Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

Technologie WiFi Direct a její praktické využití

Bakalářská práce

Tomáš Starý

Vedoucí práce: Ing. Rudolf Vohnout

České Budějovice 2014

Bibliografické údaje

Starý T., 2014: Technologie WiFi Direct a její praktické využití. [WiFi Direct Technology and its practical use. Bc. Thesis, in Czech.] – 44 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Cílem této bakalářské práce je zjistit praktické využití technologie Wi-Fi Direct na základě experimentálního ověření, které bude probíhat prostřednictvím dvou mobilních zařízení. Na těchto zařízeních bude provedena základní analýza vlastností sítě a naměřené výsledky budou porovnány s teoretickými hodnotami technologií Ad-hoc a BlueTooth. Prostřednictvím tohoto porovnání určíme, kde bychom tuto novou technologii mohli v praxi využít.

Annotation

The aim of this bachelor thesis is to determine the possibilities of practical usage of Wi-Fi Direct technology based on experimental verification which will be carried out using two mobile devices. Basic analysis of network properties will be performed on these two devices and the measured results will be compared with the theoretical values of Ad-hoc and BlueTooth technologies. We will determine where this new technology could be used in practice based on this comparison.

Klíčová slova

Wi-Fi, Wi-Fi Direct, Ad-hoc, BlueTooth

Keywords

Wi-Fi, Wi-Fi Direct, Ad-hoc, BlueTooth

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 stejnou 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 ..... dne ..... Podpis autora

Poděkování

Rád bych poděkoval panu Ing. Rudolfu Vohnoutovi, nejen za to že mě umožnil zabývat se tímto zajímavým tématem, ale hlavně za odborné rady a celkovou korekturu práce. Také bych rád poděkovat svým přátelům a rodině za velikou podporu při tvorbě práce, bez kterých by byly určité pasáže této práce těžko proveditelné.

Obsah

Úvod

Technologie bezdrátové komunikace pro tvorbu lokálních sítí je tu s námi již dlouhou dobu, ale masový rozvoj nastal až koncem devadesátých let 20. století a to především kvůli zvýšení rychlostí dosavadních standardů bezdrátové komunikace a velkému rozvoji mobilních zařízení. V poslední době vliv bezdrátové komunikace ještě vzrostl a téměř každé elektronické zařízení má v sobě zabudovaný čip pro bezdrátovou komunikaci, který nám umožňuje připojit se k lokální síti téměř všude. Bezdrátová komunikace je oblíbená především kvůli své jednoduchosti a mobilitě, díky které se můžeme uvnitř sítě volně pohybovat a nemusíme být neustále připojeni k metalickému vedení. Budování rozsáhlých sítí pomocí metalického vedení je cenově náročné a proto pro většinu lidí představuje bezdrátová komunikace nejlepší možné řešení přístupu k internetu.

Jednou z nejpoužívanějších technologií bezdrátové komunikace dnešní doby je technologie Wi-Fi, kterou popisuje standard IEEE 802.11. Tato technologie je tvořena dvěma základními architekturami sítě a to infrastrukturní a takzvaným módem Ad-hoc. Obě tyto architektury se velice liší a každá z nich se používá pro jiný případ komunikace. Architektura infrastrukturní sítě je tvořena pomocí přístupových bodů, které jsou nejčastěji zastoupeny takzvanými Wi-Fi routery, které kombinují funkce přístupového bodu, routeru a switche. Pomocí těchto zařízení je možné se do sítě připojit a využívat přístup k internetu a k ostatním zařízením sítě. Zatímco architektura Ad-hoc žádné přístupové body pro připojení do sítě nevyužívá. Tato architektura je tvořena již koncovými zařízeními, která spolu komunikují přímo. Architektura Ad-hoc je využita především v mobilních zařízeních, u kterých je potřeba vytvoření lokální sítě bez přístupového bodu daleko vyšší.

Další velmi oblíbenou bezdrátovou technologií mobilních zařízení je technologie Bluetooth, která umožňuje vytvářet dočasné lokální sítě. Bluetooth se nejčastěji využívá pro přenos malých dat a připojení vstupních zařízení k pracovním stanicím. Mnohem novější technologií, která nevyužívá žádného přístupového bodu je technologie Wi-Fi Direct. Tuto technologii představila Wi-Fi Alliance v roce 2010 na celosvětově známém veletrhu CES v Las Vegas. Tento druh spojení umožňuje každé zařízení, jehož součástí je Wi-Fi čip a jeho ovladače mají podporu Wi-Fi Direct. Mezi hlavní představitele této technologie patří především síťové tiskárny a mobilní zařízení. Právě tímto druhem spojení se zabývá tato bakalářská práce, která má za úkol zjistit provozní parametry této technologie na základě experimentálního měření a následně výsledky porovnat s ostatními specifikacemi nejpoužívanějších bezdrátových technologií.

1. Metodika

- Získání informací o technologiích bezdrátové komunikace pro lokální sítě.
- Výběr zařízení, která podporují technologii Wi-Fi Direct.
- Výběr správného místa, které nebude podléhat rušení okolních sítí.
- Stanovení parametrů pro porovnání technologií.
- Výběr aplikací pro měření vlastností sítě.
- Vytvoření lokální sítě prostřednictvím technologie Wi-Fi Direct.
- Měření vlastností sítě.
- Porovnání bezdrátových technologií.

Omezující podmínky

- Menší výkon bezdrátových adaptérů v dostupných mobilních zařízeních.
- Proměnlivé počasí.
- Malá aplikační podpora technologie Wi-Fi Direct.
- Nastavení mobilních zařízení.

2. Bezdrátová komunikace v lokálních sítích

Bezdrátová komunikace je druh komunikace, který pro spojení dvou či více zařízení nevyužívá metalické ani optické vedení, ale přenáší informaci vzduchem pomocí rádiového rozhraní. Toho můžeme využít v místech, kde nelze zavést metalické vedení nebo v případě potřeb uživatelů sítě na mobilitu koncových zařízení. Přenos informace vzduchem sebou ovšem nese i nějaké nevýhody. Mezi hlavní nevýhody patří bezpečnost, která je velice náchylná na odposlech informací. Problém s odposlechem na bezdrátové síti se řeší pomocí šifrování přenášené informace, ale ani šifrování nám nezajistí úplnou bezpečnost přenosu. Další velkou nevýhodou je rušení signálu, ke kterému dochází z důvodů velkého obsazení radiových frekvencí, které jsou provozovány na bezlicenčním frekvenčním pásmu. V lokálních bezdrátových sítích se jedná především o frekvence 2.4GHz a 5GHz, na kterých pracuje mnoho běžných zařízení, jako jsou například bezdrátové klávesnice, myši, kamery ale také i mikrovlnné trouby. Dalším problémem je překrývání okolních sítí. Tento problém se řeší při prvotním nastavení přístupového bodu správnou volbou kanálu pro bezdrátovou komunikaci. [1]

Druhy bezdrátové komunikace pro lokální sítě:

- Wi-Fi
  - Infrastrukturní síť
  - Ad-hoc
  - Wi-Fi Direct
- BlueTooth

2.1 Technologie Wi-Fi

Technologie Wi-Fi byla vynalezena v roce 1991 v nizozemském městě Nieuwegein firmou NCR Corporation/AT & T, která jako první použila bezdrátovou technologii 802.11 ve svých produktech WaveLan. Této technologie se ujal Vic Hayes, který byl později nazván otcem technologie Wi-Fi, jenž byl u samého počátečního vyjednávání s organizací IEEE, která usiluje o vzestup nových technologií souvisejících s elektrotechnikou. Technologii Wi-Fi, takovou jakou ji známe dnes, založila společnost Wireless Ethernet Compatibility Alliance, která v roce 1999 vyvinula standard IEEE 802.11b. Celý název této technologie zněl IEEE 802.11b Direct Sequence a proto se Wi-Fi alliance rozhodla v roce 2000 tento název změnit. Najala poradenskou firmu Interbrand Corporation, která vymyslela dnešní podobu názvu této bezdrátové technologie a to název Wi-Fi. Později bylo uvedeno, že název Wi-Fi vzniknul ze slovní hříčky Hi-Fi, což je zkratka slov High fidelity. Název Wi-Fi byl již veřejností daleko více oblíben, což bylo hlavním cílem této změny. [2] Logo této technologie je zobrazeno na obrázku číslo 2.1.

Klasické Wi-Fi sítě jsou složeny z přístupového bodu takzvaného access pointu a z klientských stanic. Tento přístupový bod rozesílá do okolí svoje identifikační jméno SSID, které je šířeno prostřednictvím beacon frame každých 100ms. Při zachycení více takovýchto identifikátorů si klient může vybrat, ke kterému přístupovému bodu se připojí. Při šíření stejného SSID prostřednictvím více přístupových bodů si opět klient může vybrat, ke kterému přístupovému bodu se připojí a to především na základě síly signálu. Technologie Wi-Fi nijak neřídí připojení ke konkrétnímu přístupovému bodu a rozhodnutí vždy ponechá zcela na uživateli koncového zařízení. Tato vlastnost má ale i své nevýhody, které mohou zapříčinit kolizi na sdíleném médiu, a proto technologie Wi-Fi používá protokol CSMA/CA k řízení přístupu k tomuto sdílenému médiu. [3]

Obrázek 2.1: Logo technologie Wi-Fi [2]

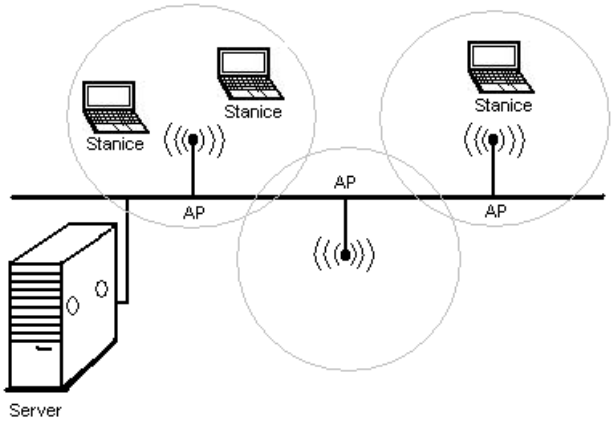
2.1.1 Topologie

Topologie sítě Wi-Fi určuje strukturu lokální bezdrátové sítě. Dělí se na dva základní typy podle způsobu komunikace mezi takzvanými Basic Service Set, což jsou základní soubory služeb v sítích 802.11. Jedná se o množinu zařízení, mezi kterými probíhá komunikace v území, které je dáno průniky dosahů signálu. Tyto území jsou nazývány Basic Service Area, které umožňují zařízením, právě v tomto prostoru, komunikovat s ostatními členy BSS. Lokální bezdrátové sítě tvoří infrastrukturní sítě a sítě Ad-hoc, které jsou určeny spíše pro dočasné použití.

Infrastrukturní sítě

Tento druh sítí je tvořen přístupovými body, o kterých již byla zmínka v kapitole 2.1. Přístupové body tvoří strukturu dané sítě, ve které zajišťují rozhraní mezi metalickou a bezdrátovou sítí. Jedná se o datový most mezi těmito rozhraními, což můžete vidět na obrázku číslo 2.2, kde jsou přístupové body znázorněny jako zařízení AP. Přístupový bod také umožňuje komunikaci mezi více stanicemi bez nutnosti používat rozhraní mezi metalickou a bezdrátovou linkou. Data, která putují mezi těmito dvěma koncovými stanicemi, procházejí nejdříve přístupovým bodem, který data zpracuje a následně je přepošle na příslušnou cílovou stanici. V případě, že je stanice v dosahu signálu přístupového bodu, je schopna komunikovat s každou další stanicí. V infrastrukturní síti jsou nároky na spojovací

kapacitu převedeny z koncových zařízení na přístupový bod, což je výhodné především z důvodu šetření baterie na přenosných zařízeních. V případě druhého typu spojení módu Ad-hoc tomu tak není. Zařízení pracující právě v tomto módu musí udržovat komunikaci s ostatními zařízeními samy, a tudíž jsou nároky, které byly v předchozím případě kladeny na přístupový bod převedeny na samotná koncová zařízení, které spolu komunikují. [4]



Obrázek 2.2: Infrastrukturní síť [5]

Ad-hoc sítě

Tento druh sítí je tvořen pouze koncovými stanicemi, které pro komunikaci mezi sebou nevyužívají žádné další síťové prvky. Tyto sítě jsou využívány především v mobilních zařízeních, kterým umožňují vytvořit dočasnou lokální síť, díky které je možno ihned sdílet různé druhy dat. Více se tomuto druhu spojení budeme věnovat v samostatné kapitole.

2.1.2 Standardy technologie Wi-Fi

Základním standardem této bezdrátové technologie je standard IEEE 802.11, který byl dále rozšiřován a vylepšován. Tento standard umožňoval kódování infračervené, FHSS a DSS při rychlostech komunikace 1 Mb/s až 2 Mb/s a byl chráněn metodou zabezpečení WEP, která zajišťovala v bezdrátových sítích stejnou ochranu jako nešifrovaný přenos v sítích s metalickým vedením. Nyní si stručně popíšeme jednotlivá rozšíření bezdrátových sítí IEEE 802.11.

IEEE 802.11b

Rozšíření původního standardu 802.11, které umožnilo komunikaci pouze prostřednictvím kódování DSSS. Došlo ovšem ke zvýšení rychlostí a to z 1 a 2 Mb/s na 5,5 a 11 Mb/s. Tento standard stejně jako jeho předchůdce pracuje na frekvenčním pásmu 2,4GHz.

IEEE 802.11a

Tento nový standard pracuje na vysokofrekvenčním pásmu 5GHz, což sebou přináší rapidní zvýšení rychlostí a to na 6, 9, 12, 18, 24, 36, 48, 54 Mb/s. Změna frekvenčního pásma na vyšší frekvenci ovšem také přináší menší dosah signálu a menší kompatibilitu s ostatními zařízeními, které na těchto frekvencích neuměly pracovat.

IEEE 802.11c

Toto rozšíření nedefinuje nové frekvenční pásma ani zvětšování rychlostí, ale zaobírá se problematikou přemosťování. Přístupový bod, jak už jsme si řekli, slouží jako datový most mezi metalickou a bezdrátovou sítí a tento standard definuje, jak tyto přístupové body získávají potřebné adresy v oné bezdrátové síti.

IEEE 802.11d

Rozšiřující standard IEEE 802.11d přidává do fyzické vrstvy funkce, díky kterým jsou přístupové body schopny určit, v jaké se nalézají zemi a podle toho uzpůsobit povelené frekvence, čímž zajistí legální využití tohoto zařízení v konkrétní zemi.[6]

IEEE 802.11e

Tento standard přináší do rodiny IEEE 802.11 podporu takzvaných QoS mechanizmů, díky kterým můžeme upřednostnit určité aplikace jako je zvuk nebo video prostřednictvím bezdrátových sítí LAN. Více se o tomto standardu dočtete v článku [7].

IEEE 802.11g

Rozšíření IEEE 802.11g je standard z roku 2003, který pracuje na frekvenčním pásmu 2,4 GHz s dvěma druhy modulace dat. Prvním typem modulace je DSSS, která je použita již ve starších standardech a je zde hlavně z důvodu zpětné kompatibility a druhým typem modulace je OFDM, kterou můžeme znát ze standardu IEEE 802.11a. Tato modulace nám umožnuje dosáhnout přenosových rychlostí až okolo 54 Mb/s. [8]

IEEE 802.11h

Rozšíření IEEE 802.11h pracuje pouze na frekvenčním pásmu 5GHz a umožňuje uživatelům, kteří se nacházejí v blízkosti přístupového bodu snížit spotřebu energie pomocí funkce TPC. Dále přidává takzvanou funkci DFS, která v případě zjištění kolize signálů zajistí přepnutí na jiný přenosový kanál.

IEEE 802.11i

IEEE 802.11i rozšiřuje stávající rodinu bezpečnostních protokolů o protokol TKIP a standard AES, které zaručují zvětšení bezpečnosti oproti starému zabezpečení WEP. Součástí této specifikace je také standard 802.1x, který zabezpečuje

ověřování klientů přímo na přístupových bodech a možnost ověřování pomocí konkrétních portů. [6]

IEEE 802.11n

Tento standard, který byl vydán v roce 2009, podporuje frekvenční pásma 2,4GHz a 5GHz. Standard opět využívá modulace OFDM s podporou takzvaného modelu MIMO, který umožňuje zvýšení dosavadních rychlostí z 54 Mb/s až na 600 Mb/s. Tato rychlost je ale pouze teoretická a reálné hodnoty se pohybují okolo 100 Mb/s.

IEEE 802.11ac

IEEE 802.11ac umožňuje komunikaci pouze ve frekvenčním pásmu 5GHz při modulaci dat OFDM. Toto rozšíření vychází ze standardu IEEE 802.11n, u kterého rozšiřuje model MIMO na takzvaný MU-MIMO, což umožňuje dosahovat rychlostí až kolem 1,3Gb/s. [9]

IEEE 802.11ad

IEEE 802.11ad také nazývaný jako WiGig využívá 60GHz frekvenčního pásma, což má za následek velice malý dosah signálu od přístupového bodu. Tento dosah signálu se bude pohybovat okolo 10 metrů od přístupového zařízení. Svůj malý dosah bude tato technologie vynahrazovat přenosovou rychlostí, která by měla dosahovat až zázračných 5Gb/s. Standard IEEE 802.11ad by měl být dostupný až v roce 2015. [10]

2.1.3 Zabezpečení Wi-Fi sítí

Lokální bezdrátová komunikace je v dnešní době velice oblíbenou technologií, která je součástí každé moderní domácnosti. To sebou ovšem nese veliké bezpečnostní riziko pro uživatele a to především kvůli špatné znalosti zabezpečení těchto bezdrátových sítí. V případě špatně zabezpečené sítě mohou nastat případy, které budou porušovat zákony určité země a odpovědnost za tyto nezákonné činy jsou připisovány správci takovéto sítě. Proto je velice důležité mít bezdrátovou síť dobře zabezpečenou. Pro tyto případy máme několik možností jak bezdrátovou síť zabezpečit.

Skryté SSID

Jednou ze základních prevencí proti napadení lokální bezdrátové sítě, je skryté vysílání názvu. Název Wi-Fi sítí je označován jako takzvané SSID, které je vysíláno do okolí přístupovými body. Pro přístup do skryté sítě je nutné zadat přesný název, který byl nastaven při prvotním vytváření sítě. Tento bezpečnostní prvek ale není bezchybný a při cíleném skenování okolí lze i takto skryté sítě detekovat, a proto se tento druh zabezpečení využívá jen jako doplňková funkce k nějaké silnější formě zabezpečení.

Filtrování Mac adres

Každá síťová karta je opatřena unikátním číslem takzvanou Mac adresou, která jednoznačně identifikuje konkrétní zařízení. Tohoto lze využít a nastavit na přístupovém bodu jaká zařízení se do sítě mohou či nemohou připojit. V případě, že se pokusí připojit zařízení, které nemá svou Mac adresu zanesenou do množiny povolených zařízení, nastane fáze zablokování a odepření přístupu do bezdrátové sítě. V dnešní době se ale i tato technika zabezpečení dá obejít a to takzvanou metodou duplikování Mac adresy, která je v seznamu povolených zařízení zanesena. Proto je opět doporučena jen jako doplňková funkce, která by měla být doplněna šifrováním komunikace. [11]

Šifrování komunikace

Nejbezpečnější metodou, která se v bezdrátových sítích používá, je metoda šifrování paketů, které proudí mezi jednotlivými bezdrátovými zařízeními. Mezi základní druh šifrování patří protokol WEP, který je založen na symetrickém šifrování. Odposlechem dostatečného množství dat lze v reálném čase tento symetrický klíč dešifrovat.

Z těchto důvodu byl již v roce 2003 vydán nový standard WPA. Tento standard již nevyužívá statické šifrování, které je největší slabinou předchozího protokolu. Protokol WPA používá takzvanou technologii TKIP, která prostřednictvím přístupového bodu mění v určitém časovém intervalu klíče, které následně šifruje klíčem starým. Na rozdíl od protokolu WEP umožňuje delší šifrovací klíče, které se dynamicky mění a silnější autentizaci uživatele.

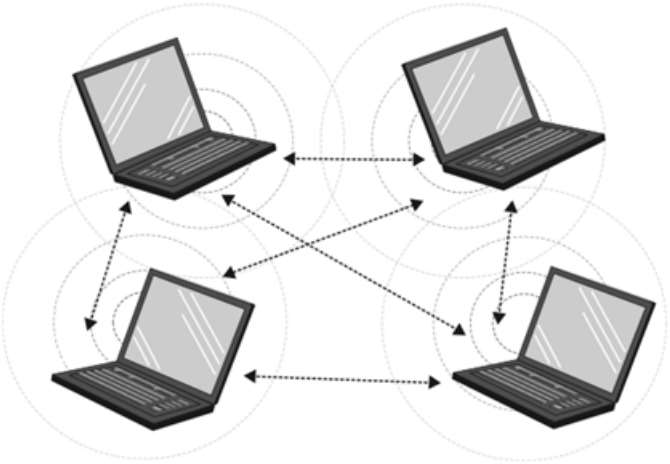
Technologie WPA, která byla Wi-Fi Alliancí vytvořena jako dočasné řešení problému protokolu WEP, byla v roce 2004 nahrazena novým zabezpečením WPA2. Tato forma zabezpečení již nevyužívá algoritmus RC4 ale nový algoritmus AES, který je dnes považován za relativně bezpečný. Algoritmus funguje ve čtyřech krocích, ve kterých dochází mezi klientem a přístupovým bodem k předání druhého klíče, což brání bezdrátovou komunikaci proti většině typů útoků. [12]

2.2 Sítě Ad-hoc

Sítě Ad-hoc jsou sítě tvořeny pouze koncovými zařízeními, které jsou vybaveny bezdrátovým Wi-Fi adaptérem a komunikují mezi sebou prostřednictvím bezdrátového média. Tyto sítě nepotřebují pro komunikaci žádného prostředníka a právě proto jsou také jinak nazývány jako nezávislé sítě. Ad-hoc sítě propojují koncová zařízení takzvaně peer-to-peer, což znamená, že jsou si všechny propojené zařízení rovny. Koncová zařízení, která spolu chtějí komunikovat, musí být v relativně malém rádiovém dosahu, což je znázorněno na Obrázku 2.3

Ad-hoc sítě jsou určeny pro malé sítě, které zahrnují jen několik koncových stanic, které nejsou od sebe příliš vzdáleny. Tohoto můžeme využít jen v relativně malém prostoru kde je vzájemný radiový dosah zajištěn. Sítě tohoto druhu jsou na rozdíl od infrastrukturních sítí nejčastěji vytvořeny jen na omezenou dobu,

potřebnou pro uskutečnění samotné komunikace mezi bezdrátovými zařízeními. Touto komunikací je míněno sdílení dat, sdílení internetu, nebo hraní počítačových her. Nezávislé sítě v dnešní době nejsou příliš používané a ne jenom kvůli svému malému dosahu a dočasnému použití, ale především kvůli složitější konfiguraci, kterou nemusí zvládnou každý uživatel koncových zařízení. U infrastrukturní sítě se o tuto konfiguraci stará přístupový bod, na kterém je spuštěn DHCP server, jenž doručí správnou konfiguraci připojení na koncové zařízení bez vnějšího zásahu uživatele. [4]



Obrázek 2.3: Ad-hoc síť složená ze čtyř stanic [13]

2.2.1 Princip sítí Ad-hoc

Bezdrátová zařízení, která jsou připojena do infrastrukturních sítí, přenášejí veškerou zodpovědnost za průběh komunikace na přístupový bod. U sítí Ad-hoc tomu takto není a celá zodpovědnost zůstává na koncových zařízeních, které musí průběh komunikace zajistit samy. Zvětšená zodpovědnost u koncových zařízení spočívá hlavně na Mac podvrstvě, která je určena pro komunikaci mezi fyzickou vrstvou a hostitelským zařízením.

Bezdrátová stanice, která zakládá IBSS, začne vysílat beacon frame, což jsou data obsahující informace o síti a slouží pro udržení synchronizace mezi stanicemi. Na rozdíl od infrastrukturních sítí, kde beacon vysílá pouze přístupový bod, jsou v sítích Ad-hoc beacony vysílány každou bezdrátovou stanicí. Všechna zařízení, která se připojí do Ad-hoc sítě, musí posílat beacon opakovaně, pokud neobdrží beacon z jiné stanice ve velmi krátkém náhodném časovém úseku. Jestliže stanice neobdrží beacon během náhodného zpoždění předpokládá, že další stanice nejsou aktivní a je potřeba odeslat beacon znovu. Po obdržení signálu každá stanice aktualizuje své místní vnitřní hodiny s časovou značkou, která se nachází v beacon framu. Tím je zajištěno, že všechny stanice jsou schopny provádět operace ve stejnou dobu. [16]

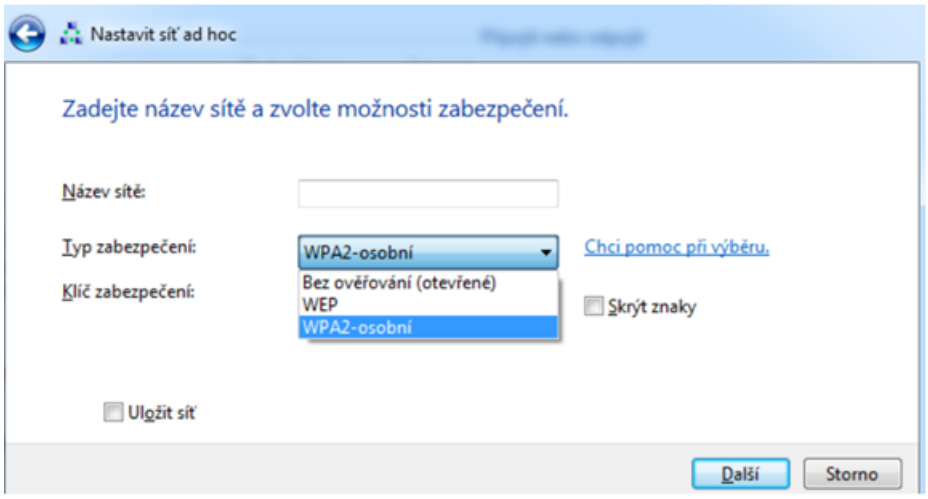
2.2.2 Konfigurace sítě

Pro konfiguraci bezdrátové sítě v režimu Ad-hoc, je zapotřebí vlastnit alespoň dvě koncová zařízení, které obsahují bezdrátový adaptér a mít dostatečné zkušenosti s ručním nastavením bezdrátového připojení. Na prvním zařízení, které je vybráno pro vytvoření sítě, se nastaví IP adresa a maska sítě. Také je nutné nastavit název sítě a popřípadě přihlašování pomocí hesla. U druhého bezdrátového zařízení je nutné nastavit jinou IP adresu, která bude ovšem ze stejného rozsahu jako IP adresa zakládajícího bezdrátového zařízení. Nastavení nám zaručí, že nedojde ke konfliktům kvůli stejným IP adresám. Poté druhé zařízení pomocí vyhledávání bezdrátových sítí nalezne námi vytvořenou síť, ke které se po zadání správného hesla připojí. Pokud předchozí nastavení bylo učiněno správně, mělo by být již možné sdílet data s ostatními připojenými zařízeními. [14]

2.2.3 Bezpečnost

Bezpečnost sítí Ad-hoc je daleko komplikovanější než u infrastrukturních sítí především kvůli obtížné autorizaci, která u sítí bez infrastruktury má problémy s určením identity uživatele. Nicméně Ad-hoc sítě je možné rozšířit o velice dobré autentizační mechanizmy. Mezi takovéto mechanizmy patří například výměna klíčů Diffie-Hellman více stranami, která je autentizovaná heslem.

Šifrování dat je v Ad-hoc sítích další velký problém, který ale lze řešit právě pomocí autentizačních mechanizmů. Tyto mechanizmy umožňují zabezpečit komunikaci prostřednictvím dostupných klíčů. Teprve s příchodem zabezpečení WPA2 lze tento druh sítí plnohodnotně zabezpečit, což nám umožnuje proces autentizace, který je u WPA2 složen ze čtyř zpráv pro přístup a předání klíče PMK, který se používá při odvození dynamických šifrovacích klíčů. [15]



Obrázek 2.4: Zabezpečení sítě Ad-hoc v operačním systému Windows 7

V operačním systému Windows lze zvolit při vytváření Ad-hoc sítě druh zabezpečení WEP, WPA2-osobní nebo možnost „Bez ověřování“ což znamená, že vytvořená síť nebude vyžadovat pro přístup žádné heslo. Nastavení metod zabezpečení v operačním systému Windows 7 je znázorněno na Obrázku 2.4.

2.2.4 Sdílení internetu

Při vytváření sítě Ad-hoc lze provést několik snadných uprav v nastavení, které povolí sdílení internetu prostřednictvím této sítě. Úpravy se týkají pouze zařízení, které obsahují dva síťové adaptéry, protože mód Ad-hoc neumožňuje připojit zařízení prostřednictvím stejného bezdrátového adaptéru do dvou sítí zároveň. Tato nevýhoda je řešena připojením zařízení, které slouží pro sdílení internetu do sítě Ad-hoc pomocí metalického vedení. Příliš komplikované nastavení a nutnost připojení k metalickému vedení je pro většinu uživatelů hlavní překážkou pro použití sdílení internetu prostřednictvím Ad-hoc sítí. Z tohoto důvodu se pro bezdrátové připojení k internetu využívá hlavně infrastrukturní síť, která tyto nevýhody eliminuje.

2.3 BlueTooth

BlueTooth je jednou z nejpopulárnějších bezdrátových technologií, která se využívá pro komunikaci na malé vzdálenosti. Technologie BlueTooth spadá pod standard IEEE 802.15.1. Její oblíbenost spočívá především v malé ceně, miniaturní velikosti a jednoduchosti konfigurace spojení.

Obrázek 2.5: Logo technologie BlueTooth [25]

Komunikace prostřednictvím této technologie probíhá stejně jako u Wi-Fi na frekvenčním pásmu 2,4 GHz. Přesný rozsah využívaných frekvencí je od 2,4 – 2,483 GHz, který je na rozdíl od technologie Wi-Fi rozdělen na 79 kanálů po 1 MHz. Přenos pomocí této technologie využívá takzvanou metodu FHSS, která při přenosu dat mění frekvence až 1600 krát za sekundu. Tento princip zajišťuje probíhající komunikaci daleko větší odolnost vůči rušení na stejném frekvenčním pásmě. Standard BlueTooth definuje tři třídy zařízení. Tyto třídy jsou rozděleny podle maximálního výstupního výkonu a určují tak maximální dosah komunikace, který se pohybuje od 10 metrů až do 100 metrů s přímou viditelností. V případě komunikace přes překážky jakou jsou například zdi, se vzdálenost značně snižuje až na jednotky maximálně desítky metrů. Komunikace pomocí technologie BlueTooth umožnuje spojení dvou nebo více zařízení. Takovéto sítě, které obsahují více zařízení, se nazývají piconet. Síť tvoří jedno hlavní zařízení, které řídí celkovou komunikaci v síti a zařízení podřízené, které síť využívá pouze pro spojení s ostatními. Síť piconet může tvořit sedm podřízených zařízení, které jsou aktivní a další mohou být v pohotovostním režimu. Všechna zařízení v rámci piconetu musí s hlavním zařízením udržovat synchronizaci frekvencí a metodu přeladování kmitočtů. Zařízení v rámci piconetu mohou být součástí i jiné sítě piconet a to včetně hlavního zařízení. To ovšem v ostatních sítích nemůže plnit roli hlavního

zařízení, ale pouze podřízeného. Prostřednictvím tohoto prolínání sítí je tvořena síť scatternet, která může obsahovat až 10 sítí piconet. [25]

2.3.1 Bezpečnost BlueTooth

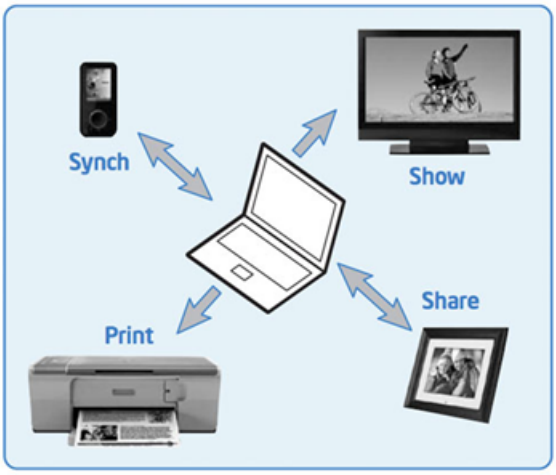
Pro zajištění bezpečnosti technologie blueTooth, je využita celá řada mechanizmů, které mohou pro zabezpečení komunikace využívat různé principy autentizace a šifrování. Při vytváření spojení mezi jednotlivými zařízeními se musí nejdříve na zařízení zapnout funkce vyhledávání, která zobrazí všechny okolní zařízení. Aby se zařízení mohly detekovat, musí být nastaveny v režimu viditelnosti a v případě vyžádání předají potřebné informace pro vytvoření sítě. Mezi takovéto informace patří například název a třída zařízení, seznam služeb a technické informace, které zahrnují výrobce a používanou specifikaci BlueTooth. Všechny zařízení obsahují unikátní 48bitobou adresu. Zařízení, které zakládá spojení, musí požádat druhé zařízení o navázání komunikace. Posléze uživatelé obou zařízení musí vyplnit společný tajný klíč, prostřednictvím kterého dojde k navázání komunikace. Pro další možnou komunikaci již klíč není potřeba a autentizace probíhá plně automaticky. V případě, že chceme ukončit synchronizaci obou zařízení, může se klíče ze zařízení odstranit a při dalším navázání komunikace bude klíč opět vyžadován. Prostřednictvím autentizace lze předejít nežádoucímu přístupu k datům a pomocí šifrování se mohou ochránit data před odposlechem, který je u bezdrátových komunikací velkým problémem. [25] Podrobnější popis zabezpečení technologie BlueTooth lze nalézt v publikaci [15].

Bezpečnostní slabiny

- Krátký Pin kód, který je ve většině případů čtyřmístný, což je velice málo možných kombinací
- Distribuce Pin kódu, která je ve větších sítí špatně proveditelná
- Délka šifrovacího klíče – ve většině případů je vybrána minimální možná délka klíče
- Klíč zařízení je veřejně dostupný
- Hlavní klíč je sdílený
- Slabá autentizace, která je založena na základě výzvy a odpovědi, neautentizují se uživatelé, ale pouze zařízení
- Zabezpečení je určeno pro spojení BlueTooth zařízení, nikoli pro koncovou komunikaci [15]

2.4 Wi-Fi Direct

Wi-Fi Direct je poměrně nová technologie, která byla představena Wi-Fi aliancí v roce 2010 na veletrhu CES, který se konal v Las Vegas. Technologie je také nazývána jako Wi-Fi Peer-To-Peer což znamená, že pro spojení mezi zařízeními nepotřebuje žádného prostředníka jako je například přístupový bod v infrastrukturních sítích. Spojení několika různých zařízení, které využívají komunikaci prostřednictvím technologie Wi-Fi Direct je zobrazeno na obrázku 2.6.



Obrázek 2.6: Spojení zařízení prostřednictvím sítě Wi-Fi Direct [17]

Jedná se o softwarovou nadstavbu nám již dobře známé technologie IEEE 802.11, která je dnes obsažena téměř v každém zařízení. Softwarové rozšíření technologie Wi-Fi Direct je možné implementovat i do starších bezdrátových adaptérů, které tuto možnost komunikace získají prostřednictvím nových ovladačů s podporou technologie Wi-Fi Direct. Komunikace prostřednictvím této technologie bude stejně jako u standardu IEEE 802.11 možná na frekvenčních pásmech 2,4GHz a 5GHz. Pomocí Wi-Fi Direct technologie lze propojit dvě koncová zařízení, ale také zařízení v síti nebo ve skupině. Navíc je možno připojit koncová zařízení do sítě Wi-Fi a současně komunikovat s ostatními stanicemi prostřednictvím technologie Wi-Fi Direct, což starší velice podobná technologie Ad-hoc neumožňuje. Na rozdíl od technologie Ad-hoc, Wi-Fi Direct také umožnuje lepší možnosti zabezpečení, snadnější nastavení při vytváření sítě a daleko větší výkon, který by měl zajistit mnohonásobně větší přenosové rychlosti a dosah signálu. Technologii lze využít u nejrůznějších zařízení, jako jsou notebooky, mobilní telefony, multimediální přehrávače, herní konzole, televizory, tiskárny a další podobné zařízení, které umožňují sdílení dat, synchronizaci nebo bezdrátový tisk. [18]

2.4.1 Vytvoření sítě Wi-Fi Direct

Vytvořit síť prostřednictvím technologie Wi-Fi Direct je možné kdekoliv a kdykoliv, dokonce i když není dostupná síť Wi-Fi. Zařízení, které tuto technologii podporují, vysílají signál, díky kterému lze zobrazit dostupné stanice v jeho okolí a požádat je o navázání komunikace. Při obdržení pozvánky do cizí sítě se uživatel může rozhodnout, zda pozvánku přijme či nikoli. V případě, že se rozhodne pozvánku přijmout, musí své rozhodnutí potvrdit prostřednictvím pop-up okna, které se uživateli zobrazí na hlavní obrazovce. Stejně jako u tradičních sítí Wi-Fi je doporučeno připojovat se pouze k sítím, které považujete za důvěryhodné. Výměna klíčů proběhne pomocí funkce Wi-Fi Protected Setup, která zajišťuje snadné a rychlé nastavení bezpečnosti. [19]

Jednotlivé kroky spojení:

1. Na zařízení, které vytváří spojení, zapneme funkci Wi-Fi Direct. Toto zařízení začne vyhledávat ostatní bezdrátová zařízení v jeho okolí, které podporují technologii Wi-Fi Direct prostřednictvím takzvaného Probe Request. Jedná se o speciální paket, který identifikuje kompatibilní zařízení v okolí.

2. Při nalezení druhého zařízení, vyšle prvotní zařízení požadavek na spojení.

3. Druhé zařízení na tento požadavek odpoví.

4. Navázání komunikace je potvrzeno Pin kódem. U nových zařízení lze potvrdit navázání komunikace i prostřednictvím technologie NFC, u které stačí obě zařízení k sobě přiložit.

Zařízení, které nemají dotykovou obrazovku ani klávesnici, nejsou schopny potvrdit navázání komunikace prostřednictvím Pin kódu. Jak již bylo zmíněno výše, novější zařízení s NFC čipem jsou schopny potvrdit komunikaci prostřednictvím přiblížení obou zařízení ale zařízení, která NFC čip neobsahují, budou potvrzovat navázání komunikace pomocí speciálního tlačítka. Mezi takovéto zařízení patří především tiskárny. [20]

2.4.2 Bezpečnost

Bezpečnost spojení prostřednictvím sítě Wi-Fi Direct pro většinu uživatelů znamená zadání Pin kódu nebo pouze přiblížení obou zařízení, ale jen málo kdo ví, jaké bezpečnostní mechanizmy skutečně chrání naši komunikaci. Bezpečnost u technologie Wi-Fi Direct je poměrně na dobré úrovni a to především díky tomu, že se ponaučila od podobných bezdrátových technologií, které doposud „chrání“ zastaralé metody šifrování. Využívá pro zabezpečení své komunikace prozatím velice bezpečný standard WPA2, jenž je hojně využíván i u infrastrukturních Wi-Fi sítí. Tento bezpečnostní standard implementuje schéma CCMP, které je založeno na šifrování AES. V současné době je standard WPA2 považován za jednu z nejbezpečnějších možností zabezpečení, a proto je komunikace prostřednictvím Wi-Fi Direct sítí velice bezpečná. [17]

2.4.3 Podporovaná zařízení

Všechny zařízení, které podporují technologii Wi-Fi Direct prochází důkladnou kontrolou ohledně bezpečnosti, spolehlivosti a interoperability, která umožnuje systémům efektnější spolupráci a vzájemnou výměnu služeb.[21] Výběr Wi-Fi CERTIFIED produktů umožňuje kombinovat zařízení od různých výrobců.

Obrázek 2.7: Mezinárodně uznávaná pečeť Wi-Fi CERTIFIED™ [22]

Volitelné certifikační mechanizmy ověřují další možné funkce jako je například snadný způsob nastavení, provoz peer-to-peer nebo zrcadlení obrazovky. Výrobky, které splňují tato přísná kritéria, jsou zveřejněny na stránkách Wi-Fi Aliance citedvacatadruha a jejich počet činí již 4589. Bohužel produkty podporující technologii Wi-Fi Direct se na našem trhu objevují velice pomalu a produkty z mezinárodního trhu nemusí vždy dostát slibovaným vlastnostem, jak uvádí autor bakalářské práce [23].

2.4.4 Wi-Fi Direct vs. BlueTooth 4.0

Bezdrátové technologie, které se používají pro komunikaci v rámci lokálních sítí, mezi sebou svádí neustálý souboj. Jak bylo již v předchozích kapitolách zmíněno technologie Ad-hoc se svým složitým nastavením a malou přenosovou rychlostí, která se pohybuje okolo 11 Mb/s není již moc využívaná. To technologie BlueTooth tvoří již velice oblíbený standard, který je známý svou jednoduchostí a vyšší přenosovou rychlostí. Nejnovější verze technologie BlueTooth 4.0 umožňuje komunikaci přenosovou rychlostí až 25 Mb/s. U méně známé technologie Wi-Fi Direct mají maximální přenosové rychlosti dosahovat až neuvěřitelných 250 Mb/s, což by znamenalo značné navýšení přenosových rychlosti v lokálních bezdrátových sítích. Tyto hodnoty jsou ovšem pouze teoretické a v reálném provozu těžko dosažitelné.

Stejně jako u přenosové rychlosti technologie Wi-Fi Direct zvýšila i vzdálenost dosahu signálu a to až na 200 metrů. Technologie BlueTooth ve své nejvyšší třídě umožňuje komunikaci maximálně do 100 metrů, což opět přispívá větší oblíbenosti Wi-Fi Direct. Nabízí se ovšem otázka, zda takto velké vzdálenosti jsou uživatelé lokálních sítí schopni využít.

Rozdíly těchto dvou velkých konkurentů jsou i v rámci zabezpečení. Zatímco BlueTooth 4.0 používá AES 128-bitové šifrování, tak Wi-Fi Direct spoléhá stejně jako standard Wi-Fi na zabezpečení WPA2, které využívá šifrování AES 256-bit. Obě dvě nové technologie tak poskytují dostatečné zabezpečení komunikace.

Spotřeba energie je u obou technologií velkou slabinou, a proto se tento problém snaží řešit novými metodami. Technologie BlueTooth používá takzvanou

nízkoenergetickou funkci, která novým čipům BlueTooth 4.0 umožní běh na malou baterii po dobu jednoho roku. Ovšem lze takto přenášet jen velice malá data a nelze komunikovat se staršími zařízeními, které nízkoenergetickou funkci neumožňují. Bude proto nutné, aby standard BlueTooth 4.0 neustále přepínal mezi nízkoenergetickou funkcí a normálním režimem komunikace. Na rozdíl od BlueTooth technologie Wi-Fi Direct bude podporovat takzvaný program WMM-Power Save, který slibuje zlepšení výdrže baterie až o 40 %.

Dalším rozdílem těchto technologií je zpětná kompatibilita se staršími zařízeními. Wi-Fi Direct umožňuje podstatně jednodušší zpětnou kompatibilitu především z toho důvodu, že se jedná o softwarové rozšíření stávajícího standardu Wi-Fi, který je obsažen v mnoha dnes používaných zařízeních. Wi-Fi aliance také slibuje, že pro komunikaci prostřednictvím Wi-Fi Direct bude stačit podpora jenom jednoho zařízení a druhé zařízení musí obsahovat pouze bezdrátový Wi-Fi adaptér. U technologie BlueTooth 4.0 bude zpětná kompatibilita o poznání složitější a to právě kvůli již zmiňované nízkoenergetické metodě komunikace. [24]

3. Technologie Wi-Fi Direct v praxi

Tato část bakalářské práce se zabývá samotnou specifikací technologie Wi-Fi Direct a jejím použitím v reálném provozu. Popisuje přesné postupy a použité prostředky, které jsou pro dosažení našeho cíle nezbytné.

3.1 Použité aplikace

Iperf

Jedná se o volně šiřitelnou aplikaci, která slouží k testování provozu na síti. Tato aplikace není určena pouze pro správce sítě, ale také pro obyčejné uživatele, kteří si chtějí zjistit potřebné informace o síti, na které se nacházejí. Program Iperf je dostupný pro platformy Windows, Linux, MacOS, iOS a Android. Pro obyčejné uživatele byla také vytvořena modifikace, která se jmenuje Jperf. Tato modifikace na rozdíl od základní verze programu umožňuje uživatelům jednoduché ovládání a grafický náhled na testování sítě. Základní verze je tvořena „pouze“ příkazovou řádkou, která nám ovšem poskytuje stejné možnosti nastavení jako grafická modifikace programu. Jedná se o klasickou aplikaci Client-Server, kdy na jedné straně spojení nastavíme zařízení jako server a na straně druhé jako Client. Iperf nám poskytuje mnoho nastavení jak danou síť testovat. Mezi základní nastavení patří: výběr typu spojení (TCP a UDP), nastavení portů, velikost přenášených dat a doba přenosu. [26]

Wifi analyzer

Tato aplikace od firmy farproc je určena zejména pro mobilní platformy Android a iOS. Wifi analyzer, jak už název napovídá, je nástroj vhodný pro analýzu okolních sítí. Aplikace umožňuje skenování obou dostupných pásem a to pásma 2,4 GHz a 5GHz. Dále umožňuje u jednotlivých sítí zjistit kvalitu signálu, SSID, zabezpečení a na jakém kanálu se síť nachází.

InSSIDer

Aplikace InSSIDer slouží stejně jako Wifi analyzer k analýze sítě s tím rozdílem, že má podrobnější informace o dané síti. Tato aplikace firmy MetaGeek je zdarma dostupná pro platformy Windows, Android a MacOS.

Ping tools

Ping tools od firmy StreamSoft je aplikace, která v sobě ukrývá mnoho nástrojů pro testování sítě. Jedním z nejdůležitějších součástí programu je nástroj ping, který umožňuje měřit latenci dané sítě.

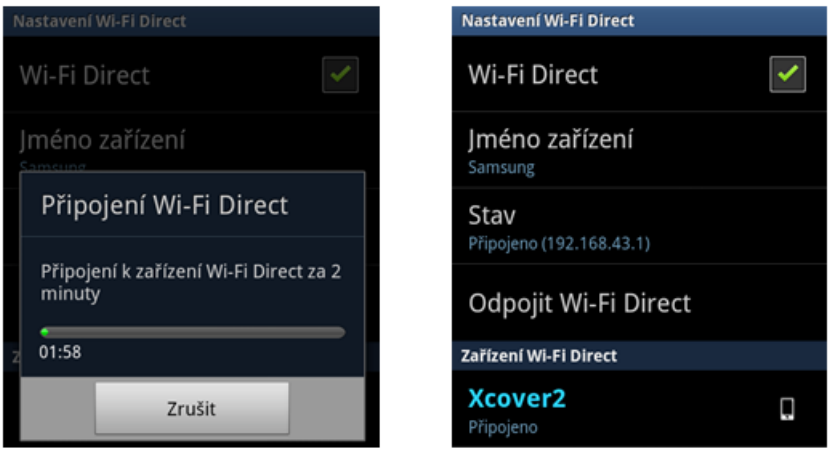
3.2 Specifikace mobilních zařízení

Obě dvě mobilní zařízení jsou od firmy Samsung, která v technologii Wi-Fi Direct vidí velký potenciál a umožnuje její použití ve velkém množství svých produktů. Pro naše účely byly vybrány dva mobilní telefony právě od této firmy, pomocí kterých se bude zkoumat specifikace technologie Wi-Fi Direct. Jedná se o modely Samsung Galaxy Xcover 2 a Samsung Galaxy Ace 2. Obě tyto zařízení disponují dotykovým displejem, dvoujádrovým procesorem o taktu 800 a 1000 Mhz, standardy 802.11 b/g/n 2,4 GHz, Wi-Fi Direct, GSM 3G, BlueTooth, GPS a operačním systémem Android ve verzích 2.3 a 4.1. Podrobnější specifikace jsou uvedeny na stránkách výrobce [27], [28].

Přesné specifikace Wi-Fi adaptérů se nám bohužel nepodařilo zjistit a to i přes kontakt s technickým oddělením firmy Samsung, kde nám bylo sděleno, že se jedná o interní informace společnosti, které nejsou veřejnosti dostupné.

3.3 Vytvoření Wi-Fi Direct sítě

Vytvoření fungujícího Wi-Fi Direct spojení je pro uživatele velice snadné a dá se srovnávat s vytvořením spojení prostřednictvím technologie BlueTooth. Pro naše účely byly využity dvě mobilní zařízení, které jsou podrobněji popsány v předešlé kapitole. Na obou zařízeních došlo k aktivovaci Wi-Fi čipu, který umožní spojení mezi oběma zařízeními pomocí technologie Wi-Fi Direct. Poté bylo jedno ze zařízení vybráno jako přístupový bod, prostřednictvím kterého bylo možno skenovat okolí. Po pár vteřinách bylo objeveno druhé mobilní zařízení, jenž podporuje tutéž technologii spojení. Zařízení bylo přidáno do námi vytvořené sítě a po několika vteřinách byly obě zařízení spárované. Bezpečnost této sítě zaručuje nejnovější šifrovací algoritmus WPA2, který je automaticky zvolen při vytvoření sítě.



Obrázek 3.1: Postup spárování mobilních zařízení

3.4 Měření vlastností sítě

Měření vlastností sítě je nedílnou součástí bezchybného datového přenosu. Pro tyto účely existuje mnoho zařízení a nástrojů, které nám umožní přesné určení kvality přenosu. Pro zkoumání přenosových vlastností sítě se používají tyto tři základní kvalifikační parametry:

1. Kvalita signálu [dBm]
2. Zpoždění [ms]
3. Přenosová rychlost [Mb/s]

Právě pomocí těchto parametrů bude určena kvalita sítě, vytvořená technologií Wi-Fi Direct. Naměřené výsledky budou následně porovnány s teoretickými specifikacemi podobných technologií a také s výsledky bakalářské práce pana Bc. Lejtnara [23], který zkoumal vlastnosti spojení Ad-hoc.

3.4.1 Kvalita signálu

Jedná se o jeden z nejdůležitějších parametrů u bezdrátových sítí, bez kterého bychom nebyli schopni rozpoznat, na jakou vzdálenost lze technologii Wi-Fi Direct účinně využít. Tento parametr závisí na mnoha vnějších faktorech. Tyto faktory mohou kvalitu signálu zásadně ovlivnit. Mezi takovéto faktory patří například: síla vyslaného signálu a okolní šum rušící vyslaný signál. Hlavními příčinami šumu je rušení okolních sítí, jenž pracují na stejné frekvenci jako síť, na které je kvalita signálu měřena. Velice záleží také na viditelnostních podmínkách a vzdálenosti obou komunikujících zařízení. Kvalita signálu je nejčastěji měřena v dBm, což je poměr jednotek decibel a miliwatt, ale není to pravidlem. Jednotkou kvality signálu mohou být i samotné mW nebo procenta. Kvalita signálu pro standard 802.11 se pohybuje od 0 až do -100 dBm. Přičemž platí, že čím menší hodnota, tím horší je výsledná kvalita signálu. Pro dostatečnou kvalitu signálu by se hodnoty měly pohybovat od 0 do -70 dBm. [29]

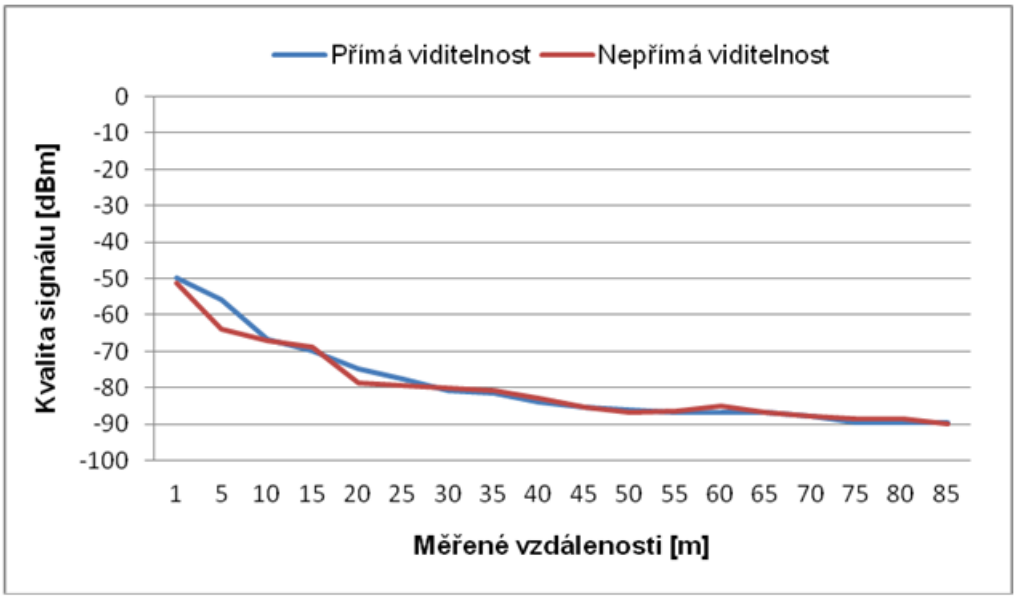
Pro naše účely bylo vybráno místo, na kterém nebyla zaznamenána žádná další bezdrátová síť, která by naše výsledné měření mohla ovlivnit. Toto místo také poskytovalo dostatečný prostor pro zkoumání dosahu technologie Wi-Fi Direct a zároveň i možnost prozkoumat dosah za nepřímé viditelnosti. Jako překážka posloužila cihlová zeď. Celá zeď byla prověřena na přítomnost kovu, který by mohl náš signál rušit, měřicím přístrojem MV9 XENOX. Dosah měřicího přístroje, na který je schopen detekovat kov, je 10 cm. Zeď byla celkově široká 16,7 cm a proto bylo nutné provést měření z obou stran. Bylo zjištěno, že naše překážka neobsahuje žádné známky kovu a tudíž je zcela vyhovující pro naše měření. Po proměření zdi došlo k natažení dostatečně dlouhé pásmo, na kterém byly vytyčeny měřené vzdálenosti. Tyto měřené vzdálenosti byly od sebe vzdáleny 5m v celkovém rozsahu 1-85m.

Po přípravě místa, byly obě mobilní zařízení spárovány, stejně jako je popsáno v předchozí kapitole. Na jednom z těchto zařízení byla spuštěna aplikace Wifi analyzer, pomocí které lze změřit kvalitu signálu v dBm. Zařízení na každé měřené

vzdálenosti naměřilo tři hodnoty, z kterých byl vytvořen průměr. Hodnoty jsou zobrazeny v tabulce číslo 1. Měření bylo zopakováno i pro nepřímou viditelnost obou zařízení, kde překážku tvořila zeď. Celková kvalita signálu byla pro jistotu kontrolována pomocí aplikace InSSIDer.

VZDÁLENOST [m]	PŘÍMÁ V. [dBm]	NEPŘÍMÁ V. [dBm]
1	-50	-51
5	-56	-64
10	-67	-67
15	-70	-69
20	-75	-79
25	-78	-79
30	-81	-80
35	-82	-81
40	-84	-83
45	-85	-85
50	-86	-87
55	-87	-86
60	-87	-85
65	-87	-87
70	-88	-88
75	-90	-89
80	-90	-89
85	-90	-90

Tabulka č. 1 Hodnoty kvality signálu za přímé a nepřímé viditelnosti



Obrázek 3.2: Kvalita signálu za přímé a nepřímé viditelnosti

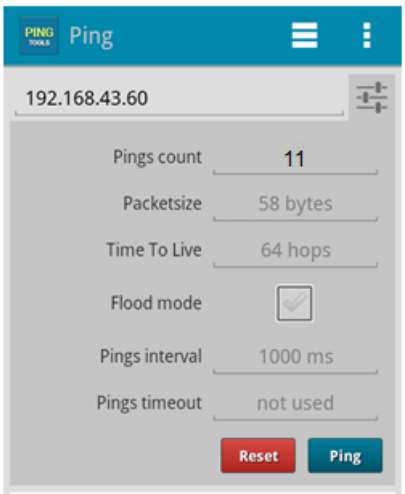
Z hodnot lze vyčíst, že maximální dosažená vzdálenost je rovna 85 metrů a rozdíl mezi přímou a nepřímou viditelností je nepatrný. Hodnoty se pohybují

v rozmezí od -50 dBm až do -90 dBm. U nejvyšší hodnoty však již docházelo ke značným výpadkům spojení a muselo se často obnovovat. Pro lepší názornost byly výsledky zaneseny do grafu na obrázku číslo 3.2.

3.4.2 Zpoždění

Zpoždění neboli latence je parametr, který nám určuje časový rozdíl mezi časem odesláním a přijetím paketu. Do tohoto času je zahrnuta doba potřebná k dosažení cíle a doba návratu, ke které je následně přičten časový údaj o délce zpracování dat koncovým zařízením. Tento parametr je především důležitý u služeb či aplikací, které posílají požadavky na vzdálený server a ihned čekají na odpověď. Typickým příkladem pro toto chování jsou webové stránky, telefonování po internetu nebo počítačové hry. Každá z těchto služeb se pohybuje na jiných hranicích zpoždění, které jsou schopny tolerovat. Pro obvyklou komunikaci by zpoždění mělo být co nejmenší v řádech milisekund, ale například pro internetové hovory se zpoždění může pohybovat až okolo 150 ms. [30]

Pro měření latence byly nejdříve spárovány obě mobilní zařízení, na kterých jsou předem nainstalovány potřebné aplikace Ping Tools, pomocí které bude provedeno měření latence a aplikace Iperf, která nám zajistí možnost připojení na konkrétní IP adresu. Nejprve se spustí na prvním zařízení již zmiňovaná aplikace Iperf, ve které se pomocí řádkových příkazů zapne server. Tento server má nastavenou IP adresu na 192.168.43.60 a naslouchá na portu 5001. Na druhém zařízení se spustí aplikace Ping Tools, ve které se mírně pozmění výchozí nastavení. Celkové nastavení je uvedeno na obrázku číslo 3.3. Změna se týkala především počtu opakování příkazu ping, které bylo nastaveno na hodnotu jedenáct. Pro



Obrázek 3.3: Nastavení programu Ping Tools

měření se použily naměřené vzdálenosti z předchozí kapitoly. Měření se opakovalo jak pro přímou tak i nepřímou viditelnost. Měření latence bylo z důvodu chybně zaznamenaných průměrných hodnot provedeno dvakrát. Původní měření bylo ovlivněno prvním přenosem, který zapisoval údaje do arp tabulky a jeho hodnoty se pohybovaly až v rámci stovek ms. Ostatní pokusy ICMP přenosu

se pohybovaly okolo přijatelných 20 ms. Z toho důvodu bylo měření provedeno znovu a to s 11 opakováními, kdy se u každé měřené vzdálenosti nezapočítal do průměrné hodnoty první ICMP přenos. Z toho vyplývá, že průměrné hodnoty v následující tabulce jsou vypočítány z deseti opakování.

VZDÁLENOST [m]	LATENCE PŘÍMÁ V.[ms]	LATENCE NEPŘÍMÁ V.[ms]
1	20	21
5	20	20
10	21	21
15	21	21
20	21	20
25	21	21
30	21	21
35	20	21
40	21	21
45	21	22
50	21	21
55	22	22
60	22	21
65	21	21
70	21	22
75	22	22
80	23	22
85	22	22

Tabulka č. 2 Latence sítě Wi-Fi Direct

Dále je z tabulky patrno, že při rostoucí vzdálenosti se hodnoty latence příliš nemění. To je způsobeno nastavením mobilních zařízení, které latenci vyrovnávají klesající teoretickou rychlostí. Ta se nám bohužel u této technologie nepodařila naměřit a to především z důvodu, že dostupné aplikace dovolují změřit teoretickou rychlost pouze u technologie Wi-Fi ale nikoli u Wi-Fi Direct. Ani operační systém samotných zařízení nám neumožnil zjistit, jakou teoretickou rychlostí se v určitých vzdálenostech přenos pohybuje.

3.4.3 Přenosová rychlost

Přenosová rychlost je veličina, která nám udává, jak velký objem informace lze přenést prostřednictvím dané sítě za určitou jednotku času. Tato veličina je uváděna v bitech za sekundu, což přesně znamená kolik bitů je síť schopna přenést během jedné sekundy. Jedná se však pouze o základní jednotku a daleko častěji se v dnešní době hovoří o jednotkách s předponami Kilo, Mega nebo Giga bit za sekundu. [31] Měření této veličiny na internetu nejčastěji probíhá prostřednictvím testovacích serverů. Tyto servery posílají klientovi určitá data, u kterých se sleduje, jak dlouho daný přenos trvá. Postup lze i obrátit a sledovat dobu přenosu od klienta k serveru a toho bylo využito pro naše měření.

Měření bylo demonstrováno na naší vytvořené síti, která je složena ze dvou mobilních zařízení a je vytvořena pomocí technologie Wi-Fi Direct. Pro samotné měření byla použita aplikaci Iperf, která je nainstalovaná na obou zařízeních a je určena přesně pro takovéto příležitosti. Aplikace pro operační systém android bohužel nepodporuje grafické ovládání programu a proto bylo vše ovládáno prostřednictvím řádkových příkazů. Tento druh ovládání nám ovšem poskytuje velké množství způsobů jak danou síť otestovat.Více o aplikaci Iperf a jejím nastavení je uvedeno na stránkách [26]. V našem případě bylo první zařízení nastaveno jako server pomocí příkazu:

```
# iperf -s
```

Ten zajistí, že dané zařízení bude dostupné na adrese, kterou mělo přiděleno při vytváření spojení mezi zařízeními. Druhé zařízení se naopak nastavilo jako klient, který sloužil pro odesílání dat na server. To bylo učiněno pomocí příkazu:

```
# iperf -c 192.168.43.60 -n 10M
```

Příkaz byl složen z parametru -c, který udával, že se jedná o klienta, z IP adresy serveru a následně z parametru -n, který nám znázorňoval velikost odeslaného souboru. Velikost se v průběhu měření měnila a to z 10 MB na 50 MB a 100 MB. Průměrné hodnoty našeho měření jsou znázorněny v následujících tabulkách.

VZDÁLENOST [m]	ČAS PŘENOSU [s]	PŘENOSOVÁ RYCHLOST [Mb/s]
1	2,6	32,4
5	2,5	33,8
10	3,1	27,5
15	3,8	22,2
20	4,4	19,5
25	3,6	22,2
30	5,0	18,1
35	6,7	13,6
40	6,4	13,8
45	10,1	8,5
50	11,4	7,4
55	10,1	8,4
60	11,5	7,7
65	11,5	7,3
70	13,5	6,3

Tabulka č. 3 Přenosová rychlost za přímé viditelnosti pro soubor veliký 10MB

VZDÁLENOST [m]	ČAS PŘENOSU [s]	PŘENOSOVÁ RYCHLOST [Mb/s]
1	12,1	34,6
5	11,9	35,4
10	12,4	33,7
15	14,6	28,8
20	18,0	23,4
25	22,2	18,9
30	25,4	16,5
35	20,4	20,6
40	24,4	17,2
45	29,0	13,5
50	31,8	13,7
55	32,9	12,8
60	37,5	11,3
65	47,9	8,8
70	51,5	8,2

Tabulka č. 4 Přenosová rychlost za přímé viditelnosti pro soubor veliký 50 MB

VZDÁLENOST [m]	ČAS PŘENOSU [s]	PŘENOSOVÁ RYCHLOST [Mb/s]
1	24,4	34,4
5	24,2	34,7
10	25,6	32,8
15	29,3	28,7
20	32,5	25,9
25	41,8	20,1
30	49,9	16,8
35	51,4	16,4
40	55,6	15,1
45	68,1	12,4
50	76,5	11,0
55	86,4	9,7
60	102,2	8,2
65	95,4	8,8
70	106,2	7,9

Tabulka č. 5 Přenosová rychlost za přímé viditelnosti pro soubor veliký 100 MB

V předešlých tabulkách jsou vidět hodnoty, které znázorňují výsledky přenosové rychlosti za přímé viditelnosti. Z těchto hodnot je patrné, že se přenosová rychlost s přibývající vzdáleností zmenšuje až na hodnoty okolo 7 Mb/s. Měření bylo provedeno pro vzdálenosti 1-70 metrů. Při vzdálenostech okolo 70m již byla zaznamenána velká časová prodleva mezi jednotlivými pokusy a také se zvýšil počet chybných přenosů dat. Delší vzdálenosti se jevily značně nestabilní a pro praktické využití zcela nevhodné.

VZDÁLENOST [m]	ČAS PŘENOSU [s]	PŘENOSOVÁ RYCHLOST [Mb/s]
1	2,9	29
5	3,1	28,4
10	3,6	23,9
15	3,1	26,8
20	3,4	24,6
25	4,7	17,9
30	7,9	10,6
35	9,5	8,9

Tabulka č. 6 Přenosová rychlost za nepřímé viditelnosti pro soubor veliký 10 MB

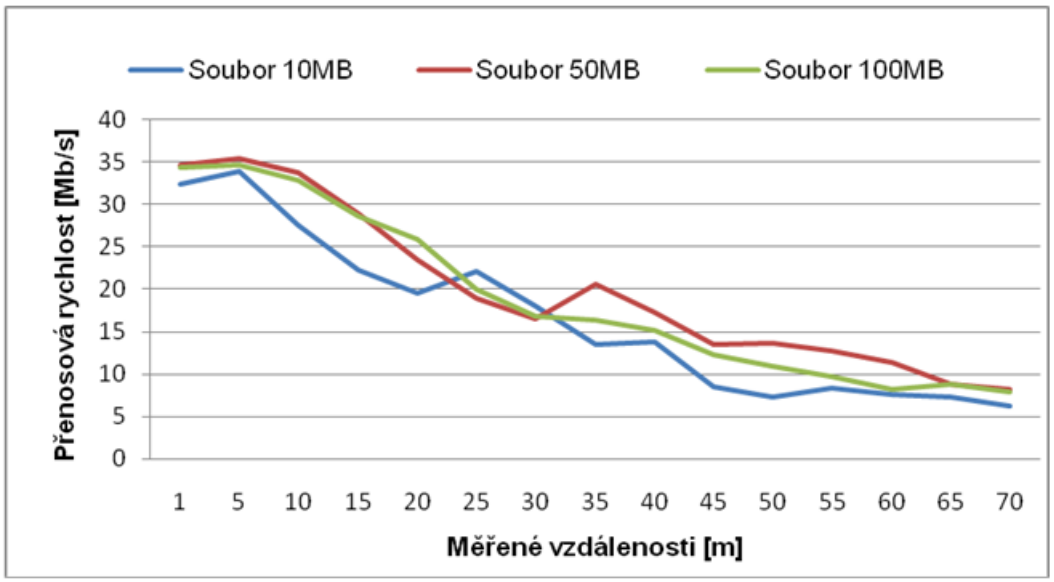
VZDÁLENOST [m]	ČAS PŘENOSU [s]	PŘENOSOVÁ RYCHLOST [Mb/s]
1	12,2	34,3
5	12,2	34,6
10	22	19,6
15	19,8	21,7
20	26,6	15,9
25	30	14,3
30	27,7	14,3
35	41,1	10,2

Tabulka č. 7 Přenosová rychlost za nepřímé viditelnosti pro soubor veliký 50 MB

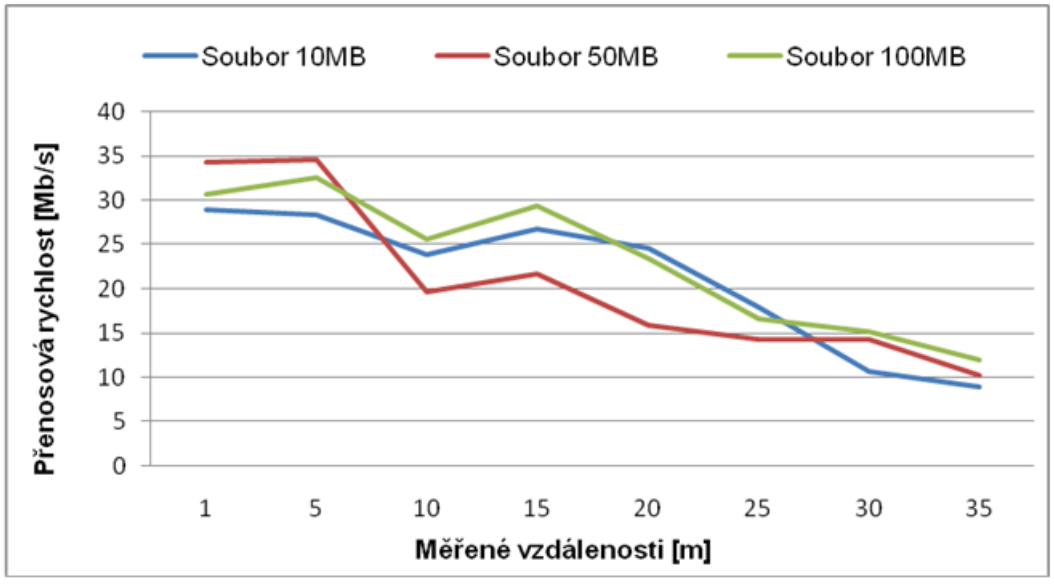
VZDÁLENOST [m]	ČAS PŘENOSU [s]	PŘENOSOVÁ RYCHLOST [Mb/s]
1	26	30,7
5	25,8	32,6
10	32,9	25,5
15	28,7	29,3
20	35,9	23,5
25	50,7	16,6
30	55,3	15,2
35	70,9	11,9

Tabulka č. 8 Přenosová rychlost za nepřímé viditelnosti pro soubor veliký 100 MB

Měření přenosové rychlosti za nepřímé viditelnosti na vyšší vzdálenosti nebylo vůbec možné a bylo z důvodu velké nestability ukončeno ve vzdálenosti 35m. Na následujících grafech číslo 3.4 a 3.5 je zobrazena přenosová rychlost za přímé a nepřímé viditelnosti, která v obou případech značně klesá s přibývající vzdáleností. Dále můžeme z grafu vyčíst, že obě měření začínají na přibližně stejné hodnotě 35 Mb/s a končí okolo 10 Mb/s, ovšem se značně rozdílnou naměřenou vzdáleností.



Obrázek 3.4: Přenosová rychlost za přímé viditelnosti



Obrázek 3.5: Přenosová rychlost za nepřímé viditelnosti

3.4.4 Vyhodnocení naměřených výsledků

Z výše zaznamenaných výsledků lze jasně odvodit, že daná technologie je pro reálné použití naprosto vyhovující a v mobilní sféře určitě nalezne své uplatnění. Naměřené hodnoty dokonce přesahují teoretické hodnoty ostatních bezdrátových technologií, jako jsou například BlueTooth a Ad-hoc. Bohužel se ale nepodařilo dosáhnout teoretických hodnot technologie Wi-Fi Direct a to především z důvodu menšího výkonu antén na mobilních zařízeních. Přístrojů, které by těchto hodnot mohlo dosáhnout, je zatím velmi málo z důvodu malé podpory ze strany výrobců bezdrátových čipů, kteří by museli vyvinout nové ovladače s podporou této technologie. Technologie nalezá uplatnění především u mobilních telefonů a některých televizních zařízení, což je u takového bezdrátové technologie zcela pochopitelné.

3.5 Porovnání technologií Wi-Fi Direct a Ad-hoc

Naměřené výsledky byly porovnány s výsledky měření pana Bc. Lejtnara [23], který zkoumal technologii Ad-hoc. Bylo zjištěno, že dané technologie jsou ve výsledku velmi rozdílné. Obě technologie dosahují různých hodnot naměřené vzdálenosti, latence a především přenosové rychlosti, kde se výsledky liší až o 16 Mb/s. Porovnání přenosové rychlosti bylo provedeno na malém souboru (10 MB) a na souboru velkém (100 MB) ve vzdálenostech 1m, 10m a 50m při přímé i nepřímé viditelnosti. Porovnané výsledky jsou zobrazeny v následujících tabulkách.

Vzdálenost [m]	**Ad-hoc Přenosová rychlost [Mb/s]**	**Wi-Fi Direct Přenosová rychlost [Mb/s]**
1	16,09	32,4
1 + překážka	-	29
10	16,91	27,5
10 + překážka	13,42	23,9
50	14,46	7,4
50 + překážka	6,16	-
70	-	6,3
100	11,93	-
100 + překážka	-	-

Tabulka č. 9 Porovnání přenosové rychlosti pro malý soubor 10 MB

Vzdálenost [m]	Ad-hoc Přenosová rychlost [Mb/s]	Wi-Fi Direct Přenosová rychlost [Mb/s]
1	18,43	34,4
1 + překážka	-	30,7
10	18,46	32,8
10 + překážka	15,06	25,5
50	14,53	11
50 + překážka	7,43	-
70	-	7,9
100	7,43	-
100 + překážka	-	-

Tabulka č. 10 Porovnání přenosové rychlosti pro velký soubor 100 MB

Z těchto tabulek lze vyčíst, že technologie Wi-Fi Direct je vhodnější na menší vzdálenosti, kde převyšuje všechny dostupné bezdrátové technologie, zatímco technologie Ad-hoc je vhodná pro větší vzdálenosti komunikace a to až do 100 metrů.

3.6 Shrnutí provedeného exprimentu

Měření probíhalo ve vzdálenostech 1-85 metrů, kde se jednotlivé pokusy pohybovaly v rozmezí 5 metrů. Ve větších vzdálenostech bylo spojení velice nestabilní a pro reálné využití zcela nevhodné. Největší hodnota přenosové rychlosti se pohybovala okolo 35 Mb/s, což sice není slibovaná hodnota specifikace, ale i tak převyšuje teoretické hodnoty ostatních technologií. Při měření vlastností sítě bylo odesláno a přijato velké množství dat, které by v reálném provozu představovalo například: posílání e-mailů, sdílení obrázků, hudby a videa. Při měření přenosové rychlosti bylo odesláno celkem 12935 MB. Číslo ovšem zahrnuje i neúspěšné pokusy, které do konečného hodnocení nebyly zahrnuty. Velikost úspěšně přenesených dat je 11040 MB o časové délce 5770,7 sekund. Tento časový údaj odpovídá pouze datům, která byla úspěšně přenesena a zaznamenána, ale neodpovídá o délce celého měření, které bylo mnohonásobně delší. Celkový počet měření se pohybuje okolo 364.

Závěr

Cílem bakalářské práce bylo prokázat praktické využití technologie WiFi Direct. Pro splnění cíle bylo nejdříve nutné seznámení s ostatními bezdrátovými technologiemi, které se využívají pro vytvoření malých lokálních sítí a mohly by tak ohrožovat novou nastupující technologii. Mezi tyto technologie patří infrastrukturní síť Wi-Fi, Ad-hoc síť a BlueTooth, u kterých bylo zjištěno, ve které oblasti se nejčastěji využívají a jejich výhody či nevýhody.

Následně byla zkoumána samotná technologií Wi-Fi Direct, u které byly opět zjištěny hlavní klady a zápory, proč by se měla tato technologie více využívat či nikoli. Následně se porovnávaly teoretické hodnoty, kde technologie Wi-Fi Direct jednoznačně převyšuje všechny ostatní dostupné bezdrátové technologie, kromě infrastrukturní Wi-Fi sítě, která se ovšem využívá pro jinou oblast komunikace.

Teoretické hodnoty se v mnoha případech mohou od reálných hodnot velice lišit. Proto bylo provedeno měření kvality sítě na základě tří základních parametrů. Mezi tyto parametry patří kvalita signálu, zpoždění neboli latence a přenosová rychlost, která byla pro srovnání bezdrátových technologií nejdůležitější. Po naměření reálných hodnot bylo zjištěno, že neodpovídají teoretickým hodnotám specifikace. Hlavní příčinou nedosažení slibovaných teoretických hodnot bylo využití mobilních zařízení, která mají nižší výkon bezdrátových adaptérů. Jiná zařízení, která by podporovala technologii Wi-Fi Direct a zároveň umožňovala měření vlastností sítě, nebyla pro český trh dostupná. Jak bylo již zmíněno, technologii Wi-Fi Direct je možné implementovat i na staré síťové adaptéry s pomocí aktualizací ovladačů, což ovšem výrobci bezdrátových adaptérů ve většině případů neumožnili a bude se muset počkat na nová síťová zařízení. Dostupnost zařízení, která podporují technologii Wi-Fi Direct se výrazně zlepšila na začátku roku 2014, kdy přišly na český trh rozšiřující síťové karty s podporou Wi-Fi Direct, které je možno propojit se stávajícími stanicemi prostřednictvím slotu PCIe. Mezi ostatní zařízení, které tuto technologii umožňují, patří mobilní telefony, síťové tiskárny, multimediální přehrávače, fotoaparáty a kamery, televizory a herní konzole. Z toho můžeme usoudit, že tato nová technologie je na vzestupu a je jen otázkou času, kdy se její použití rozšíří mezi veřejností.

Seznam použité literatury

[1] Pužmanová, Rita. *Moderní komunikační sítě od A do Z*. Vyd. 1. Praha: Computer Press, 1998, xvi, 446 s. ISBN 80-722-6098-7.

[2] Wi-Fi. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-03-03]. Dostupné z: `http://en.wikipedia.org/wiki/Wi-Fi`

[3] Wi-Fi. *I15.cz - Vše podstatné za 15 minut* [online]. 26. 8. 2011 [cit. 2014-03-03]. Dostupné z: `http://www.i15.cz/wi-fi/`

[4] Zandl, Patrick. *Bezdrátové sítě WiFi: praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-722-6632-2.

[5] Základy wifi sítí – IV. Typy sítí. *IT-Koko* [online]. 27. 12. 2009 [cit. 2014-03-04]. Dostupné z: `http://kokosaurus.cz/?s=ad-hoc`

[6] Bigelow, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[7] 802.11e brings QoS to WLANs. *Network World* [online]. 23. 6. 2003 [cit. 2014-03-06]. Dostupné z: `http://www.networkworld.com/news/tech/2003/0623techupdate.html`

[8] 802.11g: rychlejší WiFi?.. *Lupa.cz - server o českém Internetu* [online]. 19. 2. 2004 [cit. 2014-03-06]. Dostupné z: `http://www.lupa.cz/clanky/802-11g-rychlejsi-wifi/`

[9] IEEE 802.11. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-03-06]. Dostupné z: `http://en.wikipedia.org/wiki/IEEE_802.11`

[10] WiFi v roce 2015: Standard 802.11ad na frekvenci 60 GHz s až 5 Gb/s. In: *PCTuning* [online]. 24. 2. 2014 [cit. 2014-03-06]. Dostupné z: `http://pctuning.tyden.cz/index.php?option=com_content&view=article&id=29244&catid=1&Itemid=57`

[11] Jak zabezpečit WiFi síť. *DSL Internet, nabídky připojení k Internetu - DSL.cz* [online]. 10. 3. 2014 [cit. 2014-03-10]. Dostupné z: `http://www.dsl.cz/jak-na-to/5-site-a-ochrana/35-jak-zabezpecit-wifi`

[12] Šifrovací protokoly využívané WiFi. In: *B2B magazín o bezpečnosti ICT ze všech úhlů* [online]. 2010 [cit. 2014-03-11]. Dostupné z: `http://www.ictsecurity.cz/09/07/1-wi-fi/sifrovaci-protokoly-vyuzivane-wifi.html`

[13] Ad hoc síť. Jak na ochranu osobních údajů a bezpečnost informací. *InFuture.ru - Pociťte budoucnost! Denní on-line magazín pokročilých vědeckých a technologických úspěchů* [online]. 29. 6. 2013 [cit. 2014-03-12]. Dostupné z: http://www.infuture.ru/article/9130

[14] Sítě ad-hoc. *Marigold.cz* [online]. 20. 8. 2012 [cit. 2014-03-13]. Dostupné z: http://www.marigold.cz/wifi/doku.php/adhoc

[15] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit wi-fi, Bluetooth, GPRS či 3G*. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[16] Understanding Ad Hoc Mode - Page 2. *Wi-Fi Planet - The Source for Wi-Fi Business and Technology* [online]. 23. 8. 2002 [cit. 2014-03-15]. Dostupné z: http://www.wi-fiplanet.com/tutorials/article.php/10724_1451421_2/Understanding-Ad-Hoc-Mode.htm

[17] WiFi Direct: Konečně bezpečné dostaveníčko. *Lupa.cz - server o českém Internetu* [online]. 23. 11. 2010 [cit. 2014-03-18]. Dostupné z: http://www.lupa.cz/clanky/wifi-direct-konecne-bezpecne-dostavenicko/

[18] Wi-Fi Direct - za snadnější komunikaci mezi našimi přístroji. *NOTEBOOK.cz - notebooky, testy, recenze* [online]. 3. 11. 2010 [cit. 2014-03-18]. Dostupné z: http://notebook.cz/clanky/technologie/2010/wi-fi-direct

[19] Wi - Fi CERTIFIED Wi - Fi Direct^{TM}. In: *Broadcom Connected — News and Views to Stay Connected* [online]. 1. 10. 2010 [cit. 2014-03-18]. Dostupné z: http://blog.broadcom.com/wp-content/uploads/2013/10/Wi-Fi-Direct-White-Paper.pdf

[20] Wi-Fi Direct: Přímé spojení. *Informace, testy a novinky o hardware, software a internetu – CHIP.cz* [online]. 13. 10. 2011 [cit. 2014-03-18]. Dostupné z: http://www.chip.cz/trendy/wi-fi-direct-prime-spojeni/

[21] Pojem interoperabilita. *ABZ.cz: slovník cizích slov - on-line hledání* [online]. 19. 3. 2014 [cit. 2014-03-19]. Dostupné z: http://slovnik-cizich-slov.abz.cz/web.php/slovo/interoperabilita

[22] Certified Products Search Results - Wi-Fi Alliance. *Wi-Fi Alliance* [online]. 25. 10. 2010 [cit. 2014-03-19]. Dostupné z: http://www.wi-fi.org/certified-products-results?capabilities[50]=50

[23] LEJTNAR, Michal. Komparativní analýza ad hoc a direct spojení v bezdrátových sítích. Č. Bud., 2012. bakalářská práce (Bc.). JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH. Přírodovědecká fakulta

[24] Wi-Fi Direct vs. Bluetooth 4.0: A Battle for Supremacy. *PCWorld - News, tips and reviews from the experts on PCs, Windows, and more* [online]. 26. 10. 2010 [cit. 2014-03-20]. Dostupné z: http://www.pcworld.com/article/208778/Wi_Fi_Direct_vs_Bluetooth_4_0_A_Battle_for_Supremacy.html

[25] Techbox: Bluetooth sjednotilo bezdrátovou komunikaci - mobilenet.cz. *Mobilenet.cz* [online]. 24. 5. 2013 [cit. 2014-03-25]. Dostupné z: http://mobilenet.cz/clanky/techbox-bluetooth-sjednotilo-bezdratovou-komunikaci-12085

[26] Iperf: měření rychlosti spojení. *Root.cz - informace nejen ze světa Linuxu* [online]. 27. 7. 2012 [cit. 2013-10-26]. Dostupné z: http://www.root.cz/clanky/iperf-mereni-rychlosti-spojeni/

[27] GALAXY Ace2. *SAMSUNG Česká republika* [online]. 26. 10. 2013 [cit. 2013-10-26]. Dostupné z: http://www.samsung.com/cz/consumer/mobile-phone/mobile-phone/touchphone/GT-I8160OKAXEZ-spec

[28] GALAXY Xcover2. *SAMSUNG Česká republika* [online]. 26. 10. 2013 [cit. 2013-10-26]. Dostupné z: http://www.samsung.com/cz/consumer/mobile-phone/mobile-phone/touchphone/GT-S7710TAAETL-spec

[29] Jak zapojíme síť: WiFi bez tajemství. *Svět hardware* [online]. 7. 10. 2009 [cit. 2013-11-02]. Dostupné z: http://www.svethardware.cz/jak-zapojime-sit-wifi-bez-tajemstvi/12953-3

[30] Jak vzniká zpoždění při přenosu dat v mobilních sítích. *MobilMania.cz – O mobilech víme vše* [online]. 12. 5. 2005 [cit. 2013-11-10]. Dostupné z: http://www.mobilmania.cz/clanky/jak-vznika-zpozdeni-pri-prenosu-dat-v-mobilnich-sitich/sc-3-a-1110027/default.aspx

[31] Bit rate. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-11-16]. Dostupné z: http://en.wikipedia.org/wiki/Bit_rate

Seznam tabulek

Seznam obrázků

Seznam použitých zkratek

1. **AES** - Advanced Encryption Standard
2. **AMP** - Alternate MAC/PHY
3. **BSS** - Basic Service Set
4. **CES** - Consumer Electronics show
5. **CSMA/CA** - Carrier Sense Multiple Access with Collision Avoidance
6. **DFS** - Dynamic Frequency Selection
7. **DHCP** - Dynamic Host Configuration Protocol
8. **DSSS** - Direct-sequence Spread Spectrum
9. **FHSS** - Frequency-hopping spread spectrum
10. **Hi-Fi** - High fidelity
11. **IBSS** - Independent Basic Service Set
12. **IEEE** - Institute of Electrical and Electronics Engineers
13. **IP** - Internet Protocol
14. **LAN** - Local Area Network
15. **MAC** - Media Access Control
16. **MIMO** - multiple-input and multiple-output
17. **MU-MIMO** - multi-user MIMO
18. **NFC** - Near field communication
19. **OFDM** - Orthogonal frequency-division multiplexing
20. **PCIe** - Peripheral Component Interconnect Express
21. **PIN** - Personal identification number
22. **PMK** - Pairwise Master Key
23. **QoS** - Quality of Service
24. **SSID** - Service Set Identifier
25. **TCP** - Transmission Control Protocol
26. **TCP** - Transmit Power Control

27. **TKIP** - Temporal Key Integrity Protocol
28. **UDP** - User Datagram Protocol
29. **WEP** - Wired Equivalent Privacy
30. **WPA** - Wi-Fi Protected Access

Přílohy

VZDÁLENOST [m]	PŘÍMÁ VIDITELNOST [dBm]			NEPŘÍMÁ VIDITELNOST [dBm]		
1	-50	-46	-53	-51	-53	-50
5	-54	-57	-56	-65	-63	-64
10	-66	-69	-65	-65	-67	-69
15	-68	-72	-70	-69	-70	-68
20	-75	-76	-73	-79	-76	-81
25	-75	-78	-80	-80	-81	-77
30	-79	-81	-82	-79	-81	-80
35	-82	-80	-83	-81	-83	-79
40	-81	-87	-84	-81	-88	-80
45	-87	-84	-85	-85	-84	-87
50	-87	-86	-85	-87	-88	-85
55	-88	-87	-86	-86	-89	-84
60	-89	-87	-85	-85	-84	-86
65	-88	-87	-85	-87	-86	-88
70	-90	-86	-88	-88	-89	-87
75	-87	-92	-90	-88	-91	-87
80	-88	-89	-92	-88	-91	-87
85	-90	-89	-	-89	-91	-

Měření kvality signálu

VZDÁL. [m]	ping [ms]										průměr [ms]
1	19	22	16	19	16	20	18	22	25	18	20
5	19	23	17	20	24	17	21	25	17	20	20
10	23	16	20	25	21	23	16	21	23	17	21
15	20	23	26	19	24	17	20	24	18	22	21
20	18	22	17	20	23	27	21	24	17	19	21
25	20	23	16	22	16	21	24	26	20	22	21
30	25	17	19	24	18	22	17	21	24	21	21
35	20	16	20	23	17	20	25	18	23	16	20
40	20	21	25	19	26	19	20	17	20	25	21
45	18	26	17	21	24	18	24	17	21	23	21
50	18	22	25	19	23	25	18	21	17	18	21
55	23	20	24	20	21	25	18	20	23	21	22
60	22	25	19	22	26	18	22	20	23	26	22
65	22	26	19	18	23	24	17	20	24	19	21
70	23	18	20	24	18	21	18	24	18	21	21
75	17	22	24	20	23	29	19	25	19	23	22
80	19	32	18	24	19	22	26	21	25	19	23
85	19	23	26	19	18	21	26	21	26	20	22

Měření zpoždění signálu bez překážky

VZDÁL. [m]	ping [ms]										průměr [ms]
1	20	24	17	21	24	19	20	25	16	22	21
5	20	23	17	20	24	17	20	24	17	21	20
10	19	23	17	21	23	24	18	21	19	23	21
15	18	22	19	25	18	21	24	18	21	22	21
20	17	21	23	17	20	23	16	19	23	16	20
25	18	22	18	22	26	18	21	24	18	21	21
30	24	24	18	22	18	21	26	19	22	19	21
35	22	21	18	23	25	18	20	23	16	20	21
40	19	23	21	24	18	25	19	24	18	22	21
45	21	27	22	25	18	22	26	19	23	16	22
50	18	22	19	22	17	21	25	20	24	18	21
55	17	22	26	19	22	26	21	25	18	25	22
60	20	22	15	20	16	23	24	20	24	25	21
65	19	24	17	21	24	17	20	25	18	21	21
70	18	20	26	21	22	17	30	26	22	17	22
75	23	26	20	22	26	19	22	26	20	18	22
80	21	23	20	26	20	23	17	22	26	19	22
85	19	23	20	22	24	18	21	25	24	26	22

Měření zpoždění signálu s překážkou

VZDÁLENOST [m]	INTERVAL (ČAS) [s]			PŘIJATO [MB]	PŘENOSOVÁ RYCHLOST [Mb/s]		
1	2,7	2,6	2,5	10	31,6	32,3	33,3
5	2,4	2,6	2,4	10	35,0	32,2	34,3
10	2,7	3,1	3,4	10	30,9	27,2	24,4
15	3,7	3,9	3,8	10	22,8	21,7	22,1
20	5,4	3,3	4,5	10	14,1	25,6	18,7
25	3,3	2,5	4,9	10	25,2	24,0	17,3
30	3,3	6,3	5,4	10	25,2	13,4	15,7
35	5,7	9,5	4,9	10	14,7	8,9	17,1
40	7,9	6,4	4,8	10	10,7	13,1	17,6
45	8,3	9,8	12,1	10	10,1	8,5	7,0
50	10,8	12,1	11,2	10	7,8	6,9	7,5
55	10,4	9,0	11,0	10	8,1	9,3	7,9
60	9,4	9,8	15,4	10	8,9	8,6	5,4
65	11,4	10,9	12,2	10	7,3	7,7	6,9
70	12,6	12,2	15,6	10	6,7	6,9	5,4

Přenosová rychlost - soubor 10 MB bez překážky

VZDÁLENOST [m]	INTERVAL (ČAS) [s]			PŘIJATO [MB]	PŘENOSOVÁ RYCHLOST [Mb/s]	
1	12,0	12,1	12,3	50	35,0	34,6	34,2
5	11,7	12,2	11,7	50	35,8	34,5	35,8
10	12,4	12,5	12,4	50	33,9	33,5	33,8
15	15,8	14,4	13,6	50	26,6	29,2	30,7
20	16,6	18,8	18,6	50	25,2	22,3	22,6
25	22,8	21,8	22,1	50	18,4	19,2	19,0
30	24,2	26,4	25,7	50	17,4	15,9	16,3
35	20,9	19,3	21,1	50	20,1	21,7	19,9
40	26,3	24,1	22,9	50	15,9	17,4	18,3
45	25,7	37,0	24,2	50	11,8	11,3	17,3
50	24,6	38,2	32,6	50	17,1	11,0	12,9
55	34,7	32,1	31,8	50	12,1	13,0	13,2
60	42,9	36,0	33,6	50	9,8	11,6	12,5
65	44,7	49,9	49,1	50	9,4	8,4	8,6
70	48,7	55,3	50,5	50	8,6	7,6	8,3

Přenosová rychlost - soubor 50 MB bez překážky

VZDÁLENOST [m]	INTERVAL (ČAS) [s]			PŘIJATO [MB]	PŘENOSOVÁ RYCHLOST [Mb/s]		
1	25,1	23,6	24,5	100	33,4	35,6	34,3
5	23,7	24,2	24,6	100	35,4	34,6	34,1
10	26,7	25,5	24,6	100	31,5	32,9	34,1
15	30,1	28,7	29,0	100	27,9	29,3	28,9
20	33,3	31,7	32,4	100	25,2	26,5	25,9
25	41,2	41,2	43,0	100	20,3	20,4	19,5
30	50,4	47,2	52,1	100	16,6	17,8	16,1
35	54,6	46,2	53,3	100	15,4	18,1	15,7
40	52,5	59,7	54,6	100	16,0	14,0	15,4
45	66,6	66,8	70,8	100	12,6	12,6	11,9
50	78,7	77,0	73,8	100	10,7	10,9	11,4
55	83,0	86,4	89,8	100	10,1	9,7	9,4
60	97,0	99,9	109,8	100	8,7	8,4	7,6
65	96,8	97,7	91,8	100	8,7	8,6	9,1
70	97,7	107,1	113,8	100	8,6	7,8	7,4

Přenosová rychlost - soubor 100 MB bez překážky

VZDÁLENOST [m]	INTERVAL (ČAS) [s]		PŘIJATO [MB]	PŘENOSOVÁ RYCHLOST [Mb/s]	
1	2,8	2,7	3,2	10	30,1	31,0	25,9
5	3,6	2,9	2,7	10	24,4	29,4	31,3
10	3,3	3,6	3,8	10	25,7	23,6	22,4
15	2,8	3,6	3,0	10	29,8	23,0	27,6
20	3,7	3,2	3,4	10	22,7	26,1	24,9
25	5,4	4,6	4,2	10	15,4	18,2	20,1
30	7,1	8,7	8,0	10	11,9	9,6	10,4
35	8,9	9,2	10,3	10	9,4	9,1	8,1

VZDÁLENOST [m]	INTERVAL (ČAS) [s]		PŘIJATO [MB]	PŘENOSOVÁ RYCHLOST [Mb/s]	
1	12,4	12,0	12,3	50	33,7	35,1	34,1
5	13,2	11,7	11,6	50	31,8	35,7	36,2
10	27,4	19,6	19,0	50	15,3	21,4	22,1
15	17,7	24,5	17,1	50	23,6	17,1	24,5
20	30,2	26,7	23,0	50	13,9	15,7	18,2
25	36,6	28,3	25,1	50	11,5	14,8	16,7
30	24,3	27,2	31,6	50	14,3	15,4	13,3
35	40,1	39,9	43,2	50	10,5	10,5	9,7

Přenosová rychlost - soubor 10 MB a 50 MB s překážkou

VZDÁLENOST [m]	INTERVAL (ČAS) [s]			PŘIJATO [MB]	PŘENOSOVÁ RYCHLOST [Mb/s]		
1	24,4	25,2	28,4	100	34,4	33,3	24,5
5	24,5	26,2	26,8	100	34,2	32,1	31,4
10	30,7	33,8	34,3	100	27,3	24,8	24,5
15	29,5	29,7	26,8	100	28,4	28,2	31,3
20	34,2	34,3	39,1	100	24,5	24,5	21,4
25	56,0	48,6	47,6	100	15,0	17,3	17,6
30	56,2	56,8	53,0	100	14,9	14,8	15,8
35	63,3	73,7	75,6	100	13,3	11,4	11,1

Přenosová rychlost - soubor 100 MB s překážkou