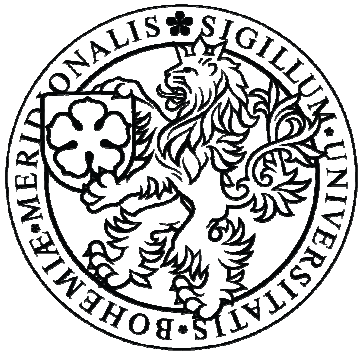
Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta



Komparativní analýza ad hoc a direct spojení v bezdrátových sítích

Bakalářská práce

Michal Lejtnar

Školitel: Ing. Rudolf Vohnout

České Budějovice 2012

Bibliografické údaje

Lejtnar M., 2012: Komparativní analýza ad hoc a Direct spojení v bezdrátových sítích. [Comparative analyse ad hoc and Direct connection at wireless networks. Bc. Thesis, in Czech.] – 29 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Bakalářská práce se zabývá porovnáním dvou druhů bezdrátového spojení typu peer-to-peer. Staršího spojení IBSS, které je známé jako ad hoc a nového spojení Wi-Fi Direct. Cílem je zjištění, zda Wi-Fi Direct může nahradit ad hoc mód. Porovnání je prováděno na základě naměřených hodnot, jako latence, síla signálu, přenosová rychlost a ztráta paketů.

Annotation

This bachelor thesis is oriented to consider two types of wireless connection known as peer-to-peer. Elderly connection IBSS which is known as ad hoc and new connection Wi-Fi Direct. The intention of this thesis is finding if Wi-Fi Direct can replace ad hoc mode. Comparing is performed by measured values like latency, signal strength, baud rate and packet loss.

Klíčová slova:
Ad hoc, Wi-Fi Direct, BlueTooth, parametry bezdrátových sítí

Keywords:
Ad hoc, Wi-Fi Direct, BlueTooth, parameters of wireless networks

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

V Žirovnici dne 25.4.2012

…….
Michal Lejtnar

Poděkování
Rád bych zde poděkoval panu Ing. Rudolfu Vohnoutovi za cenné rady a za celkovou pomoc při zpracování bakalářské práce. Dále bych zde rád poděkoval celé své rodině a přátelům za podporu při tvorbě práce.

Obsah

1. Úvod

1.1 Úvod do problematiky

V dnešní době se stále více používá pro tvoření sítí bezdrátová technologie, která ve velké míře nahrazuje a rozšiřuje stávající sítě tvořené pomocí kabelů. Hlavní a nespornou výhodou bezdrátových sítí je fakt, že nejsme k ničemu pevně připojeni kabely, a tak nám nic nebrání ve volném pohybu. Dalšími důležitými výhodami jsou úspora nákladů, protože není potřeba žádných kabelů, a jednoduchá rozšiřitelnost těchto sítí.

Nejrozšířenější technologie je Wi-Fi, která se používá pro vytváření bezdrátových lokálních sítí a tzv. hotspotů pro připojení k internetu. Pod tímto názvem se ukrývá standard IEEE 802.11, který specifikuje způsob, jakým počítače využívají tuto technologii.

V IEEE 802.11 sítích existují dvě různé topologie. Prvním typem je infrastrukturní síť, která používá přístupový bod k připojení jednotlivých zařízení. Druhým typem spojení je ad hoc síť, která pro spojení dvou nebo více počítačů nepotřebuje žádné další zařízení, protože tyto počítače spolu dokážou komunikovat přímo. Tato bakalářská práce pojednává právě o tomto typu spojení a o jeho novém, možném nástupci, který se nazývá
Wi-Fi Direct.

Nejprve něco málo o ad hoc typu spojení. Ad hoc se také jinak nazývá zkratkou IBSS, což znamená, že není závislé na žádném dalším zařízení. Tento typ spojení je možné použít jen na malé vzdálenosti, řádově několik desítek metrů. Proto je tato technologie málo využívaná.

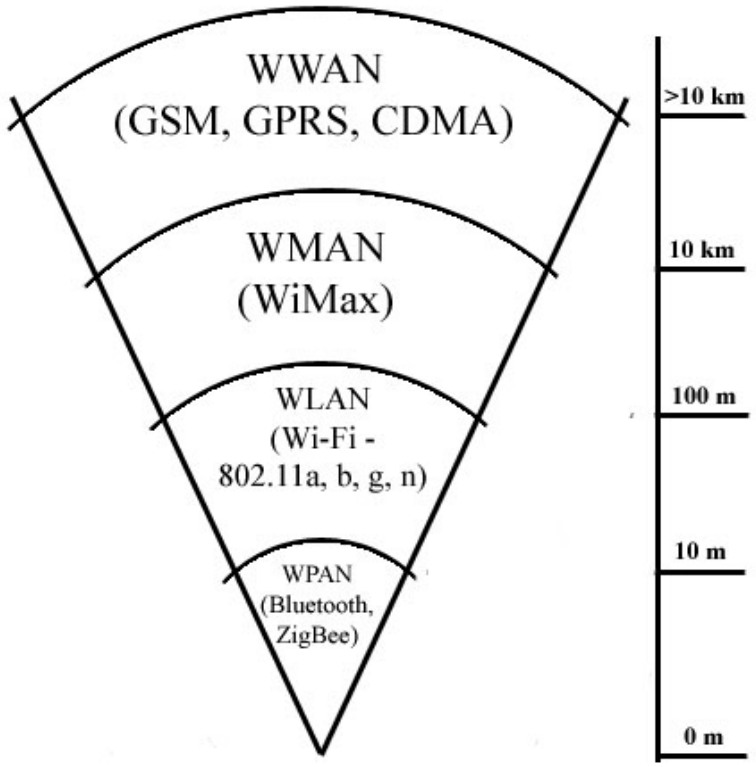
Wi-Fi Direct je novější způsob spojení jednotlivých zařízení bez přítomnosti přístupového bodu a možný nástupce ad hoc spojení. V současnosti probíhá certifikace zařízení, která budou podporovat právě toto nové peer-to-peer spojení. Tento proces probíhá pod taktovkou Wi-Fi Alliance.

1.2 Cíle práce

Hlavním cílem této bakalářské práce je potvrzení nebo vyvrácení hypotézy nahrazení spojení Wi-Fi ad hoc technologií Wi-Fi Direct. Vedlejším cílem práce je stanovení kritérií pro provedení komparace a následné doporučení pro nasazení technologie Wi-Fi Direct jako celku.

2. Struktura bezdrátové sítě

Dělení bezdrátových datových sítí se nejčastěji provádí v závislosti na geografické rozloze, na které jsou tyto technologie používány. Hlavním kritériem tohoto rozdělení je tedy dosah signálu u jednotlivých technologií, které jsou ve značné míře normalizovány institutem IEEE. Bezdrátové sítě jsou nejčastěji rozděleny do čtyř skupin, a to WPAN, WLAN, WMAN a WWAN. Na následujícím obrázku můžeme vidět zástupce těchto skupin i s přibližnými vzdálenostmi, kterých dosahují.



Obrázek 1: Dosah sítí

Z výše uvedený druhů sítí nás nejvíce zajímá Wi-Fi, které poskytuje svobodné připojení uživatelů k síti či internetu z jakéhokoli místa doma, v práci nebo na ulici. Wi-Fi pracuje ve volném frekvenčním spektru, což znamená, že pro komunikaci na této frekvenci nepotřebujeme žádnou licenci. Volné části radiového spektra, které používá tento standard, jsou pásma 2,4 GHz a 5 GHz.[5] V České republice je ovšem provoz v pásmu 5 GHz omezen

pouze na vnitřní prostory, stejně jako v celé Evropské unii, a proto se používají pouze některé standardy IEEE 802.11. Následující tabulka zobrazuje několik nejznámějších standardů.

Standard	Rok vydání	Pásmo (GHz)	Maximální teoretická rychlost (Mbit/s)	Použité kódování
původní IEEE 802.11	1997	2,4	2	DSSS/FHSS/IrDa
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM/DSSS
IEEE 802.11n	2009	2,4 nebo 5	600	MIMO-OFDM

Tabulka 1: Přehled standardů IEEE 802.11
Zdroj: [14]

2.1 Topologie sítě

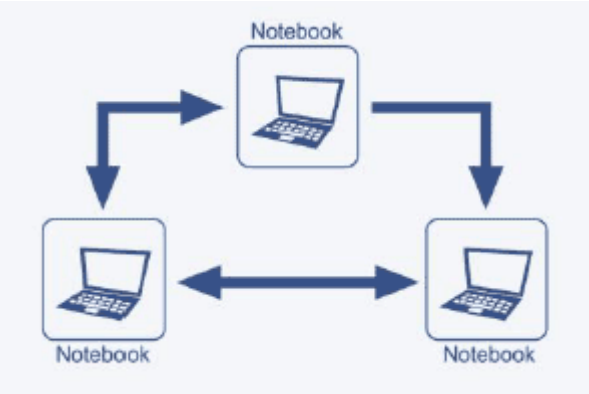
Bezdrátová síť Wi-Fi může být vybudována různými způsoby podle potřeb uživatelů nebo podle požadovaných funkcí. Základní stavební blok Wi-Fi sítí je tzv. BSS (Basic Service Set), což je něco jako základní soubor služeb. Jedná se o množinu stanic, které spolu komunikují v určité oblasti, která se nazývá BSA (Basic Service Area). Velikost této oblasti je závislá na dosahu signálu jednotlivých členů BSS. Podle toho, jak probíhá komunikace mezi jednotlivými členy BSS, rozlišujeme dvě různé topologie Wi-Fi sítí, které se liší v určitých parametrech, jako je dosah signálu a nutnost použití dalšího zařízení.

Prvním typem je infrastrukturní síť, která je nejvíce používaná hlavně pro tvorbu malých domácích nebo firemních sítí. Tento typ spojení používá tzv. hvězdicovou topologii. Pro vytvoření takové sítě je zapotřebí přístupový bod (AP), který zprostředkovává komunikaci mezi jednotlivými stanicemi a zároveň tvoří bránu pro přístup na internet. Z toho tedy vyplývá, že veškerá komunikace probíhající mezi zařízeními musí projít právě přes toto zařízení. Díky tomu je možné komunikovat na delší vzdálenost, protože dvě stanice, které spolu komunikují, na sebe nemusí vůbec vidět. Nespornou výhodou je také jednoduchost nastavení takové sítě, protože zde stačí řádně nastavit pouze jedno zařízení, již zmiňovaný přístupový bod.

Ovšem druhý typ spojení, který se nazývá ad hoc, nepotřebuje žádné další zařízení. Zde se spojují přímo koncová zařízení mezi sebou. Toto přímé spojení dokáže vytvořit také novinka Wi-Fi Direct, která nejspíše nahradí zmiňované ad hoc spojení, ale o tom už pojednávají samostatné kapitoly.

3. Ad hoc síť

Ad hoc síť sestává pouze z jednotlivých počítačů propojených bezdrátovým způsobem. Na této bezdrátové síti není k dispozici žádný přístupový bod (AP), který by ji řídil a poskytoval by další služby, jako například DHCP, firewall, přístup na internet nebo zdokonalené zabezpečení. Na druhé straně je ad hoc síť možno zřídit všude, kde jsou alespoň dva počítače s wi-fi adaptéry.[4] Toto spojení je typu peer-to-peer, což znamená, že jsou si všechny připojené počítače rovné viz. obr. 2. Ačkoliv se při vytváření sítě zakládající počítač tváří jako server, tak po připojení už probíhá komunikace přímo mezi jednotlivými stanicemi.



Obrázek 2: Ad hoc síť
Zdroj: [9]

Síť ad hoc se nepoužívá pro trvalé vytváření sítí, jako je tomu například u domácích sítí tvořených za pomoci dalšího zařízení, převážně AP. Právě naopak, tato síť je tvořena pouze na krátkou dobu, nezbytně nutnou pro splnění svého účelu (např. přenos dat), a pak je spojení ukončeno. Tato síť je využívána převážně k hraní her, sdílení souborů nebo k provozování jiných síťových aplikací či komunikace, případně pro dočasné sdílení připojení k internetu. Ad hoc mód je předurčen pro místa, kde je malé množství počítačů v malé vzdálenosti od sebe. Sítě ad hoc nedoznaly větší obliby nejenom proto, že nemohou být příliš rozlehlé, ale také proto, že jsou omezené počtem připojených počítačů. Čím víc zařízení je připojeno k síti, tím horší je výkonnost sítě. Navíc jejich nárazové vytvoření vyžaduje správné nakonfigurování sítě, což ne každý laický uživatel zvládne. Proto je pro mnoho lidí jednodušší si data vyměnit na CD, flash disku, nebo se připojit přes přístupový bod s DHCP serverem, jenž zaručí správné nastavení sítě bez zásahu uživatele.[26]

3.1 Ad hoc funguje jinak

Jelikož v ad hoc režimu chybí přístupový bod, musí na sebe samotná zařízení vzít určitou odpovědnost MAC vrstvy.

První stanice, která zavádí IBSS, začne posílat signály (tzv. „beacon“), které jsou potřeba k udržení synchronizace mezi stanicemi.

Další stanice se mohou připojit k síti po obdržení tohoto signálu, kde přijmou IBSS parametry. Všechny stanice, které jsou připojené do ad hoc sítě, musí poslat „beacon“ pravidelně, pokud nebyl vyslán signál z jiné stanice v době, kdy byl předpokládaný příchod „beaconu“.[24]

3.2 Vytvoření ad hoc sítě

Pro vytvoření ad hoc sítě potřebují mít uživatelé pouze bezdrátový adaptér v každém zařízení, které chtějí spojit dohromady. Žádné další zařízení již není třeba.

Obecně a nezávisle na operačním systému vypadá vytvoření ad hoc sítě takto:

1. Nejprve je nutné vytvořit nastavení sítě na počítači, který se v tomto procesu nazývá server
2. V nastavení bezdrátového síťového adaptéru je nutné nastavit IP adresu a masku podsítě na požadované hodnoty.
3. Nezapomeňme nastavit název SSID, případně také nějaký druh zabezpečení.
4. Bezdrátový adaptér začne vysílat signál tzv. „beacon“, díky kterému se ostatním zařízením zobrazí tato síť v seznamu dostupných sítí, a tudíž se k ní mohou připojit.
5. Nejprve však musí mít i tato ostatní zařízení nastavenou IP adresu ve stejném rozsahu jako zařízení, které vytvořilo síť.

3.3 Sdílení Internetu v ad hoc režimu

Jak už bylo výše zmíněno, ad hoc může sloužit také ke sdílení internetu. Pro sdílení internetu stačí provést několik kroků, které by průměrně zkušenému uživateli neměli dělat větší problémy. Nevýhodou však je, že první počítač bude muset být připojen k internetu pomocí kabelu, aby mohl být bezdrátový adaptér použit pro vytvoření ad hoc spojení. Toto řešení není však uspokojivé pro větší skupinu uživatelů.

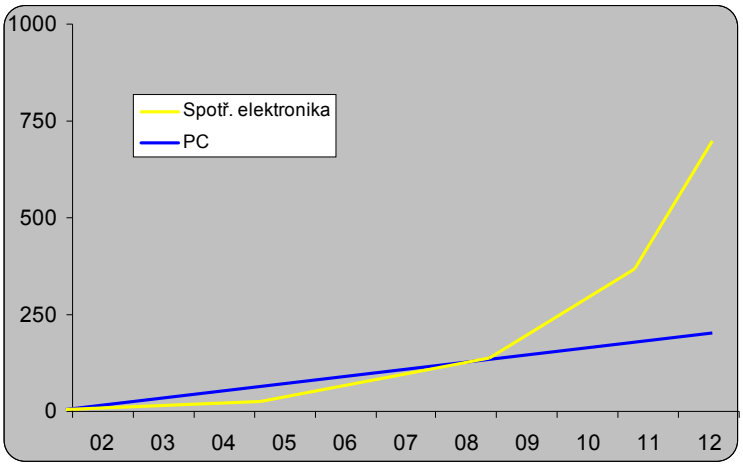
Pokud tedy uživatel chce sdílet své připojení k internetu s dalšími počítači, pak musí jeho počítač vlastnit síťovou kartu tzv. NIC a bezdrátový adaptér, což stejně většina přenosných počítačů má.

4. Wi-Fi Direct

V roce 2010 oznámila skupina Wi-Fi Alliance spuštění certifikace nových zařízení, která budou schopna využívat novou technologii Wi-Fi Direct. Tato technologie byla poprvé představena na veletrhu CES 2010 v Las Vegas.

Tato nová technologie umožňuje přímé (peer-to-peer) spojení mezi dvěma stanicemi, kde není třeba žádné další zařízení pro zprostředkování spojení (např. router, switch). Tuhle funkci však zastávalo i starší ad hoc spojení. Oproti němu však tento nový způsob spojení nabízí mnoho výhod. Především větší přenosovou rychlost, která je zajištěna MIMO modulační technologií a delší dosah signálu. U této technologie se používá přenos za pomoci více antén na vysílači i na přijímači a díky tomu můžeme dosáhnout maximální teoretické rychlosti až 250 Mbps.

Ovšem díky tomuto peer-to-peer spojení lze jednoduše a rychle spojit nejen PC a notebooky, ale také se můžou mezi sebou propojit i další zařízení, spadající do kategorie spotřební elektroniky, jako digitální fotoaparáty, MP3 přehrávače, mobilní telefony nebo herní konzole. U těchto malých zařízení se doposud spojení realizovalo pomocí USB kabelů nebo bezdrátově přes Bluetooth. Ovšem nyní je i do těchto zařízení velmi často zabudováváno Wi-Fi a jak je vidět na následujícím grafu, tak počet takových zařízení enormně stoupá a v průběhu roku 2012 by měl jejich počet přesáhnout jednu miliardu. Jak je uvedeno v [23], tak Wi-Fi Direct přináší nové uživatelské zkušenosti, protože nyní bude možné využívat bezdrátové spojení formou tzv. PlugAndPlay, ovšem bez použití té části Plug.

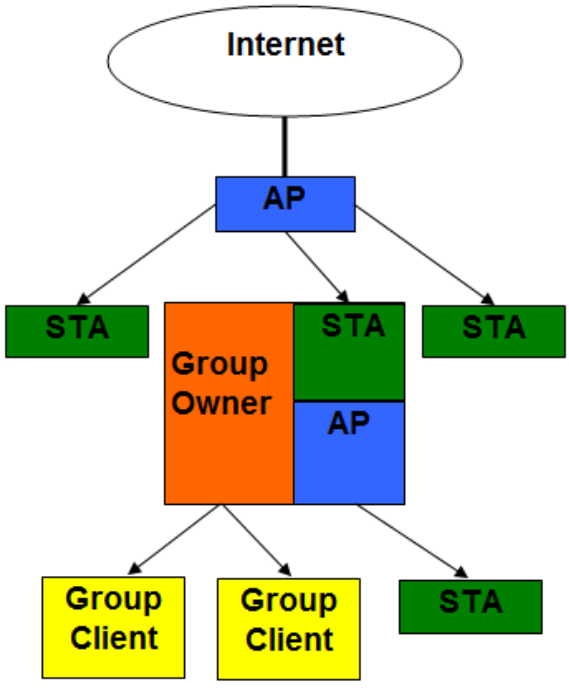


Obrázek 3: Rozšíření Wi-Fi
Zdroj: [7]

4.1 Fungování Wi-Fi Directu

Wi-Fi Direct funguje tak, že rozšiřuje stávající klient-server architekturu o další zařízení. Tato zařízení se nazývají Group Owner (GO) a Group Client (GC), která jsou schopna vytvořit ad hoc (peer-to-peer) spojení. GO funguje jako serverová stanice, která vytváří ad hoc spojení s jedním či více GC.

Velkou výhodou také je, že můžeme kombinovat klasickou Wi-Fi síť (infrastrukturní) se sítí vytvářenou pomocí Wi-Fi Direct. Budeme-li mít například mezi dvěma notebooky vytvořené peer-to-peer spojení za pomoci Wi-Fi Directu, pak zařízení, které funguje jako GO, se bude moci připojit k AP v jiné infrastrukturní síti. V této síti však bude působit jako stanice (STA). Další stanice se však mohou stále připojovat ke GO zařízení tzv. non-peer-to-peer spojením. Pro tyto stanice bude GO přístupovým bodem a bude tvořit určitý most do infrastrukturní sítě, jak je vidět na následujícím diagramu.



Obrázek 4: Wi-Fi Direct diagram
Zdroj: [13]

Možná největší výhodou pro Wi-Fi Direct je, že pokud budeme chtít používat toto spojení, tak bude možné to udělat i bez nutnosti zakoupení nového hardwaru. Wi-Fi Alliance

slibuje, že bude možné do stávajících síťových karet nahrát nový firmware, a tím budou zařízení schopná používat Wi-Fi Direct. Ovšem zatím se všichni výrobci soustředí na certifikaci nových zařízení a k vydávání nového firmwaru se zatím příliš nehlásí.

4.2 Průběh certifikace

Certifikaci nových wi-fi zařízení provádí Wi-Fi Aliance, která vznikla v roce 1999. Tato globální nezisková organizace založila v roce 2000 certifikační program Wi-Fi CERTIFIED, jehož cílem je zajištění provozuschopnosti mezi produkty založenými na standardu IEEE 802.11. O založení této skupiny se zasloužilo několik výrobců zařízení využívajících tento standard. Do této skupiny patří Cisco, Conexant, Agere, Nokia a Symbol united. Ke konci roku 2011 má tato skupina již necelých 500 členů, které můžeme nalézt na stránkách Wi-Fi Aliance [19].

Wi-Fi Aliance vlastní 15 nezávislých testovacích středisek v Severní Americe, Evropě, Japonsku atd. Každé zařízení, které uspěje v testech, obdrží značku „Wi-Fi CERTIFIED“. Ovšem před tím musí splnit tři následující kritéria[21]:

- **Interoperabilita -** je primární cíl certifikace. Přísné testy zkoumají, zda spolu mohou zařízení od různých výrobců spolupracovat.
- **Zpětná kompatibilita** - která je potřeba pro zajištění spolupráce starých zařízení s novějšími, aby mohli uživatelé postupně bez obav modernizovat svou síť.
- **Inovace** - jsou podporovány zaváděním nových certifikačních programů (např. povinné WPA2, nepovinné WMM)

Obrázek 5: Wi-Fi logo
Zdroj: [2]

Každé zařízení, které bude nosit značku „Wi-Fi CERTIFIED Wi-Fi Direct“, musí splnit následující test[22]:

- **Základní certifikační test** - zařízení musí podporovat alespoň standard 802.11g a zabezpečení WPA2-Personal
- **WMM a Wi-Fi Protected Setup test** - zařízení musí podporovat Wi-Fi Multimedia (WMM) a Wi-Fi Protected Setup
- **Povinné certifikační testy** – testy reprezentují minimální funkcionalitu, kterou musí Wi-Fi Direct zařízení podporovat
- **Test volitelných funkcí** – všechny volitelné funkce budou testovány, zda jsou implementovány

Všechna vyrobená zařízení nemusí procházet touto certifikací, ovšem zařízení, která mají na svém obalu značku Wi-Fi CERTIFIED, jsou uživateli preferována. Veškerá doposud certifikovaná zařízení můžeme najít na adrese uvedené v použité literatuře [15].

4.3 Vytvoření Wi-Fi Direct sítě

Na rozdíl od ad hoc spojení zde odpadá složité nastavování, což bylo jedním z důvodů jeho neobliby. Každé zařízení, které má Wi-Fi Direct certifikaci, musí obsahovat standard Wi-Fi Protected Setup (WPS), který právě samotné vytváření spojení velmi usnadňuje. Pro vytvoření Wi-Fi Direct spojení bude muset uživatel pouze stisknout tlačítko, zadat PIN kód nebo k sobě zařízení pouze přiblížit. O další kroky se již postará WPS.
Průběh spojení:

1. Stisknutí tlačítka, zadání PINu nebo přiblížení zařízení
2. Iniciátor spojení vyšle rozpoznávací packet zvaný Probe Request, který zjistí, zda jsou v okolí jiná zařízení
3. Iniciační zařízení vyšle požadavek pro spojení
4. Druhému zařízení se objeví pop-up okno pro přijmutí spojení
5. Oba účastníci zadají PIN pro potvrzení a spojení je navázané

I když je tento způsob vytvoření spojení velmi jednoduchý a uživatelsky přívětivý, tak podle autora článku [18] zde existuje určitá bezpečnostní chyba, která umožňuje účinný brute-force útok. Pomocí toho útočník získá PIN kód a může se připojit. Oprava bude muset přijít

od výrobců, kteří vydají nový firmware pro dané zařízení. Do té doby mohou uživatelé použít jiné řešení v podobě speciálního softwaru jednotlivých výrobců např. Intel My WiFi Utility.

4.4 Wi-Fi Direct jako náhrada za Bluetooth

Bluetooth i Wi-Fi Direct jsou obě stejně uživatelsky jednoduché technologie, které slouží ke stejnému účelu, a to k přenosu dat.

Dle článku [12] Wi-Fi Direct zasahuje do oblasti, kde dominovalo Bluetooth a tím může jeho nadvládu ukončit, o čemž vypovídá už samotný název článku. Autor tohoto článku také uvádí, že tato dosavadní jednička v peer-to-peer spojeních má svůj osud zpečetěn právě proto, že Wi-Fi adaptér je přítomný ve velkém množství zařízení (viz. výše), a tak nebude nutné, aby sem výrobci integrovali jiný prvek, který má stejnou funkci.

4.4.1 Něco málo o Bluetooth

Technologie Bluetooth, známá jako standard 802.15 se začala vyvíjet v roce 1994 ve Švédském Ericssonu.

Je to standard patřící do skupiny PAN sítí, který je primárně určen k přenášení dat na krátkou vzdálenost. Bluetooth pracuje v ISM pásmu 2,4 GHz, stejně jako Wi-Fi. Je to volné pásmo, kde je povolen provoz bez placení licenčních poplatků. Od první zmínky o Bluetooth až do dnešního dne bylo vyvinuto několik verzí tohoto standardu. Z výše zmíněných verzí nás budou nejvíce zajímat ty nejnovější, což jsou Bluetooth 3.0+HS a Bluetooth 4.0.

Bluetooth 3.0 + HS podporuje teoretickou rychlost přenosu dat až 24 Mbit/s, i když ne přes samotné Bluetooth. K rychlejšímu přenosu dat je použit další radiový kanál, tzv. AMP, který využívá 802.11a/b/g/n specifikaci. Tento AMP kanál je zcela v režii Bluetooth, a tak když se naváže spojení mezi zařízeními, proběhne zjištění, zda obě zařízení podporují AMP kanál. Pokud ano, přenesou se data a po skončení přenosu se AMP kanál vypne, pro snížení spotřeby energie. Tento druhý kanál je pro uživatele naprosto neviditelný a jeho využití zaznamenají jen zvýšenou přenosovou rychlostí.[13]

Bluetooth 4.0 se oproti verzi 3.0+HS vydalo úplně jiným směrem. Nedalo se cestou zvyšování přenosové rychlosti, ale snaží se být co nejméně energeticky náročné. U této verze je snaha o co nejmenší energetické nároky a miniaturizaci tak, aby bylo možné implementovat „čtyřku“ do zařízení poháněných baterií o velikosti knoflíku.

4.4.2 Wi-Fi Direct vs. Bluetooth

Jak je vidět, tak se Bluetooth sice stále vyvíjí a snaží se zlepšovat své dovednosti, ale vzrůstající obliba technologie Wi-Fi je stále větším strašákem. Pokud bychom chtěli tyto dvě technologie srovnávat, pak by Bluetooth vyhrálo pouze v oblasti spotřeby energie. Z tabulky číslo 2 je zřejmé, že v ostatních případech je lepší Wi-Fi Direct, ať už se jedná o dosah, zabezpečení atd. S příchodem nové technologie však přichází i určité bezpečnostní hrozby. U Bluetooth byl hrozbou Bluejacking, kde útočník mohl zneužít data na vzdálenost 5-10 m. Jelikož má Wi-Fi Direct větší dosah, tak je zde hrozba zneužití dat mnohem větší, což může být určitě plus pro BT. [12]

Nikdo se však nemusí bát žádného zániku „modrozubé“ technologie. I když bude ve svém dominantním území nahrazeno, díky jeho malé energetické náročnosti se uchytí především v lékařských, sportovních a průmyslových senzorech a všude tam, kde je hlavní nízká spotřeba.

Standard	Max. teor. rychlost	Teoretický dosah	Zabezpečení
Wi-Fi Direct	250 Mb/s	max 200 m	WPA2, AES-256
Bluetooth 2.0	3 Mb/s	max 10 m	PIN
Bluetooth 3.0+HS	24 Mb/s	max 100 m	AES-128
Bluetooth 4.0	24 Mb/s	max 100 m	AES-128

Tabulka 2: Srovnání Wi-Fi Direct a Bluetooth
Zdroj: [11, Autor]

5. Měření a porovnání

Tato část práce se zabývá měřením hodnot jednotlivých druhů spojení, které budou sloužit k porovnání již výše zmíněných typů spojení a zda je možné, že bude ad hoc mód nahrazen. Pro komparaci byly vybrány čtyři základních kvalitativní parametry bezdrátových sítí.

Zvolené parametry:

1. Přenosová rychlost (Mb/s)
2. Kvalita signálu (dBm, %)
3. Latence (ms)
4. Ztrátovost paketů (%)

5.1 Použité nástroje

Iperf

Je to jednoduchý freeware program, který generuje provoz na síti po IP vrstvě. Může generovat jak TCP, tak i UDP pakety. Iperf funguje na principu Client-Server a je dostupný pro Windows i Linux. Spuštění a běh programu se provádí z příkazové řádky. Pokud uživatel nechce psát příkazy ručně, pak se nabízí využití Java grafického rozhraní Jperf, kde jednoduše nastavíme vše, co zvládne Iperf s jednotlivými přepínači.

NetWorx

Tento jednoduchý a volně použitelný program NetWorx od společnosti SoftPerfect Research je mocný nástroj sloužící k sledování provozu na síti a měření rychlosti sítě. Umožňuje tvorbu denních, týdenních a měsíčních statistik provozu v síti a také nabízí jednoduché síťové testy jako ping a trace route.

My budeme využívat nástroj Měření rychlosti, kde si uživatel určí, kdy chce sledovat provoz na síti. V průběhu měření můžeme sledovat aktuální, průměrnou a maximální přenosovou rychlost a celkové množství přenesených dat a následně naměřené hodnoty uložit do textového souboru.

InSSIDer

Volná aplikace sloužící pro skenování okolních sítí od MetaGeek, která slouží jako náhrada za zastaralý NetStumbler. Zobrazuje mnoho informací o jednotlivých sítích, jako například kvalitu signálu, SSID, typ sítě, zabezpečení. Výhodou je také grafické zobrazení naměřených hodnot.

NetSurveyor

Bezplatný software od firmy Nuts About Nets, který slouží ke skenování okolních sítí, stejně jako InSSIDer nebo starší NetStumbler. Oproti InSSIDeru zobrazuje sílu signálu pomocí více ukazatelů.

NetDoppler

NetDoppler je testovací utilita sloužící pro měření latence a šířky pásma po celé cestě mezi oběma koncovými uzly. Naměřené hodnoty poté dokáže zobrazit také graficky. Je to bezplatný software jehož výrobcem je společnost WildPackets.

5.2 Přenosová rychlost

Přenosová rychlost udává, jaký objem informace se přenese za jednotku času. Základní jednotka je bit za sekundu a příslušné násobky. Nejčastěji udávanou hodnotou přenosové rychlosti je maximální teoretická přenosová rychlost, tedy přenosová rychlost za ideálních podmínek. Ovšem reálné rychlosti jsou vždy menší především kvůli počtu připojených klientů, kvalitě signálu (vzdálenost komponent, útlum prostředí) apod.

Když půjde o samotné měření této hodnoty, pak máme na výběr ze dvou druhů měření. Můžeme provádět aktivní nebo pasivní měření. Při aktivním měření posíláme do sítě vlastní pakety, které na jiném místě opět přijímáme. Nevýhodou může být přidaná zátěž do sítě, která může ovlivnit provoz ostatních uživatelů. Při pasivním měření žádná data do sítě neposíláme. Pouze sledujeme a vyhodnocujeme uživatelský provoz na síti. [16]

V našem případě budeme využívat jak aktivního, tak i pasivního měření. Pro měření budeme využívat program NetWorx (pasivní) a program Iperf (aktivní). Veškeré tyto hodnoty budeme měřit za různých podmínek, především vzdáleností.

Pro naše potřeby jsme si stanovili sedm různých skupin:

- 1 metr
- 10 metrů – přímá viditelnost
- 10 metrů – nepřímá viditelnost
- 50 metrů – přímá viditelnost
- 50 metrů – nepřímá viditelnost
- 100 metrů – přímá viditelnost
- 100 metrů – nepřímá viditelnost

V případě nepřímé viditelnosti bude překážka při všech vzdálenostech tvořena zdí.

5.2.1 Aktivní měření

Pro aktivní měření přenosové rychlosti budeme používat program Iperf. Ovšem abychom nemuseli zadávat veškeré příkazy ručně, budeme používat Jperf, který navíc dokáže naměřené hodnoty zobrazit v jednoduchém grafu.

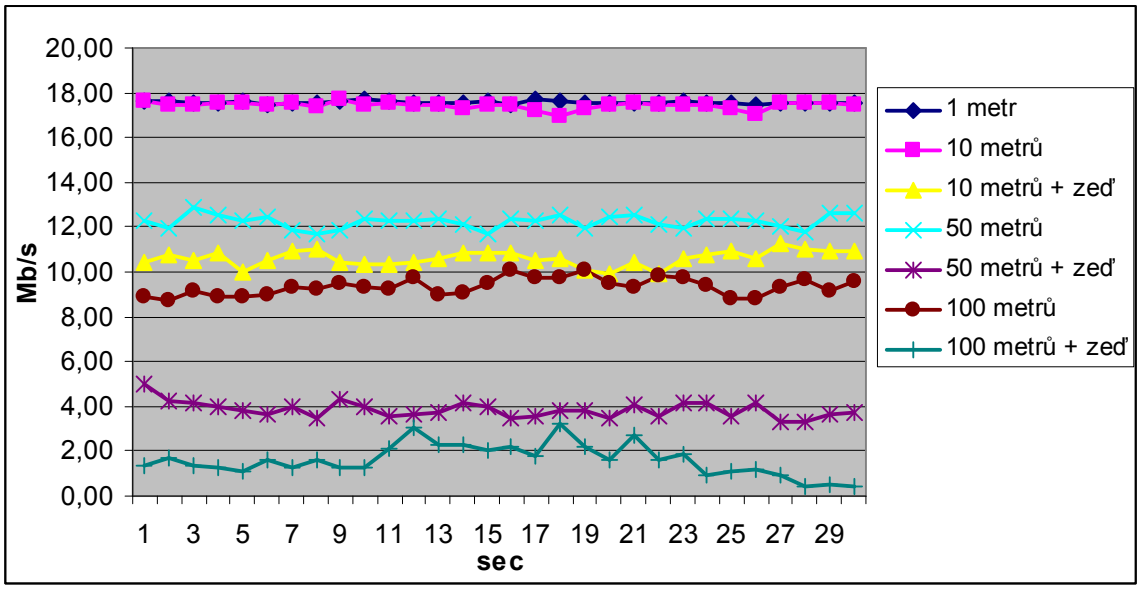
Tento program musíme spustit na obou koncových zařízeních. Na jednom zapneme Iperf jako server, kde můžeme také nastavit číslo portu, na kterém bude server naslouchat.

Na druhém počítači vybereme mód Client. Po spuštění programu v tomto módu bude počítač sloužit jako generátor provozu na síti. Před spuštěním můžeme nastavit různé hodnoty, jako je velikost posílaných dat, doba měření nebo jednotky pro zobrazení. Můžeme také vybrat, zda chceme testovat provoz TCP nebo UDP protokolů.

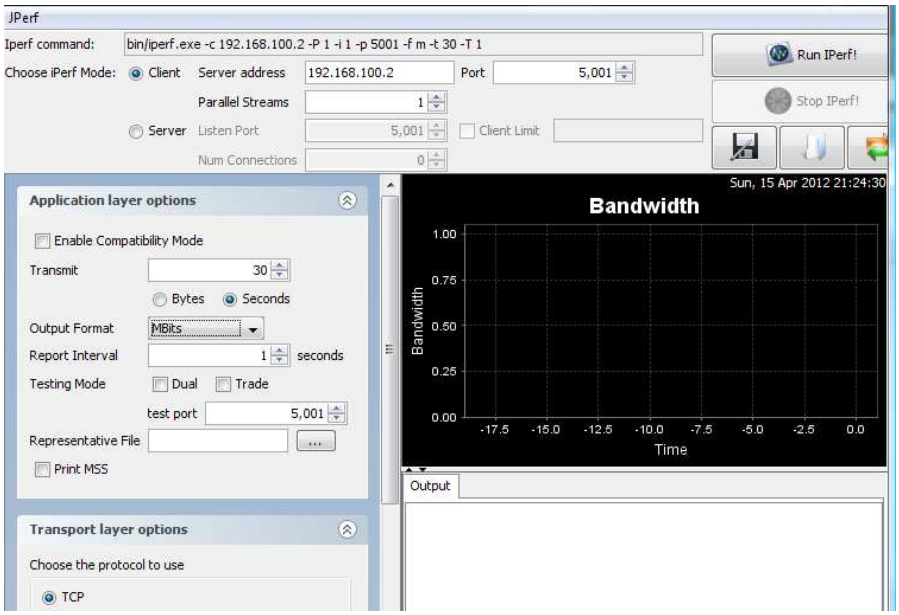
Pro naše měření jsem nastavil adresu serveru 192.168.100.2, kde nám běží Iperf server, použitý protokol na TCP a dobu měření na 30 sekund, jak je vidět na obrázku č. 6. Naměřené hodnoty, které jsme získali z výše uvedeného nastavení Iperfu, můžeme vidět v tabulce číslo 3 a následně v grafu číslo 1. Tyto hodnoty jsme získali vytvořením průměru z pěti provedených měření pro každou podmínku.

Podmínky	Přenosová rychlost (Mb/s)
1 metr	17,57
10 metrů	17,43
10 metrů + překážka	10,61
50 metrů	12,24
50 metrů + překážka	3,85
100 metrů	9,34
100 metrů + překážka	1,62

Tabulka 3: Aktivní měření přenosové rychlosti



Graf 1: Iperf - výsledky měření



Obrázek 6: Nastavení Jperf

5.2.2 Pasivní měření

Měření budeme provádět pomocí programu NetWorx a jeho nástroji Měření rychlosti. Měření bude provedeno na třech různých vzorcích, které budeme používat pro simulování provozu na síti:

Vybrané vzorky:

- malý soubor (10 MB)
- skupina souborů (50 x 1 MB)
- velký soubor (500 MB)

Pro měření budeme užívat dva notebooky (NB1, NB2). Na NB1 vytvoříme sdílenou složku, ze které budeme z NB2 kopírovat jednotlivé soubory. Tímto způsobem budeme simulovat provoz na vytvořené síti a pomocí nástroje Měření rychlosti budeme měřit hodnoty při kopírování souborů. Nejvíce nás bude zajímat průměrná a maximální přenosová rychlost. Provedeme několik měření pro jednotlivé soubory, abychom měli dostatečný vzorek, ze kterého poté vytvoříme průměrné hodnoty. Tyto hodnoty můžeme vidět v následujících tabulkách.

Podmínky	Ad hoc		Wi-Fi Direct	
	Průměrná rychlost (Mb/s)	Maximální rychlost (Mb/s)	Průměrná rychlost (Mb/s)	Maximální rychlost (Mb/s)
1 metr	16,09	18,80		
10 metrů	16,91	18,94		
10 metrů + překážka	13,42	15,29		
50 metrů	14,46	17,00		
50 metrů + překážka	6,16	7,96		
100 metrů	11,93	13,38		
100 metrů + překážka	-	-		

Tabulka 4: Pasivní měření - malý soubor
Zdroj: [Autor]

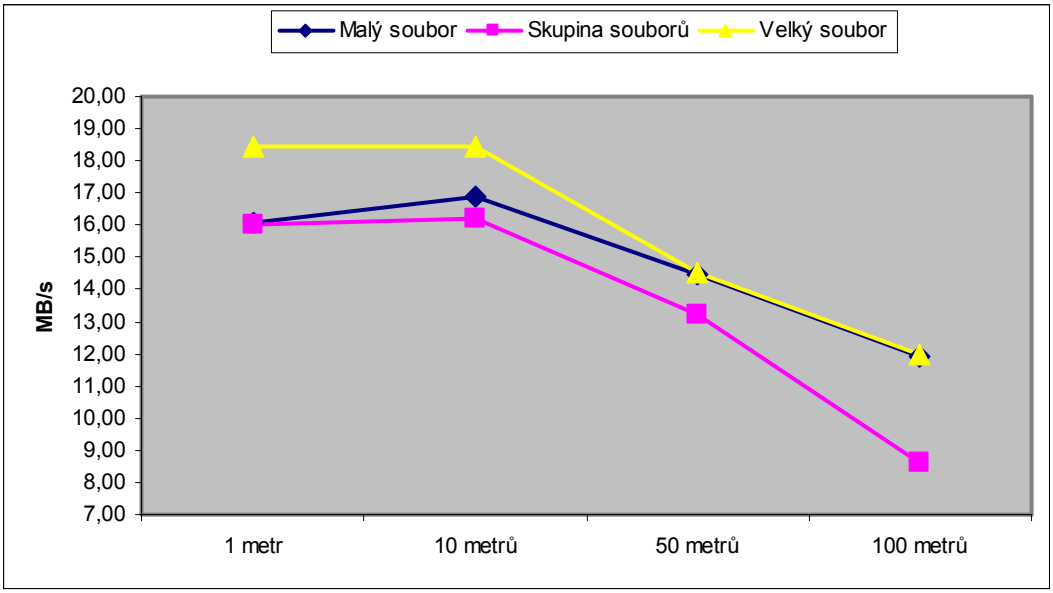
Podmínky	Ad hoc		Wi-Fi Direct	
	Průměrná rychlost (Mb/s)	Maximální rychlost (Mb/s)	Průměrná rychlost (Mb/s)	Maximální rychlost (Mb/s)
1 metr	16,00	18,37		
10 metrů	16,23	18,14		
10 metrů + překážka	13,42	15,62		
50 metrů	13,24	15,70		
50 metrů + překážka	6,15	8,70		
100 metrů	8,61	10,71		
100 metrů + překážka	-	-		

Tabulka 5: Skupina souborů
Zdroj: [Autor]

Podmínky	Ad hoc		Wi-Fi Direct	
	Průměrná rychlost (Mb/s)	Maximální rychlost (Mb/s)	Průměrná rychlost (Mb/s)	Maximální rychlost (Mb/s)
1 metr	18,43	19,16		
10 metrů	18,46	19,26		
10 metrů + překážka	15,06	17,23		
50 metrů	14,53	16,84		
50 metrů + překážka	7,43	10,55		
100 metrů	11,98	14,10		
100 metrů + překážka	-	-		

Tabulka 6: Velký soubor
Zdroj: [Autor]

Bohužel u ad hoc spojení nebylo možné naměřit žádné hodnoty na vzdálenost 100 metrů s překážkou. Jelikož spojení vypadávalo, tak nebylo možné přenášet soubory pro simulování provozu na síti. Následující graf zobrazuje, jak je přenosová rychlost ovlivněna vzdáleností propojených zařízení.



Graf 2: Graf závislosti přenosové rychlosti na vzdálenosti

5.3 Kvalita signálu

Kvalita signálu je jeden z nejdůležitějších ukazatelů měřitelných na Wi-Fi sítích. Kvalita signálu je velmi závislá na síle signálu, který je vysílán, citlivosti antény, vzdálenosti, překážkách, které se dostanou signálu do cesty a množství okolního šumu, který je tvořen jinými uživateli stejného frekvenčního pásma nebo i mikrovlnou troubou. Velmi důležitá je také přímá viditelnost jednotlivých zařízení. Další informace o rušivých elementech, můžeme nalézt zde: http://blog.klaska.net/coyot/it/site/wifi-prostupnost-signalu-v-praxi.

Měření kvality signálu je možné více způsoby. Nejjednodušší možností je měření pomocí samotného bezdrátového adaptéru, který zprostředkovává informace o signálu. Tyto informace je pak možné interpretovat pomocí utility samotného OS (např. zobrazení signálu v oznamovací oblasti Windows) nebo pomocí příslušného softwaru (Vistumbler, InSSIDer). Síla signálu může být měřena v procentech, mW (miliWatt), dBm (decibel miliwat) nebo RSSI. Další možností je specializované zařízení tzv. Wi-Fi locater, který zobrazuje sílu signálu pomocí několika LED diod.

Pro námi prováděné měření budeme používat program InSSIDer, kvůli jeho výbornému grafickému zobrazení síly signálu. Jedinou nevýhodou tohoto programu je, že síla signálu, kterou InSSIDer vydává za hodnotu RSSI, je ve skutečnosti hodnota Signal Strenght udávaná v dBm, jak je uvedeno zde [10]. Pro správné zobrazení lze použít program NetSurvey, který zobrazuje sílu signálu rovnou ve třech jednotkách (dBm, mW a %).

V našem případě budeme tedy používat jednotky dBm, které se u sítí 802.11 pohybují v rozmezí 0 až -100, kde platí, že čím větší (záporná) hodnota, tím horší je signál. V tabulce číslo 7 můžeme vidět naměřené hodnoty, které jsme získali.

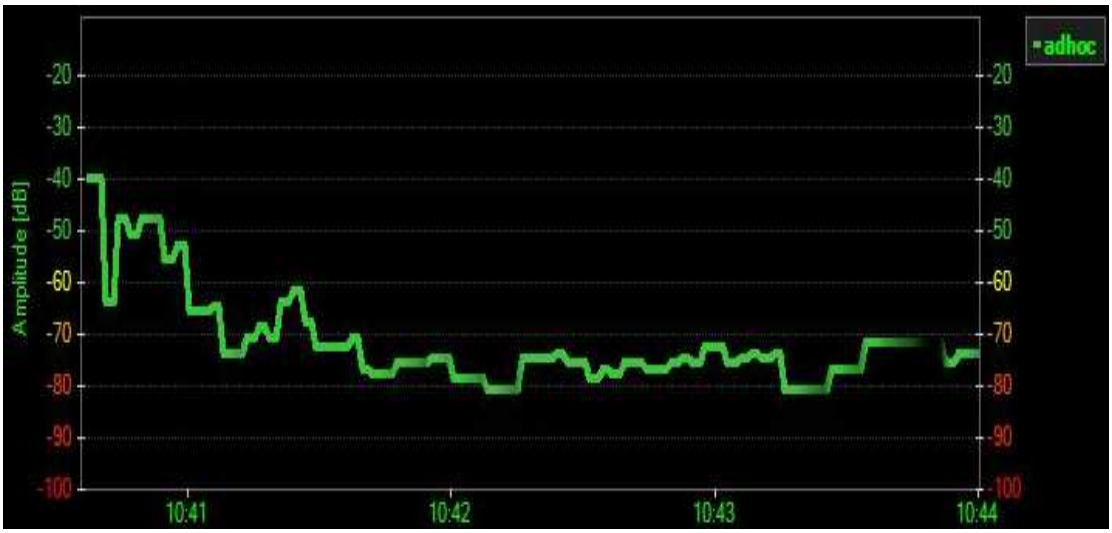
Naše měření bylo prováděno mezi dvěma notebooky. První vytvořil ad hoc síť a na druhém byl zapnut InSSIDer a NetSurvey pro monitorování signálu. Vzdálenosti do 10 m byly měřeny uvnitř budovy, zatímco delší vzdálenosti byly měřeny mimo budovu.

Jak můžeme vidět, tak signál měl dosah až 150 m při přímé viditelnosti a 75 m při nepřímé. Dále již nebyl signál přijat. Ovšem pokud chceme mít kvalitní spojení, pak se hodnota musí pohybovat do -70 dBm, jak píše autor článku [14].

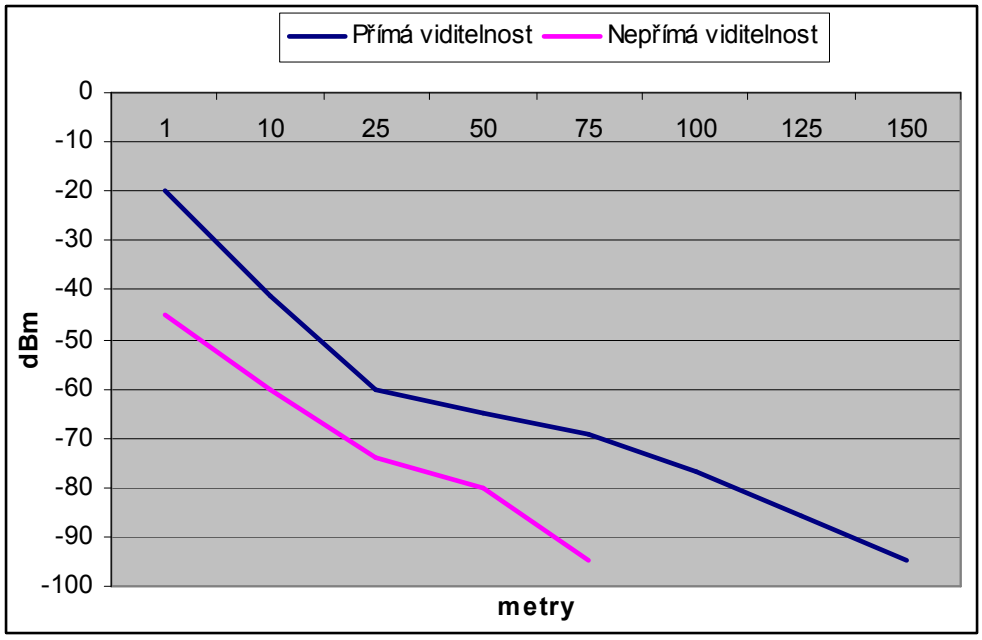
Metry	Přímá viditelnost		Nepřímá viditelnost	
	dBm	%	dBm	%
1	-20	100	-45	70
10	-41	75	-60	50
25	-60	51	-74	35
50	-65	45	-80	25
75	-69	40	-95	5
100	-77	30		
125	-86	18		
150	-95	5		

Tabulka 7: Kvalita signálu ad hoc
Zdroj: [Autor]

Na následujícím obrázku (obr. 8) vidíme graf síly signálu v InSSIDeru. Tento graf vznikl postupným oddalováním koncových zařízení. Jak je vidět signál nejvíce klesal v první části, a pak se pohyboval v určitém rozmezí. U konce grafu je vidět, že došlo k úplné ztrátě signálu.



Obrázek 8: InSSIDer nepřímo do 100 m



Graf 3: Kvalita signálu při přímé a nepřímé viditelnosti

5.4 Latence

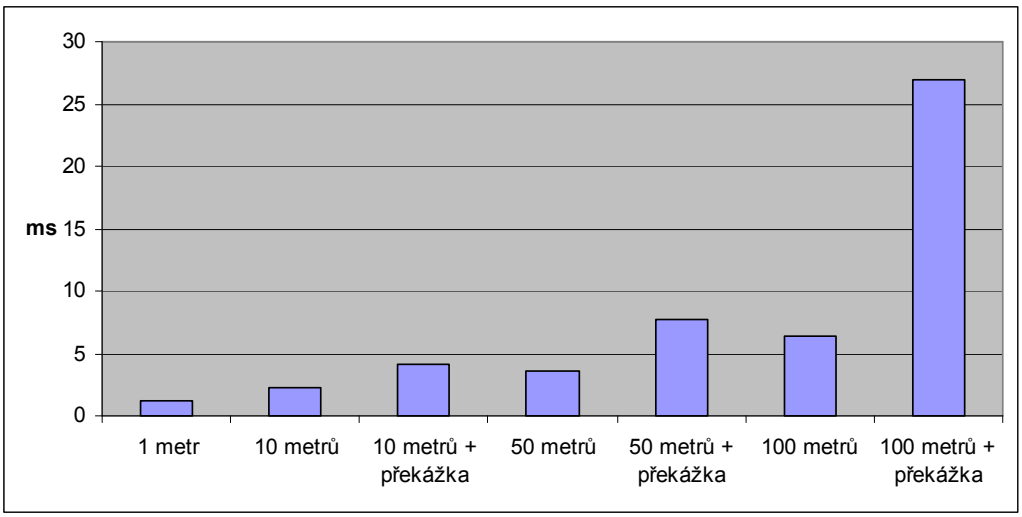
Tento parametr udává velikost zpoždění paketů putujících od jednoho koncového zařízení k druhému. Do této doby je započtena doba, po kterou cestuje paket k cílovému uzlu, doba zpracování a doba návratu. Tento časový úsek se nazývá Round Trip Time, který je měřený v milisekundách. Latence je velmi důležitý parametr pro některé síťové aplikace. Vysoké zpoždění má největší vliv na hraní her, kde je použitelnost do 50 ms, nebo videohovory přes internet použitelné do 200 ms.

Pro měření latence budeme používat stejné podmínky jako v předchozích měřeních, tedy vzdálenost a překážky. Měření budeme provádět pomocí jednoduchého programu NetDoppler, pomocí něhož můžeme změřit latenci až na setiny milisekund. Měření sestává z periodického posílání datagramů a čekání na odpověď. Pro měření využívá protokol ICMP s jeho zprávami Echo Request a Echo Reply.

NetDoppler nám umožňuje provádět dlouhodobé i rychlé testy latence. My budeme využívat rychlých testů. V nastavení změníme pouze počet opakování na 20 a spustíme test. Výstupem bude dvacet hodnot zpoždění z nichž program vypočítá průměrnou hodnotu latence a zobrazí společně s maximálním a minimálním zpožděním. Pro získání potřebného vzorku dat provedeme test vícekrát. Z takto získaných hodnot poté vytvoříme průměrné hodnoty, které můžeme vidět v tabulce číslo 8 a grafu číslo 4.

Podmínky	Latence (ms)
1 metr	1,221
10 metrů	2,212
10 metrů + překážka	4,163
50 metrů	3,576
50 metrů + překážka	7,695
100 metrů	6,348
100 metrů + překážka	26,992

Tabulka 8: Průměrné hodnoty latence ad hoc spojení
Zdroj: [Autor]



Graf 4: Velikost latence v závislosti na vzdálenosti

5.5 Ztráta paketů

Ztráta paketů je chyba, která nastane, když některý z vyslaných paketů nedorazí ke svému cíli, dorazí s velkým zpožděním nebo dorazí poškozený. Tato chyba může nastat z několika důvodů, ke kterým patří především špatná kvalita signálu nebo zahození paketu z důvodu zahlcení sítě. Ztráta paketů je jev, který může způsobit problémy především aplikacím, které jsou závislé na přímé posloupnosti paketů. To jsou především počítačové hry a videohovory, kde může ztráta paketů způsobit různé přeskakování či sekání zvuku a obrazu.

Pro naše měření budeme používat stejný program jako pro měření latence, tedy NetDoppler. V nastavení změníme počet opakování testu na hodnotu 500, interval mezi odesíláním paketů na 500 ms a dobu čekání na odpověď zmenšíme na hodnotu 500 ms. V takto nastaveném programu pak provedeme několik měření pro námi zvolené vzdálenosti.

Podmínky	Ztráta paketů (%)
1 metr	0,07
10 metrů	0,13
10 metrů + překážka	1,20
50 metrů	0,25
50 metrů + překážka	3,48
100 metrů	0,94
100 metrů + překážka	6,20

Tabulka 3: Průměrné hodnoty ztráty paketů ad hoc spojení
Zdroj: [Autor]

5.6 Vyhodnocení

Bohužel, i přes veškeré vynaložené úsilí, nebylo možné změřit hodnoty pro Wi-Fi Direct. To bylo zapříčiněno především kvůli tomu, že nebylo možné sehnat žádné zařízení podporující toto spojení.

Wi-Fi Aliance provedla koncem roku 2010 certifikaci určitého počtu zařízení, které uvádí na svých stránkách. Ovšem žádné z nich nebylo dostupné v obchodech v ČR ani v zahraničí.

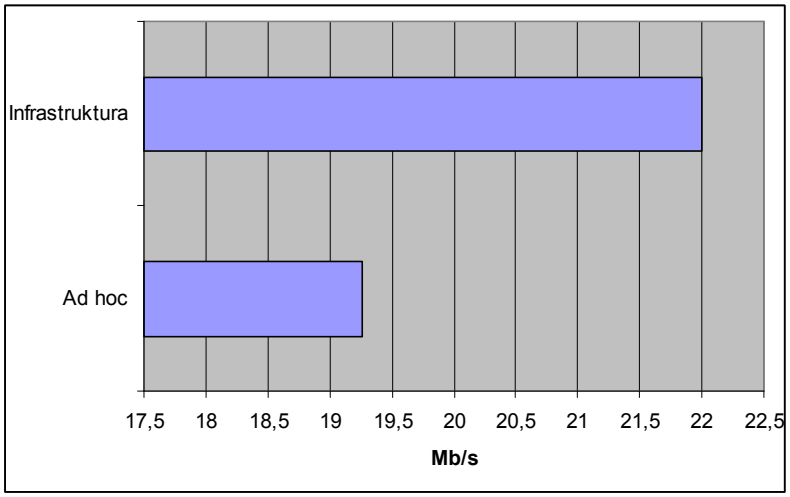
Následně po několika měsících od certifikování bylo objeveno zařízení Atheros AR5B97 od společnosti Qualcomm, které mělo podle Wi-Fi Aliance podporovat Wi-Fi Direct. Po objednání zařízení z USA a vyzkoušení přišlo zklamání, protože se nám spojení nepodařilo

vytvořit. Problém byl se zastaralými ovladači. Nejnovější ovladače k tomuto adaptéru byly z roku 2009.

Po přečtení článku [17] bylo zakoupeno zařízení Intel Centrino Advanced-N 6230. Bohužel nebylo možné sehnat notebook, ve kterém by bylo možné tento bezdrátový adaptér zprovoznit. Vyzkoušeno bylo několik notebooků značky HP, které nepodporují výměnu Wi-Fi adaptéru za jiný. Ostatní dostupné notebooky neměli potřebný mini PCI express slot, ale pouze starší mini PCI. Proto je naše měření provedeno pouze u spojení ad hoc.

I když se nám nepodařilo změřit hodnoty Wi-Fi Direct spojení, můžeme k jistému porovnání použít hodnoty udávané v použité literatuře. Z článku [25] bylo zjištěno, že Wi-Fi Direct využívá celou šířku pásma standardu 802.11g/n, na rozdíl od ad hocu, který ji využívá omezeně. Následující graf zobrazuje námi naměřenou maximální přenosovou rychlost, která byla získána při pasivním měření přenosu velkého souboru na 10 metrů, v porovnání s reálnou uživatelskou rychlostí na infrastrukturní síti, které by měl Wi-Fi Direct dosahovat také.

Podle informace, kterou uvádí Wi-Fi Aliance [20] může být Wi-Fi Direct spojení vytvořeno až na vzdálenost 200 m, kdežto námi naměřená hodnota u ad hoc sítě byla pouze 150 metrů.



Graf 5: Porovnání přenosové rychlosti ad hocu a infrastruktury
Zdroj: [8, Autor]

6. Závěr

V této bakalářské práci jsem se snažil vytvořit komparaci dvou typů spojení. Nejprve jsem se seznámil se starším typem spojení ad hoc a pokusil jsem se nastínit jeho možnosti, způsob využití a jiné. Stejné seznámení jsem provedl s jeho možným nástupcem Wi-Fi Direct. Zjistil jsem jeho výhody oproti ad hocu, způsob jakým funguje a proces, kterým musí nová zařízení projít při certifikaci. Dále jsem zjistil, že Wi-Fi Direct se může stát také nástupcem úplně jiné technologie, a to technologie Bluetooth.

Na základě prostudované literatury jsem určil čtyři základní parametry pro komparaci. Pro každý parametr jsem provedl měření na různé vzdálenosti v rozsahu 1 – 100 metrů s překážkou a bez překážky. Při měření jsem používal pouze bezplatný a volně dostupný software, který sice nenabízí takové možnosti jako placené programy, ale pro naše měření je dostačující.

Při měření se mi bohužel nepodařilo z výše uvedených důvodů zprovoznit Wi-Fi Direct spojení, a proto je měření provedeno pouze u spojení ad hoc. Nicméně, i když jsem naměřil pouze tyto hodnoty, provedl jsem komparaci určitých parametrů s hodnotami, které uvádějí stránky Wi-Fi Aliance a jiné články.

Po provedení porovnání dostupných parametrů je očividné, že Wi-Fi Direct je oproti ad hocu „výkonnější“. Přihlédneme-li ještě k dalším vlastnostem, jako je zabezpečení či složitost vytvoření spojení, které jsou porovnávány v článcích zabývajícími se touto tématikou [1][6], pak můžeme říci, že Wi-Fi Direct se může stát plnohodnotnou náhradou ad hocu.

Použitá literatura

[1] About.com: Wi-Fi Direct. [online]. [cit. 2012-04-22]. Dostupné z: http://mobileoffice.about.com/od/wifimobileconnectivity/p/wi-fi-direct.htm

[2] Androidspin.com. [online]. [cit. 2012-03-18]. Dostupné z: http://androidspin.com /2010/04/22/nexus-one-a-dog-can-learn-new-tricks-wifi-n-is-a-go/wifi-certified-logo/

[3] Bezdratovetechnologie. [online]. [cit. 2012-03-18]. Dostupné z: http://bezdratove technologie.webnode.cz/

[4] BRISBIN, Shelly. *Wi-fi postavte si svou vlastní wi-fi síť*. Neocortex. Praha : The McGraw-Hill, 2003. 248 s. ISBN 0-07-222624-2.

[5] DAVIS, Harold. *Bezdrátové sítě Wi-Fi : Průvodce úplného začátečníka*. Vydání první. Praha : Grada Publishing, 2006. 336 s. ISBN 80-247-1421-3.

[6] Indiatechonline.com: Get the most out of Wi-Fi Direct, the new personal, portable Wi-Fi. [online]. [cit. 2012-04-22]. Dostupné z: http://www.indiatechonline.com/wi-fi-direct-118.php

[7] Intel.com: Welcome to the Freedom of Portable Wi-Fi. [online]. [cit. 2012-03-18]. Dostupné z: http://download.intel.com/products/wireless/320875.pdf

[8] Lupa.cz: 802.11g: rychlejší WiFi?. [online]. [cit. 2012-04-24]. Dostupné z: http://www.lupa.cz/clanky/802-11g-rychlejsi-wifi/

[9] Marigold.cz. [online]. [cit. 2012-03-18]. Dostupné z: http://www.marigold.cz/ wifi/doku.php/adhoc

[10] Metageek.net: RSSI is NOT equal to Signal Strength (dBm). [online]. [cit. 2012-04-22]. Dostupné z: http://www.metageek.net/forums/showthread.php?2968-RSSI-is-NOT-equal-to-Signal-Strength-%28dBm%29

[11] Mobilizujeme.cz: Wi-Fi Direct – objevte možnosti nové technologie. [online]. [cit. 2012-04-24]. Dostupné z: http://mobilizujeme.cz/clanky/wi-fi-direct-objevte-moznosti-nove-technologie-vedecke-okenko/

[12] Pcworld.com: Wi-Fi Direct Could Be the Death of Bluetooth. [online]. [cit. 2012-03-18]. Dostupné z: http://www.pcworld.com/businesscenter/article/173699/wifi_direct_ could_be_the_death_of_bluetooth.html

[13] Stericsson.com. [online]. [cit. 2012-03-18]. Dostupné z: http://www.stericsson.com/ sales_marketing_resources/WiFi-Direct_versus_Bluetooth-HS_English.pdf

[14] Svethardware.cz - Jak zapojíme síť: WiFi bez tajemství: Zisk, signál a pokrytí. [online]. [cit. 2012-04-05]. Dostupné z: http://www.svethardware.cz/art_doc-121AB59EC9127B44C12570A60045C902.html

[15] Svethardware.cz: Historie Wi-Fi: od FHSS k bezdrátu. [online]. [cit. 2012-03-18]. Dostupné z: http://www.svethardware.cz/art_doc-E8854472EA5653EBC1257636003B0 3D0.html

[16] UBIK, Sven. Monitorování vysokorychlostních počítačových sítí. [online]. [cit. 2012-04-02]. Dostupné z: https://wiki.man.poznan.pl/perfsonar-mdm/images/perfsonar-mdm/7/75/Ubik-text_M.pdf

[17] Ultrabooknews.com. [online]. [cit. 2012-04-20]. Dostupné z: http://ultrabooknews.com/2012/03/13/how-to-intel-my-wifi-wifi-direct-on-an-ultrabook/

[18] VAUGHAN-NICHOLS. Wi-Fi Protected Setup is Busted. [online]. [cit. 2012-03-25]. Dostupné z: http://www.zdnet.com/blog/networking/wi-fi-protected-setup-is-busted/1808

[19] Wi-Fi Alliance: Certified Produkts. [online]. [cit. 2012-03-23]. Dostupné z: http://certifications.wi-fi.org/search_products.php

[20] Wi-Fi Alliance: How far will a Wi-Fi Direct connection travel?. [online]. [cit. 2012-04-22]. Dostupné z: http://www.wi-fi.org/knowledge-center/faq/how-far-will-wi-fi-direct-connection-travel

[21] Wi-Fi Alliance: Wi-Fi CERTIFIED™ Makes It Wi-Fi. [online]. [cit. 2012-03-18]. Dostupné z: http://www.wi-fi.org/sites/default/files/membersonly/ WFA_Certification_Overview_WP_en.pdf#overlay-context=knowledge-center/white-papers/overview-wi-fi-alliance-approach-certification-2006

[22] Wi-Fi Alliance: White Papers. [online]. [cit. 2012-03-18]. Dostupné z: http://www.wi-fi.org/knowledge-center/white-papers/wi-fi-certified-wi-fi-direct%E2%84%A2-personal-portable-wi-fi%C2%AE-connect-devices

[23] Wi-Fi Direct adds Peer-to-Peer Capabilities. *Digi-key.com* [online]. [cit. 2012-04-05]. Dostupné z: http://www.digikey.com/us/en/techzone/wireless/resources/articles/Wi-Fi-Direct-adds-Peer-to-Peer-Capabilities.html

[24] Wi-fiplanet.com: Understanding Ad Hoc Mode. [online]. [cit. 2012-03-18]. Dostupné z: http://www.wi-fiplanet.com/tutorials/article.php/1451421/Understanding-Ad-Hoc-Mode.htm

[25] Wifinetnews.com: Wi-Fi Alliance Peers into the Future with Ad Hoc Replacement. [online]. [cit. 2012-04-20]. Dostupné z: http://wifinetnews.com/archives/2009/10/wifi_direct_peering.html

[26] ZANDL, Patrick. *Bezdrátové sítě Wi-fi : Praktický průvodce*. Vydání první. Brno : Computer Press, 2003. 190 s. ISBN 80-7226-632-2.

Pojmy

AMP – Alternace MAC/PHY je označení sekundárního spojení užívaného u nejnovějších Bluetooth standardů

AP – access point je aktivní síťový prvek, který v infrastrukturní síti slouží jako řídící prvek

Ad hoc – způsob bezdrátového spojení tzv. peer-to-peer

Beacon frame – návez odvozený z anglického „beacon (maják)“ slouží k posílání časových razítek k zajištění synchronizace zařízení v síti

Bluejacking – jedná se o zasílání nevyžádaných zpráv pomocí technologie Bluetooth

DSSS – Direct Sequence Spread Spectrum je princip modulace u Wi-Fi sítí

FHSS – Frequency Hopping Spread Spectrum je princip modulace používaný u Wi-Fi

GC – Group Client je označení pro zařízení, které se pomocí Wi-Fi Direct spojení připojuje ke GO

GO – Group Owner je označení pro zařízeni, které ve Wi-Fi Direct spojení iniciuje spojení

IBSS – Independent Basic Service Set je zkratka označující Ad-hoc mód

ICMP – je protokol síťové vrstvy užívaný pro posílání chybových zpráv

IrDA – Infrared Data Association je bezdrátová technologie využívající infračervené světlo

MIMO – Multiple In Multiple Out je způsob radiové komunikace, který se používá k zvýšení přenosové rychlosti za pomoci vícecestného šíření signálu

OFDM – Orthogonal Frequency Division Multiplexing je širokopásmá modulace užívaná u WiFi sítí

STA – STAtion je označení pro koncová síťová zařízení

Wi-Fi – Wireless Fidelity je bezdrátová technologie vytvořená Wi-Fi Aliancí

Wi-Fi Aliance – nezisková organizace skládající se z několika certifikačních (testovacích) středisek

WLAN – Wireless Local Area Network je bezdrátová síť působící na malém geografickém území (např. domácnosti, malé firmy)

WMAN – Wireless Metropolitan Area Network je bezdrátová síť, geograficky větší než **WLAN**, která má rozsah od několika bloků až po celé město

WPAN – Wireless Personál Area Network je velmi malá bezdrátová síť, která pokrývá pouze pracovní prostředí jedné osoby

WPS – Wireless Protected Setup je Wi-Fi standard umožňující snadné vytvoření bezdrátového spojení

WWAN – Wireless Wide Area Network je rozsáhlá bezdrátová síť, která svým rozsahem překračuje hranice měst, dokonce i hranice států