elektrorevue
ISSN 1213 - 1539

Rok / Year:	Svazek / Volume:	Číslo / Number:	Jazyk / Language
2016	18	4	CZ

Technika, která se váže ke standardu IEEE 802.11

Technology Connected with IEEE 802.11 Standard

Josef Pokorný

pepa.pokorny@centrum.cz

-

DOI: -

Abstract: The paper overviews wireless networks and contemporary hardware used in these networks. Networks are divided into categories according to covered area. There is an example WLAN network configured in ad-hoc way in operating system Linux. The attenuation of various frequencies passing through a wall is solved and plotted in a graph. There are OSI levels of IEEE 802.11 described here. There is discussed the security of various WiFi networks which were measured here. The possibilities of WiFi geolocation are discussed here.

elektrorevue
ISSN 1213 - 1539

Technika, která se váže ke standardu IEEE 802.11

Josef Pokorný

-

Email: pepa.pokorny@centrum.cz

Abstrakt *– Článek uvádí přehled bezdrátových sítí a současnou techniku používanou v těchto sítích. Sítě jsou rozděleny do kategorií dle pokrytého rozsahu. Je provedena ukázka nakonfigurování sítě WLAN v režimu ad-hoc v operačním systému Linux. Je zpracováno graficko-početní srovnání ztrát kmitočtových pásem z hlediska útlumu signálu při průchodu zdí. Jsou popsány úrovně OSI, které pokrývá standard IEEE 802.11. Na základě změřených dat je diskutováno zabezpečení WiFi sítí. Jsou diskutovány možnosti využití WiFi sítí pro geolokaci.*

1 Úvod

S rozvojem integrace a miniaturizace součástek se litografické a implantační technologie pro výrobu polovodičových čipů pohybují kolem hranice vzdáleností 14 nm. S příchodem druhé generace FinFET tranzistorů [1] se podařilo přejít k polovodičovým strukturám obsahujícím řádově miliardu prvků na jednom čipu. Miniaturizace umožnila posunout rovněž běžně využitelné signálové frekvence do řádu gigahertzů. Současně s výrobou těchto vysoce technologicky náročných součástek je svázána standardizace činností zařízení, pro která byly tyto součástky vyrobeny. Řada komunikačních zařízení pracuje se standardem IEEE 802.11, některých rysů této problematiky by se chtěl tento článek dotknout.

2 Sítě a komunikace

Technologie bezdrátových přenosů dat se ubíraly dvěma hlavními směry. Přenos dat pomocí optických zařízení přenášejících pulsně modulované signály s frekvenčním rozsahem od 100 až do 1 000 THz s vlnovou délkou světla v rozmezí od 800 nm až do 1 550 nm.

Příkladem optického zařízení umožňujícího duplexní provoz může být například Laser Link 4EI, který dokáže na vzdálenost 800 m pomocí laserového paprsku přenést digitální signály s přenosovou rychlostí 4x2,048 Mbps [2].

Druhým základním směrem přenosu dat je využití radiových vln. V této oblasti vznikla řada druhů komunikačních sítí lišících se různými modulačními technikami, komunikačními protokoly, topologií, různým vyzářeným výkonem, dosahem, rychlostí přenosu, různým typem určení (point – multipoint) a různou úrovní zabezpečení. K dané problematice lze uvést např. sítě GSM (Global System for Mobile Communication) pracující v kmitočtové oblasti 900/1800 MHz. Rozmístění BTS (Base Transceiver Station) stanic této sítě v ČR, pro různé operátory, lze získat například z webu [3], který je průběžně aktualizován. V současné době mobilní operátoři v ČR provozují sítě druhé až čtvrté generace.

Dle velikosti lze obecně sítě rozdělit na GAN, WAN, MAN, LAN, PAN. Síť GAN (Global Area Network) představuje nejrozsáhlejší strukturu, zahrnující i družicové spoje, často je tato síť navázána na síť WAN (Wide Area Network), což je síť s postupnou cestou, na které jsou vytvořeny přípojné uzly. Síť MAN (Metropolitan Area Network) je vysokorychlostní síť tvořená spojením několika sítí LAN (Local Area Network), vzájemně spolupracujících v rámci velkého města, závodu, či univerzity. Rozsah sítě MAN se uvažuje maximálně několik desítek kilometrů. Sítě LAN jsou vysokorychlostní sítě vytvořené spojením několika počítačů, většinou v rámci jedné budovy a jsou většinou spravovány jediným správcem (supervisorem). Sítě PAN (Personal Area Network), jedná se o označení pro nejmenší počítačové sítě vytvořené zpravidla přímo v jedné místnosti, vzhledem k prudkému rozvoji bezdrátových technologií, tento typ sítě navazuje a často přechází přímo v počítačovou architekturu, příkladem může být bezdrátový dvouterabajtový pevný disk firmy Western Digital – WD My Passport Wireless, který umožňuje současné připojení několika bezdrátových WiFi zařízení dle standardu 802.11b/g/n, sdílení internetu, dále může pracovat v různých WiFi režimech – jako klient sítě nebo přístupový bod AP (Access Point), disk podporuje zabezpečení komunikace pomocí WPA (WiFi Protected Access), WPA2, WPS (WiFi Protected Setup) [4].

Bezdrátové sítě z hlediska dosahu signálu mohou být považovány za sítě typu LAN, bezdrátové sítě tohoto typu jsou někdy také označovány jako sítě WLAN (Wireless Local Area Network). Sem spadají především sítě typu WiFi, které jsou normalizovány standardem IEEE 802.11X. Z některých současných zařízení určených pro sítě typu WiFi lze uvést například router, výrobek firmy Asus Wireless–AC5300 Tri-band Gigabit Router, jehož 8 antén je určeno pro komunikaci v pásmech 2,4 GHz a 5 GHz s modulací 1024QAM (Quadrature Amplitude Modulation), se zabezpečením WEP, WPA, WPA2, WPS, Radius [5].

Špičkovou platformu pro techniku přístupových WiFi bodů představil světový lídr ve vývoji čipů pro WiFi komunikačních zařízení, Quantenna Communications, Inc., na veletrhu CES 2015 firma předvedla novou čipovou sadu typu 8x8 MU MIMO (Multi-User Multiple-Input Multiple-Output), která jako první na světě při plné konfigurovatelnosti zvládá datový tok 10 Gb/s. Čipset pracuje se standardem 802.11 ac [6].

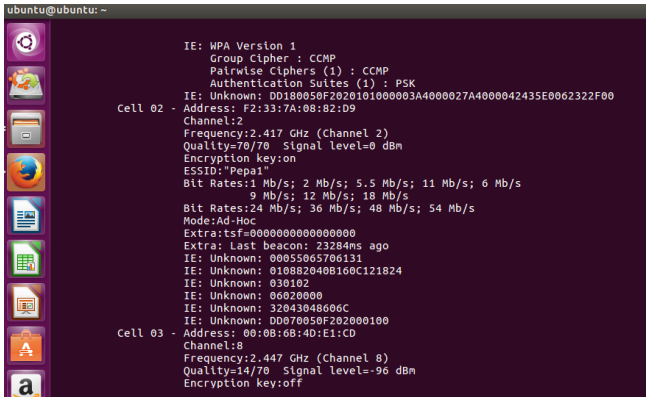
Pokud jsou počítače v rádiovém dosahu, mohou se propojit přímo, potom hovoříme o sítích typu ad-hoc. Operační systémy osobních počítačů, většinou již mají možnost tento typ sítě přímo vytvořit, například MS-Windows v nabídce Centra síťových připojení a sdílení má možnost vytvoření tohoto typu sítě.

elektrorevue
ISSN 1213 - 1539

Pro Linuxové systémy, například pro Ubuntu 16.04, je možno síť ad-hoc zkonfigurovat za použití příkazového řádku následujícím způsobem:

- Nejprve zastavíme network-manager: *sudo service network-manager stop*.
- Poté zastavíme WiFi síťové rozhraní wlo1: *sudo ip link set wlo1 down*.
- Nakonfigurujeme síťové rozhraní wlo1 do módu ad-hoc, vybereme volný komunikační kanál a zvolíme název sítě: *sudo iwconfig wlo1 mode Ad-hoc essid Pepa1 channel 2 key 123456789*.
- Spustíme síťové rozhraní s novými parametry: *sudo ip link set wlo1 up*.
- Nastavíme síťovému rozhraní internetovou IP adresu místní sítě třídy C [7]: *sudo ip addr 192.168.0.8/24 dev wlo1*.

Výsledné nastavení počítačové sítě typu ad-hoc zobrazené pomocí příkazu *iwlist* můžeme vidět na obrázku 1.



Obr. 1: Nastavené parametry WiFi sítě typu ad-hoc na operačním systému Linux Ubuntu 16.04.

Název použitého WiFi zařízení *wlo1* je přímo využívaný jádrem systému a je spravován ve většině dnešních linuxových distribucí (princip HAL opuštěn v roce 2011 [8]) programem *udev* a jeho modifikacemi, např. *eudev* distribuce Gentoo. Podrobnosti o použitém zařízení bývají zpravidla uloženy v adresáři */etc/udev/rules.d/*, kde je pro potřeby nastavení sítě můžeme vypsat příkazem *udevadm info*.

Další možností, jak vytvořit síť typu ad-hoc, je využití systému Bluetooth. Bluetooth technologie byla navržena jako bezdrátová alternativa k sériovému portu RS-232. Komunikace je provozována ve dvou variantách synchronní SCO (Synchronous Connection Oriented) a asynchronní ACL (Appshop Connectionless). SCO slouží primárně pro přenos hlasových zpráv, přenosová rychlost je 64 kbit/s, při ACL paketovém přenosu dat pro Bluetooth v4.0 je komunikační rychlost až 3 Mb/s [9]. Technologie Bluetooth se řídí standardem IEEE 802.15X. Příkladem použití technologie může být USB-BT400, což je Bluetooth adaptér pro USB port počítače, jedná se o výrobek firmy Asus. Adaptér má dosah 10 m a je schopen komunikovat i s nižšími verzemi technologie Bluetooth [10]. Pro notebooky se sběrnicí PCMCIA (Personal Computer Memory Card International Association) můžeme využít zásuvnou Bluetooth kartu 3CRWB6096B od výrobce 3Com.

Dalším typem sítí s malým dosahem jsou sítě typu UWB (Ultra-Wide Band). Tento typ sítí zatím nedoznal velkého rozšíření, je založen na principu přenosu jednotlivých bitů informace pomocí velmi krátkých impulzů, zpravidla nanosekundových, šířících se formou rozprostřeného spektra. Využití UWB aplikací se předpokládá především v sítích CATV (Community Access Television) a v automobilovém průmyslu jako antikolizní radary. Kvůli obtížné detekci nízkoenergetického rozprostřeného spektra signálu se předpokládá jejich nasazení v komunikačních systémech se skrytým provozem. Podmínky provozu UWB zařízení řeší standard 802.15.3X a evropská norma EN 302X [11].

Jako další síťovou technologii je možné uvést síť typu ZigBee (označení sítě je odvozeno od létajících včel). Síť je určena pro menší datové toky, těžiště jejího využití je především v komunikaci mezi senzory, čidly, ovladači apod. První verze sítě ZigBee 1.0 se objevila v roce 2004 a je svázána se standardem IEEE 802.15.4 pro fyzickou a MAC (Medium Access Control) vrstvu síťového protokolu. V síti ZigBee se vyskytují tři druhy zařízení, hlavním a jediným členem sítě je koordinační zařízení (ZigBee Coordinator), které řídí veškerý provoz. Na koordinační zařízení jsou navázána směrovací zařízení, která zajišťují komunikaci mezi řídícím zařízením a koncovými zařízeními. Pro práci sítě ZigBee bylo v Evropské unii vyčleněno kmitočtové pásmo 868 MHz, využívá se 16 komunikačních kanálů s šířkou 5 MHz a kódováním BPSK (Binary-Phase Shift Keying). Rychlost toku dat sítě je 20 kbit/s na jednotlivý přenosový kanál [11] [12]. Příkladem může být ZigBee modul HPTZ01X od firmy Hoperf, řízený 32 bitovým procesorem ARM Cortex – M3, výstupem je standardní komunikační port UART (Universal Asynchronous Receiver/Transmitter) [13].

Na letošním lednovém veletrhu spotřební elektroniky CES 2016 v Las Vegas byla představena nová technologie, navržená pro frekvenční pásmo 900 MHz. Nová technologie, označovaná jako WiFi HaLow, by měla zajistit větší prostupnost a dosah signálu, zejména v prostorách budov.

Jak vypadá situace volby kmitočtu pro novou technologii WiFi HaLow s ohledem na prostupnost signálu stěnou budovy v porovnání s ostatními kmitočty doporučovanými standardem IEEE 802.11, zjistíme orientačním výpočtem, který provedeme metodikou doporučenou Mezinárodní telekomunikační unií (ITU) [14].

Výpočtem určíme prostupnost signálů o kmitočtech 900 MHz, 2,4 GHz a 5 GHz betonovou stěnou různé tloušťky. Pokud se v materiálu vyskytuje proměnné elektromagnetické pole, což je případ šíření elektromagnetických vln, platí, že relativní permitivita materiálu ε_r se stává komplexní veličinou:

$$\varepsilon_r = \varepsilon_r' + j\varepsilon_r''. \qquad (1)$$

Dále platí:

$$\varepsilon = \varepsilon_r \varepsilon_0, \qquad (2)$$

kde ε_0 je permitivita vakua, $\varepsilon_0 = 8{,}854 \cdot 10^{-12} F.m^{-1}$.

Relativní permitivita pro beton podle [15] [16]:

elektrorevue
ISSN 1213 - 1539

$$\varepsilon_r = 7 + j0{,}85,$$

a ztrátový činitel:

$$tg\delta = \frac{\varepsilon_r''}{\varepsilon_r'} = 0{,}12.$$

Určíme vlnovou délku signálů ve vakuu:

$$\lambda_0 = \frac{c}{f}, \tag{3}$$

kde c je rychlost světla ve vakuu, přibližně:
$c = 3 \cdot 10^8 m.s^{-1}$.

Určíme hodnotu vlnového čísla pro signály ve vakuu:

$$k_0 = \frac{2\pi}{\lambda_0}. \tag{4}$$

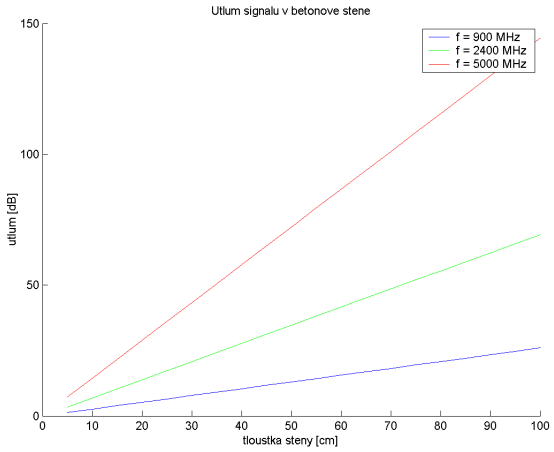
Stanovíme hodnotu útlumové vzdálenosti:

$$\Delta_{dielectric} = \frac{1}{k_0\sqrt{\varepsilon_r'}}\frac{2}{tg\delta}. \tag{5}$$

Útlum signálu procházející betonovou stěnou je dán vztahem:

$$A = \frac{20\log_{10} e}{\Delta}. \tag{6}$$

Výsledné hodnoty útlumu pro různé tloušťky stěny a různé hodnoty uvažovaných frekvencí signálu vidíme v grafu 1.



Graf 1: Závislost útlumu signálu na tloušťce stěny.

Z grafu 1 vyplývá, že pro klasickou obvodovou stěnu z betonu o tloušťce 45 cm můžeme očekávat, že touto stěnou projde až 25% signálu o frekvenci 900 MHz, ale pro frekvenci 2,4 GHz již tato stěna propustí jen 3% užitečného signálu. Tím je jasně určena výhoda nové technologie HaLow.

S novým standardem se počítá v oblasti chytrých spotřebičů, internetu věcí, předpokládá se, že nová technologie bude do určité míry konkurencí pro technologii Bluetooth.

Globální nezisková organizace – WiFi Alliance pracuje na návrhu příslušného standardu WiFi s označením 802.11ah/HaLow, který by měl být publikován v roce 2018.

3 Některé prvky komunikace WiFi definované standardem IEEE 802.11

Vzhledem k obrovskému rozsahu problematiky komunikace WiFi (samotný standard čítá 2793 stran) bylo nutné vybrat několik základních prvků komunikace daných standardem. Samotný standard IEEE 802.11 popisuje pouze dvě základní vrstvy modelu ISO/OSI (International Organization for Standardization/Open Systems Interconnection), který dělí komunikaci do sedmi hierarchických vrstev.

Základem modelu je vrstva fyzická, která definuje všechny elektrické a fyzikální vlastnosti zařízení, ve standardu je označena zkratkou PHY (Physical Layer). Datovou jednotkou, kterou tato vrstva přenáší, je bit. Při podrobnějším pohledu je možno fyzickou vrstvu rozdělit na dvě subvrstvy a to podvrstvu PMD (Physical Medium Dependent), která vysílá a přijímá signály, mění frekvenční kanály a podobně. Druhou podvrstvou fyzické vrstvy je subvrstva PLCP (Physical Layer Convergence Procedure), tato vrstva připravuje rámce pro přenos pro vrstvu PMD a přikládá informace o použitém přenosovém mechanizmu a způsobu modulace k rámcům z podvrstvy MAC [17]. Vzhledem k charakteru fyzické vrstvy, jsou spolupracujícími zařízeními této vrstvy například opakovače. Úkolem opakovačů je přijmout eventuelně zkreslený, zašumělý a jinak poškozený signál, provést opravu signálu, zesílit jej a jako správně načasovaný ho vyslat dále. Příkladem tohoto typu zařízení může být Devolo WiFi Repeater, tvořený malým pouzdrem, které je na zadní straně zakončeno síťovou zástrčkou, použití opakovače se předpokládá v místnostech. Opakovač zvládá datový tok 300 Mbit/s, pracuje v pásmu 2,4 GHz, kromě WiFi umožňuje připojení i pomocí kabelu ethernetové sítě LAN. Opakovač zvládá bezpečnostní protokoly WPA/WPA2 a WPS [18].

Další vrstvou modelu ISO/OSI je vrstva linková, která je ve standardu realizována dvěma subvrstvami MAC (Medium Access Control) a LLC (Logical Link Control). Linková vrstva poskytuje funkce k přenosu dat mezi jednotlivými síťovými jednotkami. Uspořádává data z fyzické vrstvy do logických celků (rámců). Probíhá zde v režimu CCM (Counter mode with Cipher-block chaining Message authentication code) blokové šifrování pomocí šifry AES (Advanced Encryption Standard) [17].

4 WiFi – prvky zabezpečení

Pro zjištění prvků zabezpečení běžných bezdrátových sítí použijeme programový wrapper WiFite, který kromě jiného umožňuje při použití volby *-all* zjistit zabezpečení okolních sítí, sílu jejich signálu a vysílací kanály. Dle obrázku 2 je patrné, že se běžně vyskytují různé druhy a kvalita zabezpečení bezdrátové sítě. Ze sledovaných sítí na obr. 2 se jeví jako nejslabší síť označená číslem 4, která ke své

elektrorevue
ISSN 1213 - 1539

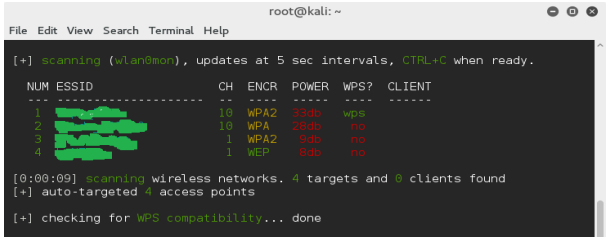
činnosti využívá zabezpečení typu WEP (Wired Equivalent Privacy).

WEP byl prolomen v roce 2001 (publikován útok FMS – Fluhrer, Mantin, Shamir), tento typ zabezpečení pracuje na linkové vrstvě a využívá pro šifrování rámců proudovou šifru RC4 s 64 nebo 128 bitovým klíčem. Při zabezpečení WEP se pro šifrování a dešifrování používá symetrický postup, tzn., že je pro obě operace stejný algoritmus i stejný klíč. Autentizace se provádí otevřeně nebo pomocí sdíleného klíče.

Lepší způsob zabezpečení představuje síť č. 2, která využívá zabezpečení pomocí WPA (WiFi Protected Access). WPA je rovněž postaveno na šifře RC4, je oproti WEP vylepšeno o protokol TKIP (Temporal Key Integrity Protocol). Tento protokol obsahuje 128 bitový dynamický klíč, který se mění za každých 10 000 paketů. Dalším vylepšením je paketový hešovací algoritmus MIC (Message Integrity Code) – Michael.

Technologie zabezpečení WPA2 provádí šifrování typu AES. Tento způsob šifrování má z hlediska zde diskutovaných technologií nejlepší parametry vzhledem k útokům na integritu, důvěrnost dat, útokům man in the middle, falešné autentizaci, útokům na slabý klíč, falšování paketů a falešného přístupového bodu [19].

S technologií WPA2 byl vyvinut bezpečnostní standard WPS (WiFi Protected Setup), který zjednodušuje vytvoření zabezpečené bezdrátové sítě. WPS může fungovat ve dvou módech – PBC (Push Button Configuration), kdy jsou zařízení automaticky spárována po současném stisku příslušných tlačítek na bezdrátovém adaptéru a routeru, a v módu PIN, kdy jsou klienti autentizováni na základě PIN kódu, který se vloží do routeru, PIN kód z routeru se obdobně vloží do klienta. Služba WPS může být na zařízení vypnuta, což vidíme na obr. 2. V některých případech může představovat služba WPS bezpečnostní riziko, neboť na rozpoznání 8 bajtového PINu může být veden útok. Ovládnutí PINu znamená obejití zabezpečení WPA2 a získání přístupu do sítě. Z těchto důvodů se doporučuje službu WPS na zařízení vypnout.



Obr. 2: Náhodný vzorek zabezpečení malých WiFi sítí.

K celkovému pohledu je třeba poznamenat, že existují metody, jak provést odposlech počítače, který není připojen k žádné síti. Byly předvedeny metody kódování rychlosti větráku počítače s následným sejmutím informací pomocí zvukové karty. Informace z počítače mohou být prozrazeny i například elektromagnetickým vyzařováním přes stěny místnosti [20].

5 Geolokace malých WiFi sítí

IP Geolokace se používá v internetových sítích ke zjištění geografické polohy síťového zařízení. Znalost geografické polohy síťového zařízení může být výhodná například pro zacílení internetové reklamy, vyhledávání dopravního spojení, předpověď počasí pro konkrétní oblast, lokalizaci uživatele internetové technologie VoIP (Voice over IP) při tísňových voláních, ochranu před podvody s platebními kartami a v neposlední řadě může sloužit i pro zábavu.

Geolokační metody rozdělujeme na dvě základní skupiny, na aktivní a pasivní. Aktivní metody jsou založeny na odhadu polohy související se změřeným zpožděním. Zpoždění je doba potřebná na přenos jednoho datového segmentu od zdroje k příjemci. Zpoždění na internetu je ovlivněno mnoha faktory a rozdělujeme ho na část deterministickou a stochastickou. Deterministické zpoždění má konstantní velikost, kterou lze vypočítat, naproti tomu stochastické zpoždění má náhodný charakter a je způsobeno aktuálním stavem sítě [21].

Dále můžeme zpoždění rozdělit podle toho, kde vzniká, na zpoždění v koncových zařízeních, mezilehlých zařízeních a přenosových linkách. Zpoždění v koncových zařízeních (zdroj a cíl) vzniká při přípravě paketu a jeho odesílání/přijímání. Zpoždění na přenosových linkách závisí na fyzické poloze stanic, přičemž délka vedení mezi stanicemi bývá zhruba dvojnásobná oproti přímé vzdálenosti, což je jednak způsobeno způsobem položení fyzických kabelů vedení sítě (podél silnic, železnic, vedení vysokého napětí apod.) a jednak může být způsobeno směrovací politikou (levnější nebo rychlejší linka, ale delší). Vzhledem k tomu, že pro transportní sítě bývá použito optické vlákno, tak uvažujeme rychlost šíření světla v optickém vláknu, což je přibližně 0,65c, tedy 194 865 km/s. Pro vzdálenosti větší než 1 000 km převažuje tato část zpoždění v celkovém zpoždění. Zpoždění v mezilehlých zařízeních (aktivní prvky, přepínače a směrovače) závisí na délce vstupní fronty, rychlosti zpracování a délce výstupní fronty. Čas, který zařízení potřebuje pro přesunutí datové jednotky ze vstupní do výstupní fronty, je závislý na rychlosti a vykonávaných funkcích daným zařízením. Pro přepínače uvažujeme obvyklou latenci 1–10 mikrosekund, pro směrovače uvažujeme několikrát více (10–100 mikrosekund), přičemž platí, že se stoupajícím zatížením prvku se zvyšuje zpoždění komunikace [21].

Měření zpoždění přenosu vyžaduje měření času mezi odesláním a příjmem paketu. Pro provedení měření je nezbytné mít přesně synchronizované hodiny u odesílatele a příjemce, což je prakticky velký problém, proto se v praxi bere v úvahu pouze čas na zařízení odesílatele. Zpoždění RTT (Round-Trip Time) se měří na trase mezi odesílatelem, příjemcem a zpět k odesílateli.

Druhou skupinou metod pro geolokaci jsou metody pasivní, spočívající v získávání dostupných informací o síťovém zařízení z různých veřejných nebo soukromých databází. Pasivní metody můžeme rozdělit na geolokaci na základě IP adresy, DNS (Domain Name System) nebo s využitím WiFi. Geolokace na základě IP adresy patří mezi nejjednodušší, protože IP adresa zařízení, případně internetové brány, je dostupná vždy. Nejrozšířenější veřejnou geolokační databází je databáze Whois, do které přispívají registrátoři domén. K vyhledávání v databázi se využívá program whois. Ze soukromých databází bych zmínil databáze Maxmind, IP2Location a další. Společnost Maxmind vyvíjí jak komerční databáze, tak i databázi open source. Vyhledávání

elektrorevue
ISSN 1213 - 1539

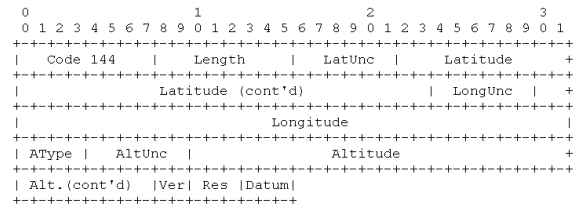
v databázích je možné prostřednictvím webu společnosti nebo s využitím knihovny v jazyce C [22].

Firma Google shromažďuje mapové údaje pomocí tzv. Google Cars, kdy mimo jiné sbírá údaje i o dostupných WiFi sítích v okolí. Služba je dynamická, takže navíc umožňuje zaměřování dalších nových WiFi sítí, které se objeví v dosahu sítí a přístupových bodů již zaměřených. Google při zaměřování využívá údaje z protokolu IEEE 802.11, zejména název sítě SSID (Service Set Identification), hardwarovou adresu MAC, a sílu signálu. Na základě změřené síly signálu k ostatním přístupovým bodům potom pomocí triangulace Google odhaduje pravděpodobnou polohu nové sítě.

Volitelný doplněk DHCP GeoLoc Option umožňuje prostřednictvím protokolu DHCP zaslání 18 bajtového pole s údaji o poloze klientovi. Na obr. 3 vidíme strukturu pole GeoLoc Option. Položka Length udává celkovou délku pole, pro verzi 1 je to 16 bajtů. Položka LatUnc udává rozlišení zeměpisné šířky (Latitude), hodnota udává počet platných bitů pole Latitude. Položka Latitude obsahuje údaj o zeměpisné šířce, 34 bitů položky je rozděleno na 9 bitovou celočíselnou část zeměpisné šířky a na desetinnou část zeměpisné šířky, pro kterou je vyhrazeno zbývajících 25 bitů. Informace je kódována ve dvojkovém doplňku, kladné číslo udává severní šířku a záporné jižní šířku. Analogicky tyto informace platí i pro zeměpisnou délku a její rozlišení (položka Longitude a LongUnc). Kladné hodnoty zeměpisné délky platí pro východním délku a záporné pro západní délku [23].

2.2.2. **DHCPv4 GeoLoc Option**

The format of the DHCPv4 GeoLoc Option is as follows:



Obr. 3: Struktura pole DHCPv4 GeoLoc Option [23].

GeoLoc Option umožňuje určit i nadmořskou výšku stanice (položka AType). Výška stanice může být udávána v metrech (AType = 1) nebo v patrech (AType = 2). Výška v patrech se používá při nasazení WiFi sítě v budovách. Položka Ver obsahuje verzi, současná verze je verze 1. Položka Res je rezervována pro budoucí využití. Položka Datum udává souřadný systém, je použit referenční elipsoid WGS84 (World Geodetic System 1984) nebo severoamerický NAD83 (North American Datum 1983). Geografická poloha je citlivá informace, proto RFC 6225 (Request For Comments) specifikuje, že informace GeoLoc Option je přenášena jen na vyžádání klienta a poté je uložena na straně klienta [23].

6 Závěr

Dnes můžeme sledovat prudký rozvoj výpočetní a telekomunikační techniky. Počítače se zrychlují, kapacita komunikačních linek se zvyšuje a internet je dostupný téměř všude. V této souvislosti se objevuje nový fenomén označovaný anglickou zkratkou BYOD (Bring Your Own Device), který znamená významný tlak na bezpečnost především firemních dat [24].

V souvislosti s rozšířením a dostupností internetu souvisí i budování příslušné infrastruktury, kdy bývá často využita technologie WiFi pro tzv. poslední míli na cestě paketů k uživateli.

Rozmachu WiFi napomáhá dostupnost notebooků s podporou bezdrátových sítí, chytrých mobilních telefonů a dalších zařízení. Zpráva OECD (The Organisation for Economic Co-operation and Development) uvádí, že v roce 2014 82% dospělé populace v členských zemích organizace používalo internet a přes 75% ho používalo denně. OECD odhaduje, že běžná domácnost se dvěma dospívajícími dětmi bude mít v roce 2017 až 25 elektronických zařízení připojených k internetu [25].

S rozvojem WiFi zařízení směrem k zařízením páté generace dochází k posunu i ve skupině standardů 802.11, a to od 802.11 a/n k standardu 802.11 ac, přičemž standard 802.11 ac je navržen jako zpětně kompatibilní [26].

Mezi širokými možnostmi, které WiFi zařízení nabízejí, patří i možnost geolokace pomocí bezdrátových sítí, datové výstupy těchto zařízení mohou být graficky zpracovány pomocí prohlížečů HTML stránek, což umožňuje nově vyvíjený standard HTML5 s možností využití prvků geolokace. V této oblasti je vyvíjeno mimořádné úsilí o sběr polohových údajů, vytváření databází, map a následné poskytování těchto údajů uživatelům.

Intenzivní vývoj v tomto oboru s sebou přináší zvyšování rychlosti, dosahu a tlak na zvyšování bezpečnosti bezdrátových sítí. Poslední vývoj směřuje k využití bezdrátových sítí v oblasti počítačových architektur, senzorových sítí, lidského zdraví v podobě monitoringu životních funkcí, dopravě a dále v internetu věcí.

Literatura

[1] MORRIS, J. *The race to the FinFETs* [online]. San Francisco: CBS Interactive, 2014-10-02 [cit. 2016-07-10]. Dostupné z: http://www.zdnet.com/article/the-race-to-the-finfets/

[2] CBL COMMUNICATION BY LIGHT. *Laser Link 4E1/155* [online]. Pardubice: CBL Communication by light, c2016 [cit. 2016-05-16]. Dostupné z: http://www.cbl.cz/pdf/opticke-bezdratove-spoje/LASER-LINK-155-4E1.pdf

[3] BÍLÝ, V. *GSMweb.cz* [online]. GSMweb.cz, c1997-2016 [cit. 2016-05-16]. Dostupné z: http://www.gsmweb.cz

[4] WESTERN DIGITAL TECHNOLOGIES. *Přenosný pevný disk* [online]. Irvine: Western Digital Technologies, c2014 [cit. 2016-05-16]. Dostupné z: http://www.wdc.com/wdproducts/library/UM/CZE/4779-705118.pdf

[5] ASUSTEK COMPUTER. *RT–AC5300* [online]. Taipei: Asustek Computer, c2015 [cit. 2016-05-16]. Dostupné z:

elektrorevue
ISSN 1213 - 1539

http://dlcdnet.asus.com/pub/ASUS/wireless/RT-AC5300/E10434_RT_AC5300_Manual.pdf

[6] QUANTENNA COMMUNICATIONS. *Quantenna Demonstrates 10G Wi-Fi Platform at CES 2015* [online]. Fremont: Quantenna Communications, 2015-05-01 [cit. 2016-08-21]. Dostupné z: http://www.quantenna.com/pressrelease-01_05_15.html

[7] YAMAMIYA, T. *WiFiDocs/Adhoc* [online]. Londýn: Canonical, 2011-05-23 [cit. 2016-07-10]. Dostupné z: https://help.ubuntu.com/community/WifiDocs/Adhoc

[8] XFCE DEVELOPMENT TEAM. *Preparations for porting thunar-volman to udev/GIO* [online]. Xfce Development Team, 2010-10-02 [cit. 2016-07-10]. Dostupné z: https://wiki.xfce.org/dev/thunar-volman-udev

[9] HOLMES, A. *A comparison of SCO and ACL packets for audio transmission in Bluetooth* [online]. Southampton: University of Southampton, 2002-12-13 [cit. 2016-07-10]. Dostupné z: http://mms.ecs.soton.ac.uk/mms2003/papers/2.pdf

[10] ASUSTEK COMPUTER. *USB-BT400* [online]. Taipei: Asustek Computer, c2015 [cit. 2016-05-16]. Dostupné z: https://www.asus.com/us/Networking/USBBT400/specifications/

[11] ZELINKA, T.; SVÍTEK, M. *Telekomunikační řešení pro informační systémy síťových odvětví*. Praha: Grada, 2009. 218 p. ISBN 978-80-247-3232-9.

[12] ORGONÁŠ, J. *ZigBee – bezdrotové technológie známe i neznáme* [online]. Bratislava: Digital Visions, 2011-06-01 [cit. 2016-05-16]. Dostupné z: http://old.itnews.sk/2011-06-01/c140924-zigbee-bezdrotove-technologie-zname-inezname

[13] HOPE MICROELECTRONICS. *HPTZ01-TTL/HPTZ01P-TTL V1.0* [online]. Xili Town: *Hope Microelectronics*, c2016 [cit. 2016-05-16]. Dostupné z: http://www.hoperf.com/upload/docs/zigbee/HPTZ01X%20Transparent%20transmission%20module%20-en.pdf

[14] ITU. *Recommendation ITU-R P.2040-1* [online]. Ženeva: ITU, c2015 [cit. 2016-07-10]. Dostupné z: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.2040-1-201507-I!!PDF-E.pdf

[15] MINISTERSTVO DOPRAVY. *Georadarová metoda konstrukcí pozemních komunikací* [online]. Praha: Ministerstvo dopravy, c2011 [cit. 2016-07-10]. Dostupné z: http://www.pjpk.cz/TP%20233.pdf

[16] KUSÁK, I. *Chování stavebních materiálů ve střídavém elektrickém poli, Impedanční spektroskopie, nový nástroj pro testování kvality stavebních materiálů* [online]. Brno: Vysoké učení technické v Brně, c2014 [cit. 2016-07-10]. Dostupné z: http://www.supmat.cz/DownloadHandler.ashx?pg=7ae3aef9-1f7f-412f-be29-2ada6b63809a&section=86ad6b7b-e618-44cb-8c9a-7f68b4902683&file=Kus%C3%A1k_impedancni_spektroskopie.ppt

[17] IEEE. *IEEE 802.11-2012. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications* [online]. New York: IEEE, 2012-03-29 [cit. 2016-05-16]. Dostupné z: http://standards.ieee.org/getieee802/download/802.11-2012.pdf. ISBN 978-0-7381-7245-3.

[18] DEVOLO. *Devolo WiFi Repeater* [online]. Aachen: Devolo, c2016 [cit. 2016-05-16]. Dostupné z: http://www.devolo.com/en/Products/devolo-WiFi-Repeater/

[19] WEB ZDARMA. *Bezdrátové sítě* [online]. Liberec: Web zdarma [cit. 2016-05-16]. Dostupné z: http://bezdratovesite.wz.cz/

[20] SAITO, W. H. Our Naked Data. *Futurist* [online], Červenec, Srpen 2011, vol. 45, no. 4, p. 42-45 [cit. 2016-07-10]. Dostupné z: EBSCOhost. ISSN 0016-3317.

[21] BALEJ, J.; KOMOSNÝ, D. Zdroje zpoždění při komunikaci v Internetu. *Elektrorevue* [online], Červen 2010, vol. 12, no. 3 [cit. 2016-05-16]. Dostupné z: http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/0/zdroje-zpozdeni-pri-komunikaci-v-internetu/. ISSN 1213-1539.

[22] VERNER, L.; KOMOSNÝ, D. Geolokace síťových zařízení v internetových sítích. *Elektrorevue* [online], Červen 2011, vol. 13, no. 3 [cit. 2016-05-16]. Dostupné z: http://www.elektrorevue.cz/cz/clanky/komunikacni-technologie/0/geolokace-sitovych-zarizeni-v-internetovych-sitich/. ISSN 1213-1539.

[23] POLK, J.; et al. *RFC 6225. Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information* [online]. Fremont: IETF, c2011 [cit. 2016-05-16]. Dostupné z: https://tools.ietf.org/html/rfc6225. ISSN 2070-1721.

[24] ČIMIB. *BYOD* [online]. Praha: ČIMIB, c2016 [cit. 2016-07-10]. Dostupné z: http://www.cimib.cz/novinka/13-byod

[25] OECD. *OECD Digital Economy Outlook 2015* [online]. Paris: OECD, c2015 [cit. 2016-08-21]. Dostupné z: http://ec.europa.eu/eurostat/documents/42577/3222224/Digital+economy+outlook+2015/dbdec3c6-ca38-432c-82f2-1e330d9d6a24. ISBN 978-92-64-23244-0.

[26] CISCO SYSTEMS. *802.11ac: The Fifth Generation of Wi-Fi Technical White Paper* [online]. San Jose: Cisco Systems, 2014-03-27 [cit. 2016-07-10] Dostupné z: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-3600-series/white_paper_c11-713103.html