Fi Technical White Paper. *Cisco* [Online]. August 2012 [cit. 27. 11. 2013]. Dostupné z: http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps11983/white_paper_c11-713103.html

Dirac Delta, 2005. Signal to Noise Ratio. *DiracDelta science and engineering encyclopedia* [Online]. May 25, 2005 [cit. 20. 2. 2014]. Dostupné z: <http://www.diracdelta.co.uk/science/source/s/i/signal%20to%20noise%20ratio/source.html#.UwXtxfl5OgY>

DOVROLIS, Constantine, 2003. Pathload tutorial. *Georgia College of Tech Computing* [Online]. April, 2003 [cit. 10. 4. 2014]. Dostupné z: http://www.cc.gatech.edu/fac/Constantinos.Dovrolis/bw-est/pathload_tutorial.html

EKPENYONG, Moses a Joseph ISABONA, 2010. Modeling Throughput Performance in 802.11 WLAN. In: *IJCSI International Journal of Computer Science Issues*. May 2010, vol. 7, iss. 3, no. 11 pp. 16-22. ISSN (online) 1694-0784. ISSN (print) 1694-0814.

- FLUKE NETWORKS, 2008. 802.11n Primer. *AirMagnet - Fluke Networks* [Online]. August 5, 2008 [cit: 7. 3. 2014]. Dostupné z: <http://airmagnet.flukenetworks.com/assets/whitepaper/WP-802.11nPrimer.pdf>
- GAST, Matthew, 2003. When Is 54 Not Equal to 54? A Look at 802.11a, b, and g Throughput. *O'Reilly Wireless Devcenter* [Online]. August 14, 2003 [cit. 28. 2. 2014]. Dostupné z: http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html.
- GAST, Matthew, 2005. *802.11 Wireless Networks: The Definitive Guide, Second Edition*. 2. vyd. Sebastopol: O'Reilly. [Elektronické vydání]. ISBN 0-596-10052-3.
- GEIER, Jim, 2003. Infrared WLAN. *Wi-Fi Planet* [Online]. March 17, 2003 [cit. 1. 2. 2014]. Dostupné z: <http://www.wi-fiplanet.com/tutorials/article.php/2110301>
- HASSAN, Mohamed, M. KRUNZ a Ibrahim MATTA, 2004. Markov-based channel characterization for tractable performance analysis in wireless packet networks. In: *IEEE Transactions on Wireless Communications*. May 2004, vol. 3, iss. 3, pp. 821– 831. ISSN 1536– 1276. DOI 10.1109/TWC.2004.827729. Dostupné z: IEEE Xplore.
- HU, Ningning a Peter STEENKISTE, 2003. Evaluation and Characterization of Available Bandwidth Probing Techniques. In: *IEEE Journal on Selected Areas in Communications*. August 4, 2003, vol. 21, iss. 6, pp. 879– 894. ISSN 0733-8716. DOI 10.1109/JSAC.2003.814505. Dostupné z: IEEE Xplore.
- HU, Ningning, 2006. *Network Monitoring and Diagnosis Based on Available Bandwidth Measurement*. Pittsburgh: Carnegie Mellon University, School of Computer Science, Computer Science Department. PhD Thesis. Dostupné také z: <http://www.cs.cmu.edu/~hnn/thesis/thesis.pdf>
- CHANG, Xinjie, 1999. Network simulations with OPNET. In: *Proceedings of the 1999 Winter Simulation Conference*. Phoenix: December 5, 1999, pp. 307-314. ISBN 0-7803-5780-9. DOI: 10.1109/WSC.1999.823089. Dostupné z: IEEE Xplore.
- IEEE Std 802.11™, 2012. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. New York: IEEE Standard, April 5, 2012, pp. 1– 2793. ISBN (online) 978-0-7381-7211-8. DOI 10.1109/IEEESTD.2012.6178212. Dostupné z: IEEE Xplore.
- IPERF, 2011. Iperf – The TCP/UDP Bandwidth Measurement Tool. *Iperf.fr* [Online]. [cit. 2. 3. 2014.]. Dostupné z: <http://iperf.fr/>.
- ITO, Seigo a Nobuo KAWAGUCHI, 2006. Data Correction Method Using Ideal Wireless LAN Model in Positioning System. In: *2006 IEEE 17th International Symposium on Personal, Indoor and Mobile Radio Communications*. Helsinki: September 2006, pp. 1– 5. ISBN 1-4244-0330-8. DOI 10.1109/PIMRC.2006.254099. Dostupné z: IEEE Xplore.

JAIN, Manish a Constantinos DOVROLIS, 2003. End-to-end available bandwidth: measurement methodology, dynamics, and relation with TCP throughput. In: *IEEE/ACM Transactions on Networking*. August 2003, vol. 11, iss. 4, pp. 537– 549. ISSN 1063-6692. DOI 10.1109/TNET.2003.815304. Dostupné z: IEEE Xplore.

JOHNSSON, Andreas, Bob MELANDER a Mats BJORKMAN, 2006. Bandwidth Measurement in Wireless Networks. In: *End-to-End Monitoring Techniques and Services, 2006 4th IEEE/IFIP Workshop on*. Vancouver: April 3, 2006, pp. 74– 81. ISBN 1-4244-0145-3. DOI 10.1109/E2EMON.2006.1651282. Dostupné z: IEEE Xplore.

JUN, Jangeun, Pushkin PEDDABACHAGARI, a Mihail SICHITIU, 2003. Theoretical Maximum Throughput of IEEE 802.11 and its Applications. In: *Network Computing and Applications*. Cambridge: April 18, 2003, pp. 249– 256. ISBN 0-7695-1938-5. DOI 10.1109/NCA.2003.1201163. Dostupné z: IEEE Xplore.

KONRAD, Almudena, a další, 2003. A Markov-Based Channel Model Algorithm for Wireless Networks. In: *Wireless Networks*. New York: Springer US, May 2003, vol. 9, iss. 3, pp. 189– 199. ISSN (print) 1022-0038. ISSN (online) 1572-8196. DOI 10.1023/A:1022869025953. Dostupné z: Springer.

LESKAROSKI, D. a W.B. MIKHAEL, 2002. Frequency Planning and Adjacent Channel Interference in a DSSS Wireless Local Area Network (WLAN). In: *Wireless Personal Communications. The International Series in Engineering and Computer Science*. New York: Springer US, vol. 592, pp. 169– 180. ISBN (online) 978-0-306-46986-2. ISBN (print) 978-0-7923-7214-1. DOI 10.1007/0-306-46986-3_16. Dostupné z: Springer.

LEUTERT, Rolf, 2009. Inside 802.11n Technical Details About the New WLAN Standard. Wire Shark [Online]. March 2009 [cit. 6. 3. 2014]. Dostupné z: http://www.wireshark.ch/download/Cisco_PSE_Day_2009.pdf

LIM, Hyuk, a další, 2006. Zero-Configuration, Robust Indoor Localization: Theory and Experimentation. In: *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*. Barcelona, Spain: April 2006, pp. 1– 12. ISSN 0743-166X. ISBN (print) 1-4244-0221-2. DOI 10.1109/INFOCOM.2006.223. Dostupné z: IEEE Xplore.

LO, Eric Cheng-Chung, 2007. *An Investigation of the Impact of Signal Strength on Wi-Fi Link Throughput through Propagation Measurement*. Auckland, Auckland University of Technology, School of Computing and Mathematical Sciences. PhD Thesis. Dostupné také z: <http://aut.researchgateway.ac.nz/bitstream/handle/10292/698/LoE.pdf?sequence=1>

MYCLE, Dino, 2011. Difference between RSSI and RSS or RSS vs RSSI. *Technical blog* [Online]. April 20, 2011 [cit. 1. 3. 2014]. Dostupné z: <http://dinomycle.blogspot.cz/2011/04/difference-between-rssi-and-rss.html>

NA, Chen, Jeremy K. CHEN a Theodore S. RAPPAPORT, 2006. Measured Traffic Statistics and Throughput of IEEE 802.11b Public WLAN Hotspots with Three Different Applications. In: *IEEE Transactions on Wireless Communications*. November 2006, vol. 5, no. 11, pp. 3296-3305. ISSN 1536-1276. DOI 10.1109/TWC.2006.05043. Dostupné z: IEEE Xplore.

NEGUS, Kevin J. a Al PETRICK, 2008. History of Wireless Local Area Networks (WLANs) in the Unlicensed Bands. In: *George Mason University Law School Conference*. Arlington: April 4, 2008. Dostupné z: http://iep.gmu.edu/wp-content/uploads/2009/08/WLAN_History_Paper.pdf

Nordic Semiconductor, 2012. A short history of spread spectrum. *EE Times* [Online]. January 26, 2012 [cit. 11. 2. 2014]. Dostupné z: http://www.eetimes.com/document.asp?doc_id=1279374

ODOM, Wendell, 2012. *CCENT/CCNA ICND1 640-822 Official Cert Guide, Third Edition*. Indianapolis: Cisco Press, Third Printing. ISBN-13 978-1-58720-425-8.

OUELLET, Eric, a další, 2002. *Building A Cisco Wireless LAN*. Rockland: Syngress Publishing Inc. ISBN 1-928994-58-X.

PARK, Jin-A, a další, 2003. Experiments on radio interference between wireless LAN and other radio devices on a 2.4 GHz ISM band. In: *Vehicular Technology Conference. The 57th IEEE Semiannual*. Jeju, South Korea: April 2003, vol. 3, pp. 1798– 1801. ISSN 0-7803-7757-5. ISBN (print) 0-7803-7757-5. DOI 10.1109/VETECS.2003.1207133. Dostupné z: IEEE Xplore.

PELLETTA, Enrico a Hector VELAYOS, 2005. Performance measurements of the saturation throughput in IEEE 802.11 access points. In: *Third International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Network.. WIOPT 2005*. April 2005. ISBN (print) 0-7695-2267-X. DOI 10.1109/WIOPT.2005.39. Dostupné z: IEEE Xplore.

Planet3 Wireless, 2002. *Certified Wireless Network Administrator: Official Study Guide*. Georgia: Planet3 Wireless, Inc. ISBN 0-9716057-2-6.

PRASAD, Ravi, a další, 2003. Bandwidth Estimation: Metrics, Measurement Techniques, and Tools. In: *IEEE Network*. IEEE Communications Society, November–December 2003, vol. 17, iss. 6, pp. 27– 35. ISSN 0890-8044. DOI 10.1109/MNET.2003.1248658. Dostupné z: IEEE Xplore.

ROSHAN, Pejman a Jonathan LEARY, 2003. *802.11 Wireless LAN Fundamentals*. Indianapolis: Cisco Press, December 23, 2003. Pp. 312. ISBN 1-58705-077-3.

ROSS, Sheldon M., 1996. *Stochastic processes*. 2nd. ed. místo neznámé: Elm Street Publishing Services. ISBN 0-471-12062-6.

SEXTON, Graham, 2012. *Wireless Computer Network Technology Lectures*. Newcastle upon Tyne: Northumbria University, 2012. Série přednášek.

Stephen MCCAN a Alex ASHLEY, 2013. IN PROCESS - Standards, Amendments, and Recommended Practices. *OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES - 2013-11-15* [Online]. November 15, 2013 [cit. 27. 11. 2013]. Dostupné z: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

STRAUSS, Jacob, Dina KATABI a Frans KAASHOEK, 2003. A Measurement Study of Available Bandwidth Estimation Tools. In: *IMC 2003*. Florida: ACM Press, October 2003, pp. 39– 44. ISBN 1-58113-773-7.

ŠLINZ, Petr, 2012. *Problematika vysokého zatížení bezdrátových sítí standardu 802.11b/g*. Brno. Diplomová práce [Online]. Masarykova univerzita, Fakulta informatiky. [cit. 15. 3. 2014.] Dostupné z: http://is.muni.cz/th/208329/fi_m/

VALADAS, Rui T., a další, 1998. The infrared physical layer of the IEEE 802.11 standard for wireless local area networks. In: *IEEE Communications Magazine*. IEEE Communications Society, December 1998, vol. 36, iss. 12, pp. 107– 112. ISSN 0163-6804. DOI 10.1109/35.735887. Dostupné z: IEEE Xplore.

WANG, Tianlin a Hazem H. REFAI, 2005. Empirical Network Performance Analysis on IEEE 802.11g with Different Protocols and Signal to Noise Ratio Values. In: *Second IFIP International Conference on Wireless and Optical Communications Networks, 2005. WOCN 2005*. March, 2005, pp. 29– 33. ISBN 0-7803-9019-9. DOI 10.1109/WOCN.2005.1435983. Dostupné z: IEEE Xplore.

XIONG, Lixiang, 2008. *A Markov Chain Approach to IEEE 802.11 WLAN Performance Analysis*. Sydney: The University of Sydney. School of Electrical & Information Engineering. PhD. Thesis. Dostupné také z: http://folk.uio.no/paalee/referencing_publications/ref-wlanmodel-xiong-phdthesis-2008.pdf

ZANDL, Patrick, 2003. *Bezdrátové sítě WiFi Praktický průvodce*. Brno: Computer Press. ISBN 80-7226-632-2.

Seznam příloh

Příloha A – vypočítané hodnoty teoretického modelu maximální propustnosti

Příloha B – ukázka z programu *WiFi Analyzer*

Příloha C – CD s naměřenými výsledky, konfiguračním nastavením AP a konfiguračním souborem programu *Jperf*. Jednotlivé soubory jsou popsány v souboru *popis_priloh.txt*.

Příloha A – hodnoty teoretického modelu maximální propustnosti

		Velikost paketu (B)																			
		1	100	200	300	400	500	600	700	800	900	1000	1100	1200	1300	1400	1500				
Propustnost (Mbps)	OFDM 6	0,04729	2,656307	3,682365	4,226567	4,563801	4,79327	4,959515	5,0855	5,184271	5,263786	5,329177	5,383898	5,430366	5,470316	5,505029	5,535472				
	OFDM 9	0,048209	3,150309	4,667006	5,559144	6,146636	6,562768	6,872973	7,113128	7,304556	7,460719	7,590541	7,700168	7,793972	7,875149	7,946086	8,008608				
	OFDM 12	0,048683	3,473277	5,387266	6,599511	7,436154	8,048344	8,515722	8,884235	9,182253	9,428238	9,634724	9,810516	9,961985	10,09385	10,20969	10,31226				
	OFDM 18	0,049162	3,869844	6,370159	8,118653	9,410104	10,403	11,19014	11,82949	12,35908	12,80496	13,18551	13,51411	13,80073	14,05291	14,27653	14,47616				
	OFDM 24	0,049407	4,104248	7,009755	9,17478	10,8504	12,18571	13,27483	14,18009	14,94443	15,59837	16,16423	16,65867	17,09442	17,48134	17,8272	18,13821				
	OFDM 36	0,049654	4,368879	7,792123	10,54677	12,81127	14,70576	16,31408	17,6965	18,89751	19,95062	20,88155	21,71041	22,45311	23,12242	23,7287	24,28047				
	OFDM 48	0,049781	4,514545	8,252882	11,39935	14,0842	16,40207	18,42339	20,20166	21,77821	23,18554	24,4495	25,59094	26,62685	27,57121	28,43566	29,22991				
	OFDM 54	0,049821	4,56511	8,418525	11,71464	14,5662	17,05746	19,25265	21,20159	22,94351	24,50974	25,92558	27,21169	28,38514	29,46009	30,44845	31,36028				
	OFDM		6	9	12	18	24	36	48	54	PHY parametry								Časovací parametry		
	N_DPBS		24	36	48	72	96	144	192	216	Sifs								T_Preamb 16		
T_ACK		26,67	25,11	24,33	23,56	23,17	22,78	22,58	22,52	Difs								T_Sym 4			
																		T_Signal 4			
																		T_BO 67,5			

Příloha B – ukázka z programu WiFi Analyzer



Program zobrazuje stav rádiového pásma před prováděním ověřovacích experimentů.