

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA DOPRAVNÍ



Bakalářská práce

ALTERNATIVNÍ TELEKOMUNIKAČNÍ ŘEŠENÍ
NA BÁZI IEEE 802.11 V ITS APLIKACÍCH

Martin Šrotýř

Praha 2007

Originál zadání



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ
FAKULTA DOPRAVNÍ

Katedra: K614

Akademický rok: 2006/2007

Rozsah grafických prací: 10 - 20 obrázků

Rozsah průvodní zprávy: 50 - 60 stran

Seznam odborné literatury: Žalud, V.: Moderní radioelektronika

Kally, F., Peniak, P.: Počítačové sítě. Grada, Praha 2003.

odborné časopisy, internet

ZADÁNÍ BAKALÁŘSKÉ PRÁCE (PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

pro

Martina Šrotýře

obor

Automatizace v dopravě a telekomunikacích

Vedoucí bakalářské práce: doc. Ing. Tomáš Zelinka, CSc.

Název tématu:

Alternativní telekomunikačních řešení na bázi IEEE 802.11 v ITS aplikacích

Datum zadání bakalářské práce:

Datum odevzdání bakalářské práce:

L.S.

Zásady pro vypracování:

Popište současný stav dostupných bezdrátových telekomunikačních systémů.

Vysvětlete úlohu performačních indikátorů v hodnocení přenosových vlastností komunikačních řešení, specifiky pokud jsou součástí telematických systémů.

Analýzujte současný stav implementace rodiny standardů řady IEEE Std. 802.11 (WiFi) a jejich postavení v dopravních aplikacích. Parametry dostupných řešení srovnajte s parametry připravovaného standardu IEEE 802.11e.

Zhodnoťte potenciál jednotlivých variant řady IEEE 802.11 ve srovnání s možnostmi systémů na bázi IEEE Std. 802.16 (WiMax). Stanovte kritéria pro volbu alternativního řešení WiFi v kontextu volby z více přístupových alternativ s využitím standardů CALM anebo i jiných nástrojů nekolizního přepínání (handover).

V rámci projektu Letiště Praha, které bude dominantně řešeno implementací mobilního Wimax řešení, navrhnete doplňkové pokrytí vybraných lokalit WiFi řešením a zhodnoťte technické a ekonomické přednosti stejně jako i případná rizika takového přístupu.

Vedoucí katedry

Děkan

V Praze dne 31.8.2007

Čestné prohlášení

Já, Martin Šrotýř, student Fakulty dopravní ČVUT v Praze prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a veškeré materiály, z nichž jsem čerpal pro svoji práci, jsou uvedeny v seznamu literatury.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne:

podpis:

Poděkování

Chtěl bych poděkovat všem, jejichž rady přispěly velkou měrou ke zpracování této bakalářské práce, za poskytnutí informací a odborných konzultací vedoucímu mé bakalářské práce doc. Ing. Tomáši Zelinkovi, CSc., a dále kolegům z projektu „Člověk a globální komunikace“.

Abstrakt

Autor: Martin Šrotýř

Název bakalářské práce: Alternativní telekomunikační řešení na bázi IEEE 802.11 v ITS aplikacích

Škola: České vysoké učení technické v Praze, Fakulta dopravní

Rok vydání: Praha 2007

Počet stran: 77

Tato bakalářská práce pojednává o alternativách komunikačních řešení na bázi IEEE 802.11 pro aplikace inteligentních dopravních systémů (ITS). Podává přehled o dostupných bezdrátových technologiích, systémech a některých službách potenciálně možných pro využití v ITS. Zpracovává přehled performačních indikátorů užívaných pro klasifikaci jak telekomunikačních, tak telematických vlastností systémů nutných pro správnou volbu komunikačního řešení. Dále se zaměřuje na ověření stavu standardu 802.11e, který má zajistit potřebnou kvalitu služeb pro přenos dat pro ITS aplikace. Výsledkem této práce je zhodnocení použitelnosti technologie WiFi pro ITS aplikace a dále návrh alternativního doplňkového řešení pro Letiště Praha na bázi IEEE 802.11 a jeho technické, bezpečnostní a ekonomické zhodnocení.

Klíčová slova:

ITS, WiFi, WiMax, IEEE 802.11, IEEE 802.11e, CALM

Abstract

Author: Martin Šrotýř

Title of bachelor work: Alternative telecommunication solution based on IEEE 802.11 for ITS applications.

School: Czech technical university in Prague, Faculty of transportation sciences

Year publication: Prague 2007

Pages: 77

This bachelor work dissert on alternative communications solutions based on IEEE 802.11 for intelligent transport systems (ITS) applications. Processes summary of accessible wireless technologies, systems and some services potentially possible for usage in ITS. Processes summary of performance indicators used to classification telecommunications and telematics systems feature necessary for correct choice of communication solution. Then we're check status of standard 802.11e, which has ensure necessary quality of services for data transmission for ITS application. Result of this work is estimation usability WiFi technology for ITS applications and further proposal of alternative additional solution for Airport Prague based on IEEE 802.11 and his technical, security and economics estimation.

Keywords:

ITS, WiFi, WiMax, IEEE 802.11, IEEE 802.11e, CALM

Obsah

SEZNAM POUŽITÝCH ZKRATEK.....	9
SEZNAM OBRÁZKŮ A TABULEK	13
SEZNAM OBRÁZKŮ	13
SEZNAM TABULEK	13
1. ÚVOD.....	14
1.1. PŘEDMLUVA.....	14
1.2. CÍL PRÁCE	14
2. SOUČASNÝ STAV BEZDRÁTOVÝCH TELEKOMUNIKAČNÍCH PŘENOSOVÝCH SYSTÉMŮ.....	15
2.1. KLASIFIKACE BEZDRÁTOVÝCH SYSTÉMŮ	15
2.2. BEZDRÁTOVÉ OSOBNÍ SÍTĚ (WPAN).....	19
2.2.1. Bluetooth – 802.15.1.....	19
2.2.2. UWB – 802.15.3	19
2.2.3. ZigBee – 802.15.4.....	20
2.2.4. WPAN – využití pro ITS.....	22
2.3. BEZDRÁTOVÉ LOKÁLNÍ SÍTĚ (WLAN)	22
2.3.1. WiFi 5 – 802.11a	25
2.3.2. WiFi – 802.11b	26
2.3.3. WiFi – 802.11g.....	26
2.3.4. WiFi – využití pro ITS.....	27
2.4. BEZDRÁTOVÉ METROPOLITNÍ SÍTĚ (WMAN)	27
2.4.1. WiMAX – 802.16	27
2.4.1.1. 802.16d.....	28
2.4.1.2. 802.16e.....	28
2.4.2. MBWA – 802.20.....	29
2.4.3. WMAN – využití pro ITS.....	29
2.5. BEZDRÁTOVÉ ROZLEHLÉ SÍTĚ (WWAN).....	29
2.5.1. DTMF (Dual Tone Multiple Frequency)	30
2.5.2. CSD (Circuit Switched Data)	30
2.5.3. HSCSD (High Speed Circuit Switched Data)	30
2.5.4. SMS (Short Message Service).....	31
2.5.5. GPRS (General Packet Radio Service).....	31
2.5.6. EDGE (Enhanced Data Rates for GSM Evolution).....	31
2.5.7. CDMA 2000 (Code Division Multiple Access)	32
2.5.8. UMTS (Universal Mobile Telecommunication System).....	32
2.5.9. WWAN – využití pro ITS.....	34
2.6. POROVNÁNÍ JEDNOTLIVÝCH TECHNOLOGIÍ	34
3. PERFORMAČNÍ INDIKÁTORY.....	35
3.1. TELEMATICKÉ PERFORMAČNÍ INDIKÁTORY	35
3.1.1. Přesnost.....	35
3.1.2. Spolehlivost.....	36
3.1.3. Dostupnost.....	36
3.1.4. Kontinuita (spojitost).....	37
3.1.5. Integrita	37
3.1.6. Bezpečnost.....	38
3.2. TELEKOMUNIKAČNÍ PERFORMAČNÍ INDIKÁTORY	39
3.2.1. Aktivační doba dostupnosti služby.....	39
3.2.2. Dostupnost služby (např. virtuálního okruhu)	39
3.2.3. Doba mezi dvěma poruchami – MTBF.....	40
3.2.4. Doba obnovení služby – MTTR.....	40
3.2.5. Zpoždění	41
3.2.6. Ztráta paketů	42
3.2.7. Bezpečnost.....	42

3.3.	VZTAH MEZI TELEMATICKÝMI A TELEKOMUNIKAČNÍMI PERFORMAČNÍMI INDIKÁTORY	43
4.	STAV IMPLEMENTACE STANDARDŮ 802.11.....	45
4.1.	ZÁKLAD – 802.11A/B/G	45
4.2.	DOPLŇEK 802.11E – WIRELESS QoS.....	46
4.3.	DALŠÍ DOPLŇKOVÉ STANDARDY 802.11.....	49
4.3.1.	IEEE 802.11i	49
4.3.2.	IEEE 802.11n	49
4.3.3.	IEEE 802.11p	50
4.3.4.	IEEE 802.11r.....	50
4.4.	CERTIFIKACE A PŘÍNOS STANDARDU 802.11E	51
5.	ZHODNOCENÍ STANDARDU 802.11 PRO ITS	54
5.1.	VLASTNOSTI 802.11	54
5.1.1.	Otázka sdíleného pásma	54
5.1.2.	Otázka bezpečnosti	54
5.1.3.	Otázka handoveru.....	55
5.1.4.	Diskuse	56
5.2.	SROVNÁNÍ 802.11 VS. 802.16.....	57
5.3.	VOLBA ALTERNATIVNÍHO ŘEŠENÍ	58
5.3.1.	CALM	59
5.3.2.	L2/L3 switching	61
5.3.3.	Kritéria volby alternativy	61
6.	NÁVRH ALTERNATIVNÍHO ŘEŠENÍ PRO LETIŠTĚ PRAHA	62
6.1.	SYSTÉMOVÉ POŽADAVKY ŘEŠENÍ PRO LETIŠTĚ PRAHA	62
6.2.	NÁVRH VLASTNÍHO DOPLŇKOVÉHO ŘEŠENÍ	65
6.2.1.	Plánování pokrytí	66
6.2.2.	Architektura	68
6.2.3.	Hardware.....	69
6.3.	ZHODNOCENÍ NÁVRHU	72
6.3.1.	Ekonomické zhodnocení	72
6.3.2.	Technické zhodnocení.....	73
6.3.3.	Bezpečnostní zhodnocení.....	74
6.3.4.	Diskuse	74
7.	ZÁVĚR	75
8.	SEZNAM POUŽITÝCH ZDROJŮ.....	76
8.1.	LITERATURA	76
8.2.	INTERNETOVÉ ODKAZY	77

Seznam použitých zkratek

Zkratka	Český název	Anglický název
AC	Řízení přístupu	Admission Control
ACK	Potvrzení	Acknowledge
AES	Pokročilý šifrovací standard	Advanced Encryption Standard
AIFS	Arbitrážní IFS	Arbitration Interframe Space
AL	Poplašný limit	Alert Limit
AP	Přístupový bod	Access Point
APSD	Automatická úspora energie	Automatic Power Save Delivery
A-SMGCS	Pokročilé řízení objektů na pohybové ploše	Advanced Surface Movement Guidance and Control System
BA	Blokové potvrzování	Block Acknowledgments
BPSK	Dvoustavové klíčování s fázovým posuvem	Binary Phase Shift Keying
BWA	Širokopásmový bezdrátový přístup	Broadband Wireless Access
CALM	Rodina standardů pro volbu nejvhodnějšího komunikačního kanálu	Communications Air-interface for Long and Medium range
CAP	Druh CFP u HCCA metody	Controlled Access Phase
CCK	Doplňkové klíčové kódování	Complementary Code Keying
CCMP	Algoritmus zajišťující integritu, autentizaci a poskytující utajení	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CDMA	Kódové dělení přenosových kanálů	Code Division Multiple Access
CFP	Nesoutěžní perioda	Contention Free Period
CME	CALM řídicí jednotka	CALM Management Entity
CP	Soutěžní perioda	Contention Period
CSD	Přepojování okruhů	Circuit Switched Data
CSMA/CA	Mnohonásobná metoda přístupu s nasloucháním nosné a zabráněním kolizí	Carrier Sense Multiple Access with Collision Avoidance
CTS	Povolení k vysílání	Clear To Send
CW	Okno sváru	Content Window
ČR	Česká Republika	Czech Republic
ČTU	Český telekomunikační úřad	Czech telecommunication department

DCF	Funkce rozložené koordinace	Distributed Coordination Function
DIFS	Mezera mezi rámci při funkci rozložené koordinace	(DCF IFS) Distributed Coordination Function Inter Frame Space
DSRC	Dedikovaná komunikace s krátkým dosahem	Dedicated Short Range Communications
DSSS	Přímá posloupnost rozprostřeného spektra	Direct Sequence Spread Spectrum
DTMF	Tónová frekvenční volba	Dual Tone Multiple Frequency
EAP	Rozšířený autentifikační protokol	Extensible Authentication Protocol
EDCA	Vylepšená DCF přístupová metoda	Enhanced DCF
EDGE	Rozšířené rychlosti pro GSM přenosy	Enhanced Data Rates for GSM Evolution
EDR	Rychlejší a úspornější Bluetooth	Enhanced Data Rate
EIRP	Střední ekvivalentní izotropicky vyzářený výkon	Equivalent Isotropically Radiated Power
FDD	Frekvenční dělení kanálů	Frequency Division Duplex
FFD	Plně funkční zařízení	Full-Functionality Device
FHSS	Rozprostřené spektrum s přeskokováním kmitočtů	Frequency-Hopping Spread Spectrum
GMSK	Gaussovská modulace s minimálním zdvihem	Gaussian Minimum Shift Keying
GNSS	Satelitní systémy pro globální navigaci	Global Navigation Satellite Systems
GPRS	Paketový radiový přenos dat	General Packet Radio Service
GPS	Globální poziční systém	Global Position System
GSM	Buňková telefonní technologie	Global System for Mobile Communications
HCCA	Přístupová metoda řízená HCF	HCF Controlled Channel Access
HCF	Hybridní koordinační funkce	Hybrid Coordination Function
HSCSD	Vysokorychlostní přepojování okruhů	High Speed Circuit Switched Data
HSDPA	Technologie vysokorychlostního stahování dat	High Speed Downlink Packet Access
HSUPA	Technologie vysokorychlostního posílání dat	High Speed Uplink Packet Access
IAPP	Protokol pro spolupráci různých AP	Inter Access Point Protocol
IEEE	Společnost elektrotechnických a elektronických inženýrů	Institute of Electrical and Electronics Engineers
IFS	Mezera mezi rámci	Inter Frame Space

IP	Protokol síťové vrstvy komunikace dle ISO/OSI modelu	Internet Protocol
ITS	Intelligentní dopravní systémy	Intelligent Transport Systems
LAN	Lokální síť	Local Area Network
MAC	Kontrola přístupu k médiu	Medium Access Control
MAN	Metropolitní síť	Metropolitan Area Network
MIMO	Více vstupů – více výstupů	Multiple Input – Multiple Output
MTBF	Doba mezi dvěma poruchami	Mean Time Between Failure
MTTR	Doba obnovení služby	Mean Time To Recover
NLOS	Nepřímá viditelnost	Non Line Of Sight
NoAck	Žádné potvrzování	Not Acknowledged
OBU	Palubní jednotka	On Board Unit
OFDM	Ortogonální multiplex s kmitočtovým dělením	Orthogonal Frequency Division Multiplexing
OFDMA	Ortogonální přístup s kmitočtovým dělením	Orthogonal Frequency Division Multiple Access
P2P	spoj typu bod – bod	Peer-to-peer
PAN	Osobní síť	Personal Area Network
PCF	Funkce bodové koordinace	Point Coordination Function
PDA	Osobní digitální asistent	Personal Digital Assistant
PHY	Fyzická vrstva	Physical Layer
QAM	Kvadrurní amplitudová modulace	Quadrature Amplitude Modulation
QoS	Kvalita Služeb	Quality of Service
QPSK	Čtyřstavové klíčování s fázovým posuvem	Quadrature Phase Shift Keying
RFD	Zařízení s redukovanou funkcí	Reduced-Functionality Device
RLC	Řízení radiového spoje	Radio Link Control
RSN	Silná bezpečnostní síť	Robust Security Network
RTS	Požadavek k vysílání	Request To Send
SAP	Místo poskytování služby	Service Access Point
SIFS	Krátká mezera mezi rámci	Short Inter Frame Space
SIG	Speciální zájmová skupina	Special Interest Group
SLA	Dohoda o kvalitě poskytovaných služeb	Service Level Agreement
SMS	Krátké textové zprávy	Short Message Services
SOFDMA	Škálovatelný ortogonální přístup s kmitočtovým dělením	Scalable Orthogonal Frequency Division Multiple Access

SS	Rozprostřené spektrum	Spread Spectrum
SSID	Identifikátor bezdrátového kanálu	Service Set Identifier
TAP	Urychlený přechodový protokol	Transition Acceleration Protocol
TC	Třídy provozu	Traffic Classes
TCP	Spojově orientovaný protokol pro přenos toku bajtů na transportní vrstvě se spolehlivým doručováním	Transmission Control Protocol
TDD	Časové dělení kanálů	Time Division Duplex
TDMA	Časové dělení	Time Division Multiple Access
TKIP	Protokol dynamicky měnící klíče	Temporal Key Integrity Protocol
TS	Proudy provozu	Traffic Streams
TTF	Čas do aktivace služby	Time To First Fix
TXOP	Přenášecí příležitost	Transmit Opportunity
UDP	Minimální protokol transportní vrstvy, orientovaný na zprávy	User Datagram Protocol
UMTS	Univerzální mobilní telekomunikační systém	Universal Mobile Telecommunication System
USB	Univerzální sériové datové rozhraní	Universal Serial Bus
UWB	Ultra Wide Band (technologie)	UltraWideBand
VSWR	Poměr mezi maximem a minimem stojaté vlny napětí	Voltage Standing Wave Ratio
WAN	Rozlehlé síť	Wide Area Network
WAVE	Bezdrátový přístup pro dopravní prostředí	Wireless Access for the Vehicular Environment
WEP	Soukromí ekvivalentní drátovým sítím	Wired Equivalent Privacy
WiFi	“bezdrátová věrnost”, konfliktní bezdrátový přenos ve sdíleném pásmu	Wireless Fidelity
WiMax	Bezdrátová technologie WiMax	Worldwide Interoperability for Microwave Access
WLAN	Bezdrátové lokální síť	Wireless Local Area Network
WMAN	Bezdrátové metropolitní síť	Wireless Metropolitan Area Network
WME	Bezdrátové multimediální rozšíření	Wireless Multimedia Extensions
WMM	Bezdrátová multimédia	Wireless MultiMedia
WPA	WiFi chráněný přístup	WiFi Protected Access
WPAN	Bezdrátové osobní síť	Wireless Personal Area Network
WWAN	Bezdrátové rozlehlé síť	Wireless Wide Area Network

Seznam obrázků a tabulek

Seznam obrázků

Obr. 1 - Rozdělení technologií v závislosti jejich mobility na přenosové kapacitě	16
Obr. 2 - Klasifikace bezdrátových systémů dle použití.....	18
Obr. 3 - Využití kmitočtového pásma	20
Obr. 4 - Topologie sítě ZigBee.....	21
Obr. 5 - Režim DCF ve WLAN.....	24
Obr. 6 - Frekvenční spektrum UMTS.....	33
Obr. 7 - IEEE 802.11e MAC architektura	46
Obr. 8 - Certifikace IEEE 802.11e	51
Obr. 9 - Test WMM priorizace.....	52
Obr. 10 - CALM architektura	60
Obr. 11 - CALM management entita (CME)	60
Obr. 12 - Disponibilní časy pro přenos a zpracování polohy při chybě 6,5 m pro různé rychlosti.....	64
Obr. 13 - Umístění a očekávané pokrytí AP.....	66
Obr. 14 - Detail pokrytí oblasti v okolí hangárů u terminálu jih.....	67
Obr. 15 - Architektura návrhu	68
Obr. 16 - Cisco Aironet 1240AG Serie	69
Obr. 17 - Instalace Cisco Aironet 1240AG Serie do plastového boxu pro venkovní použití	70
Obr. 18 - Anténa PW SA58-120-16	70
Obr. 19 - Vyzařovací diagramy antén PW SA58-120-16WB a SA58-90-17-WB.....	71
Obr. 20 - Všesměrová anténa PW OD58-12 a její vyzařovací diagram.....	71

Seznam tabulek

Tab. 1 - Přehled WPAN technologií.....	22
Tab. 2 - Přehled WLAN technologií	27
Tab. 3 - 802.11e/802.1d priority.....	48
Tab. 4 - Doba čekání na vysílání	48
Tab. 5 - SWOT analýza standardu IEEE 802.11	57
Tab. 6 - Parametry IEEE 802.11 a 802.16.....	57
Tab. 7 - Oblasti letištní plochy podle nároků na performační indikátory.....	65
Tab. 8 - Parametry přístupového bodu Cisco Aironet 1240AG Serie	70
Tab. 9 - Parametry antén PW SA58-90-17-WB a SA58-120-16-WB.....	70

1. Úvod

1.1. Předmluva

Bezdrátové telekomunikační sítě se používají již mnoho desítek let. V posledních letech jsme svědky prudkého vzestupu nebo přesněji rozšíření internetu do všech míst a technologií. Stalo se tak s nástupem nových technologií, které umožňují spojování míst bezdrátově s nízkými náklady. Bezdrátové sítě nabízejí dnes široké spektrum možností pro jejich využití. Objevuje se mnoho možných aplikací bezdrátových technologií v oblasti inteligentních dopravních systémů (ITS), ovšem pro využití těchto systémů pro profesionální telematické aplikace je potřeba řešit jejich dostupnost, spolehlivost a další parametry. Bezdrátové systémy se staly součástí našeho každodenního života.

1.2. Cíl práce

Jedním z cílů práce je zanalyzování a zhodnocení vhodnosti použití standardu 802.11 pro ITS aplikace. Dalším cílem je návrh alternativního doplňkového řešení pro Letiště Praha v rámci projektu Monitorování a řízení pohybu objektů po ploše letiště pomocí GNSS (Grant MDS 802/210/112) v rámci účasti České republiky v projektu Galileo na bázi IEEE 802.11 a jeho technické, ekonomické a bezpečnostní zhodnocení. Pro tento návrh je nutné předem podat přehled o dostupných bezdrátových technologiích, které jsou dnes a nebo brzy budou aktuální, především o doplňku standardu 802.11e zajišťujícím kvalitu služeb QoS. V souvislosti s návrhem alternativního doplňkového řešení je třeba se zabývat volbou alternativního telekomunikačního řešení.

2. Současný stav bezdrátových telekomunikačních přenosových systémů

Bezdrátové technologie se uplatňují jak v domácích sítích, podnikových sítích, tak i v řešení poslední míle přístupových sítí a často lze vidět i řešení páteřních sítí pomocí bezdrátové technologie. Širokopásmový bezdrátový přístup (BWA, Broadband Wireless Access) představuje moderní dostupný prostředek pro vytvoření telekomunikačních systémů. BWA systémy pracující na vyšších frekvencích (více než jednotky GHz) požadují přímou viditelnost. Díky novým technologiím (modulace, anténní systémy) již některé nové BWA systémy tento požadavek na přímou viditelnost nemají. Firemní řešení BWA rychle přechází k otevřeným systémům podle nových norem pro metropolitní bezdrátové sítě WMAN. BWA systémy jsou alternativou drátových (metalických, optických) telekomunikačních systémů. Poskytují větší flexibilitu a mobilitu, ale oproti drátovým systémům mají BWA systémy omezenou přenosovou kapacitu a často se můžeme setkat s dalšími specifickými problémy, jako je například provoz v bezlicenčním pásmu [3].

2.1. Klasifikace bezdrátových systémů

Bezdrátové systémy lze členit dle několika hledisek.

Jako první členění bych uvedl dělení dle **podpory mobility objektů** na:

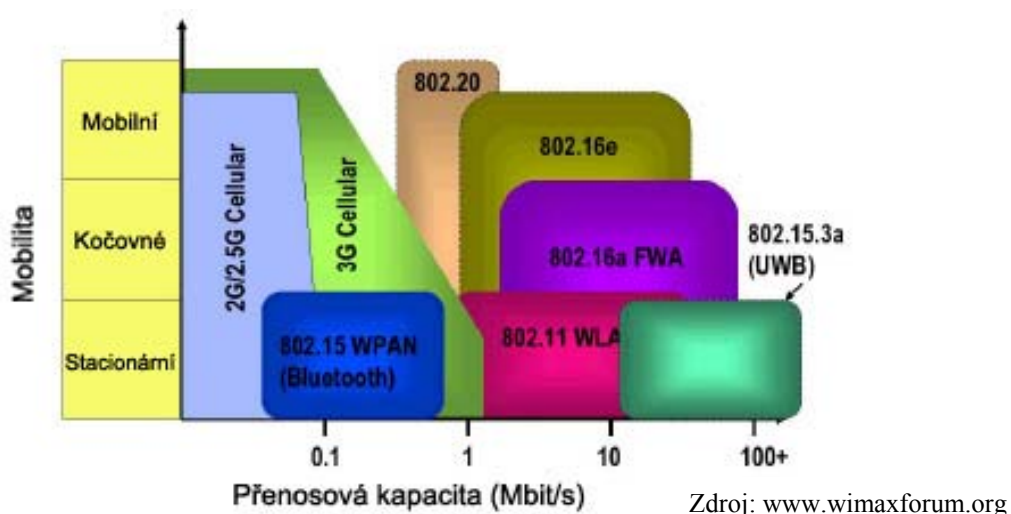
- **stacionární sítě**
- **kočovní sítě**
- **mobilní sítě**

Stacionární (Stationary) sítě jsou dle názvu sítě pro komunikaci v klidovém stavu, bez žádného přesunu objektů, tj. že bezdrátová technologie jak vysílací tak přijímací část je pevně rozmístěna na vysílacích a přijímacích bodech a v závislosti na použité technologii by při změně polohy došlo ke ztrátě komunikace.

Kočovné (Nomadic) sítě jsou sítě, kde při komunikaci je objekt v klidu (nebo ve stavu blízcímu se klidu), avšak objekt se mezi klidovými stavy pohybuje. Například u vozidla, které se pohybuje, se dá komunikace použít při jeho zastavení například na čerpacích stanicích, světelně řízených křižovatkách, při parkování, atd.

Mobilní (Vehicular) sítě jsou sítě s plnou podporou mobilních komunikujících objektů.

Rozdělení konkrétních bezdrátových technologií používaných pro různé druhy sítí je uvedeno na obr. 1.



Obr. 1 - Rozdělení technologií v závislosti jejich mobility na přenosové kapacitě

Dělení dle **typu signálu** [3] na:

- **radiové sítě**
- **optické bezdrátové sítě**
- **infračervené sítě**

Radiové sítě patří mezi nejčastější bezdrátové sítě. Mají různý dosah, od desítek kilometrů až po jednotky metrů. Jsou vhodné jak pro domácí sítě, tak i pro širokopásmový přístup k Internetu. Radiový signál je schopen proniknout různými překážkami, ovšem některé sítě potřebují přímou viditelnost (bez překážek). Čím vyšší je použitý kmitočet, tím menší je dosah sítě. Signál o nízkém kmitočtu se šíří jako povrchová vlna, tzn. že sleduje zakřivení Země a může docílit značného dosahu. Signál o kmitočtu od jednotek GHz se šíří jako přímá vlna a je omezen geometrickým (optickým) horizontem, proto je jeho dosah omezen přímou viditelností. Mikrovlnné technologie jsou vhodné pro komunikaci ve vnitřním i vnějším prostředí, kde podporují přenosy do desítek km. Pro vnitřní prostředí

se hodí systémy s rozprostřeným spektrem. Útlum signálu není přesně úměrný použitému kmitočtu a nevzrůstá rovnoměrně s vyšším kmitočtem, protože svůj vliv má nehomogenní prostředí (elektromagnetické vlny totiž utlumují i velmi malé částčky jakékoli podoby). Radiová síť pracuje v rámci rádiových buněk, tj. prostorových oblastí, v nichž mohou stanice komunikovat (prostřednictvím základnové stanice nebo přístupového bodu).

Optické bezdrátové sítě mají dosah od desítek metrů až po jednotky kilometrů. Bohužel kvalitu komunikace velmi výrazně ovlivňuje přímá viditelnost. Pokud se vyskytne mlha či sněžení mezi optickými jednotkami tak, že na druhý konec není vidět, dochází k velkým ztrátám a často i k rozpojení spoje. Na druhou stranu ale optické bezdrátové sítě nabízejí vysokou přenosovou rychlost od jednotek Mbit/s až po jednotky Gbit/s. Jsou vhodným řešením pro podnikové sítě pro komunikaci mezi budovami nebo pro domácí sítě pro přístup k Internetu, pro řešení přístupové sítě.

Infračervené sítě mají malý dosah, nedokáží překonat překážky, jako jsou zdi, stromy atd., z čehož plyne omezení na prostor mezi zdmi a současně větší bezpečnost vůči odposlechu vně místnosti. Infračervené sítě mají mnohem větší šířku pásma než radiové sítě a nejsou limitovány dostupným spektrem. Teoreticky je tedy kapacita omezena pouze výkonem transceiveru a vlastnostmi kanálu. Infračervené sítě nepodléhají regulaci.

Dělení dle **kmitočtového pásma** na:

- **licenční**
- **bezlicenční**

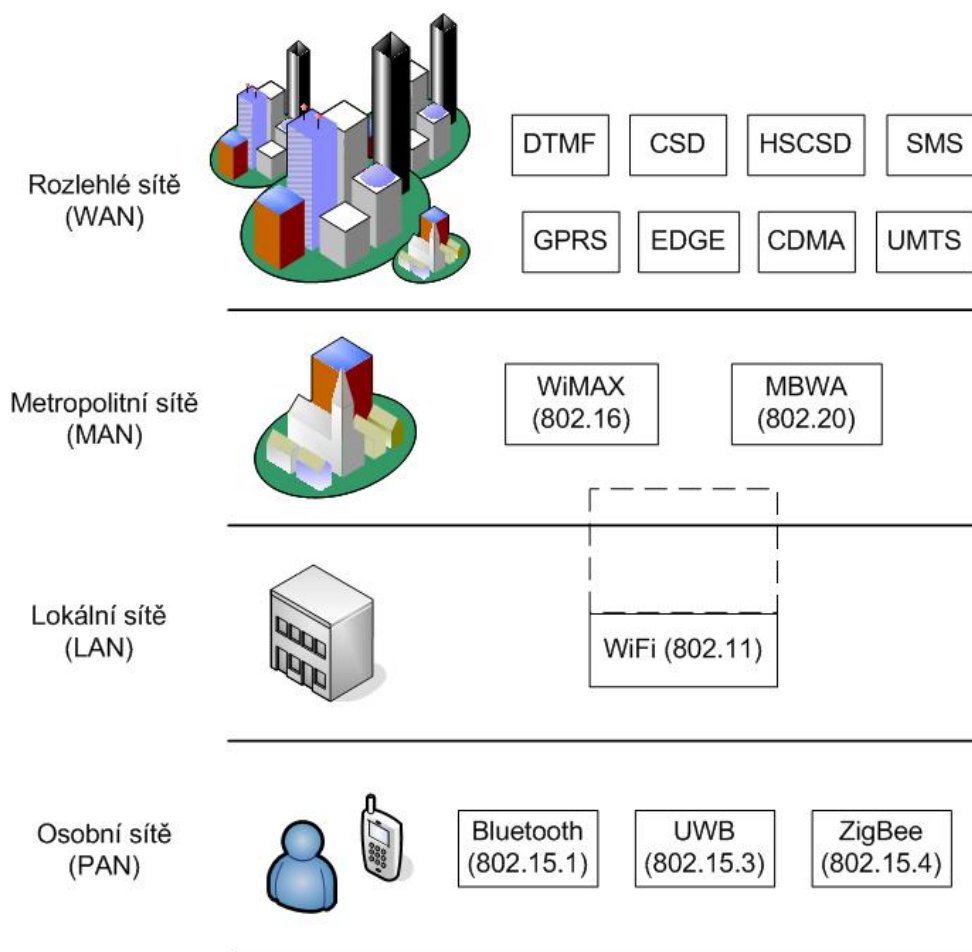
Jak již bylo uvedeno výše, bezdrátové systémy pracují buď v licencovaných pásmech, nebo bezlicenčních. Každé radiové zařízení využívá pro přenos jisté pásmo, na které je třeba v případě bezlicenčních pásem generální povolení vydávané regulačním úřadem, u nás ČTÚ (Český telekomunikační úřad) a v případě licencovaných spojů je třeba licence od regulačního úřadu. Licence na různá pásma se vydávají většinou pro celoplošné sítě v národním měřítku. Provoz rádiových sítí sleduje a upravuje regulátor a jeho kontrolní složky mají za úkol kontrolovat nejen provozovatele s udělenou licencí, ale také provozovatele sítí v bezlicenčním pásmu, kde platí pravidla omezující např. vyzařovací výkon, aby nedocházelo k vzájemnému rušení. Zatímco licenční pásma sdílí pouze vymezený počet sítí, bezlicenční pásma mohou být snadno nepříjemně přetížená

nejrůznějším typem provozu, a tak v nich často dochází k rušení negativně ovlivňujícímu kvalitu komunikace.

Dělení dle **použití** na:

- **rozlehlé** síť (WAN)
- **metropolitní** síť (MAN)
- **lokální** síť (LAN)
- **osobní** síť (PAN)

Dělení je zřejmé z obr. 2, kde jsou uvedeny konkrétní technologie, přenosové systémy či služby používané pro přenos dat. Každý druh má své specifické vlastnosti. Síť MAN a LAN se využívají při řešení první míle, zatímco LAN a PAN lze využít v domácích sítích. Rozlehlé síť představují mobilní síť 2G a 3G a jak název napovídá, jsou pro mobilní služby.



Obr. 2 - Klasifikace bezdrátových systémů dle použití

2.2. Bezdrátové osobní sítě (WPAN)

2.2.1. Bluetooth – 802.15.1

Bluetooth je rádiová technologie s relativně nízkou rychlostí určená pro bezdrátovou komunikaci v rámci osobních sítí, pro přenos hlasu, dat i videa. Technologií Bluetooth se zajímá od roku 1998 SIG (Special Interest Group), která se stará o vývoj a správu. Bluetooth standard 1.1 byl přijat normalizačním institutem IEEE jako norma pro osobní sítě pod označením IEEE 802.15.1. Norma nabízí rychlost 1 Mbit/s na fyzické vrstvě, přičemž skutečná propustnost dat se pohybuje maximálně kolem 720kbit/s. Postupem času byly do IEEE 802.15.1 zakomponovány další verze standardu Bluetooth, postupně verze 1.2 a verze 2.0. V současné době Bluetooth v2.0 EDR nabízí přenosovou rychlost 2,1 Mbit/s ve smyslu systému EDR (Enhanced Data Rate) díky nově zavedené modulaci $\pi/4$ -DQPSK, což má za následek především třikrát vyšší přenosovou rychlost (ve výjimečných případech až desetkrát vyšší) a nižší spotřebu energie [22].

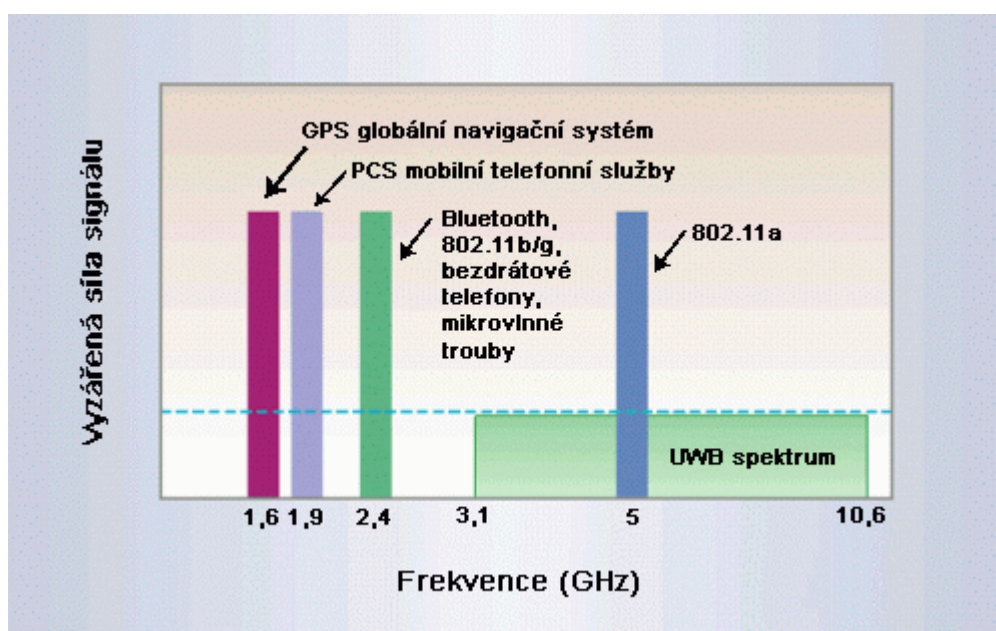
Bluetooth využívá metody rozprostřeného spektra s přeskokováním kmitočtů (FHSS, Frequency-Hopping Spread Spectrum). Během jedné sekundy provede 1600 skoků (přeladění) mezi 80 frekvencemi s rozestupem 1 MHz, čímž se brání rušení na své frekvenci, která je stejná jako u WiFi 2,4 GHz. Je definováno několik výkonových úrovní (2,5 mW, 10 mW, 100 mW), s nimiž je umožněna komunikace do vzdálenosti cca. 10 až 100 m. Hodnoty platí pouze pro volný prostor, při komunikaci přes překážky dosah rychle klesá a zvětšuje se počet chybných paketů, většinou ale nedochází ke ztrátě spojení.

2.2.2. UWB – 802.15.3

802.15.3 je norma pro malé rychlé bezdrátové sítě. Byla schválena v červnu 2003 pod označením IEEE 802.15.3. („Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks“). Verze 802.15.3a, označovaná jako UWB (UltraWideBand) patří mezi ultra rychlé bezdrátové sítě. Obě verze se ovšem podstatně liší. Základní 802.15.3 pracuje v pásmu 2,4 GHz,

kde bez problémů spolupracuje s 802.11b/g, 802.15.1 a 802.15.4. Má malou spotřebu energie a podporuje rychlost na fyzické vrstvě až do 55 Mbit/s. (11,22,33,44 a 55 Mbit/s). Systém si v závislosti na přenosových podmínkách volí jednu z pěti typů modulace pro přenos. Pro přístup k radiovému kanálu je u 802.15.3 využito časové dělení (TDMA, Time division multiple access) s podporou kvality služby (QoS, Quality of Service) a managementu napájení.

Verze 802.15.3a – UWB podporuje rychlost až 110 Mbit/s do vzdálenosti 10 m, a rychlost 480 Mbit/s do vzdálenosti 1 m s využitím pásma o šířce minimálně 500 MHz z kmitočtového intervalu 3,1 GHz až 10,6 GHz. Což při prvním pohledu vyvolává dojem, že komunikace bude rušena ostatním provozem v pásmu, ale UWB rozkládá signál v rámci širokého spektra tak, aby výkon v každém jednotlivém pásmu byl pod úrovní možného rušení jiných úzkopásmových systémů. Proto je UWB odolné vůči rušivým vlivům [3]. Na obr. 3 je vidět využití kmitočtového pásma.



Obr. 3 - Využití kmitočtového pásma

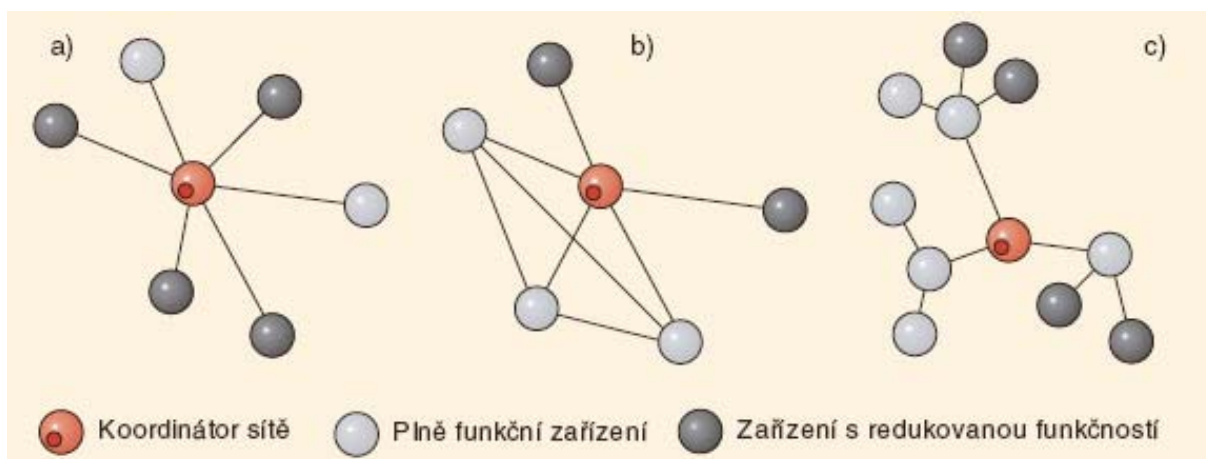
Zdroj: www.intel.com

2.2.3. ZigBee – 802.15.4

ZigBee je nízkok rychlostní rádiová technologie optimalizovaná pro statické sítě, určené pro občasný přenos menšího množství dat. V roce 2003 byla přijata jako IEEE 802.15.4.

Velkou výhodou je malá spotřeba energie a velmi nízká cena. Tím tato technologie otevírá cestu pro malá a jednoduchá bezdrátová zařízení a jejich aplikace v telematice, i v jiných oborech.

ZigBee využívá tři bezlicenční pásma. Je to celosvětově využívané pásmo 2,4 GHz s odstupem kanálů 5 MHz, to přináší 16 kanálů o celkové přenosové kapacitě 240 kbit/s na kanál. Další pásmo, které ZigBee používá, je 868 MHz, to je využíváno v Evropě a nabízí jeden přenosový subkanál o přenosové kapacitě 20 kbit/s. Poslední pásmo je 915 MHz, používané v Americe a Austrálii, které přináší 10 kanálů, každý o přenosové kapacitě 40 kbit/s. Fyzický dosah sítě je od jednotek metrů až do několika desítek metrů. Nicméně je zde možnost vytvořit samokonfigurující síť s topologií s komunikací přes více skoků. ZigBee rozeznává dvě kategorie zařízení: RFD (Reduced-Functionality Device) a FFD (Full-Functional Device). FFD může komunikovat s jakýmkoli jiným zařízením v síti jakékoli topologie a může se stát koordinátorem. RFD má velmi jednoduchou implementaci, proto nemůže být koordinátorem sítě a může komunikovat pouze s koordinátorem (v topologii hvězda). Většina senzorů patří do třídy RFD. Topologie jsou nejrozmanitější (hvězda, strom, mesh) a síť může propojovat od několika až do 65 000 zařízení [17], [23], [29]. Na obr. 4 jsou zobrazeny některé možné topologie sítě ZigBee. a) topologie typu hvězda, b) topologie typu mesh, c) topologie typu strom



Obr. 4 - Topologie sítě ZigBee

Zdroj: www.automatizace.cz

2.2.4. WPAN – využití pro ITS

	IEEE označení	Kmitočet	Dosah	Max. rychlost	Spotřeba energie	Vznik IEEE normy
Bluetooth	802.15.1	2,4 GHz	10 m	1 Mbit/s	nízká	2002
UWB	802.15.3a	3,1 – 10,6 GHz	10 m	100 – 500 Mbit/s	nízká	2007+
ZigBee	802.15.4	2,4 GHz, 868/915 MHz	20 m	20/40/250 kbit/s	nízká	2003

Tab. 1 - Přehled WPAN technologií

V tab. 1 jsem stručně a přehledně zobrazil detaily WPAN technologií. Tyto technologie jsou technologie poměrně krátkého dosahu, nicméně i v ITS lze pro ně nalézt využití. Například v servisech lze snadno z vozidla přes Bluetooth načíst stav tachometru a další údaje o vozidle. Stejně tak je možné například i pro zvýšení pohodlí a komfortu nabídnout integrované bluetooth do systému vozidla, které spojí vaše přenosné mobilní zařízení a audio systém ve vozidle a nabídne tak pohodlné hlasové ovládání funkcí vašeho mobilního zařízení. Určitě by se dalo pokračovat a našlo by se jistě mnoho dalších aplikací v oblasti ITS. Vždy by se ale jednalo pouze o aplikace možné provozovat „off-line“, tedy aniž by se vozidlo pohybovalo, a z malé vzdálenosti. Technologie z oblasti WPAN jsou tedy vhodné pro specifické ITS aplikace, kde je zbytečné, ba dokonce i na škodu, používat technologie s větším dosahem.

2.3. Bezdrátové lokální sítě (WLAN)

WLAN zastupuje především technologie WiFi, tj. standardy patřící do skupiny IEEE 802.11. Na technologie patřící do těchto sítí se v této práci zaměřím nejvíce, konkrétně na připravující se standard IEEE 802.11e, o kterém pohovořím v rámci kapitoly 4. Základní přenosové systémy standardu IEEE 802.11 se pokusím přiblížit v základních rysech, jejich kompletní popis by přesáhl rozsah této práce a není jejím cílem. Jednotlivé údaje o pracovních frekvencích a kanálech se týkají využití v Evropě, konkrétně v ČR.

V jiných zemích a kontinentech jsou frekvence často odlišné. Protože základ jednotlivých standardů z rodiny 802.11 je stejný, rád bych nejprve popsal společné parametry [23].

Dosah WiFi sítí

Dosah udávaný výrobci se pohybuje kolem 100 m, nicméně s použitím směrových ziskových antén lze dosah velmi zvýšit. Je třeba dbát na to, aby nebyl překročen povolený vyzářený výkon. Pokud v prostředí není rušení (vícecestné šíření signálu, rušení signálu jinými systémy ve stejném pásmu, nepřímá viditelnost, špatné počasí), lze docílit dosahu až několik kilometrů.

Konfigurace WiFi sítí

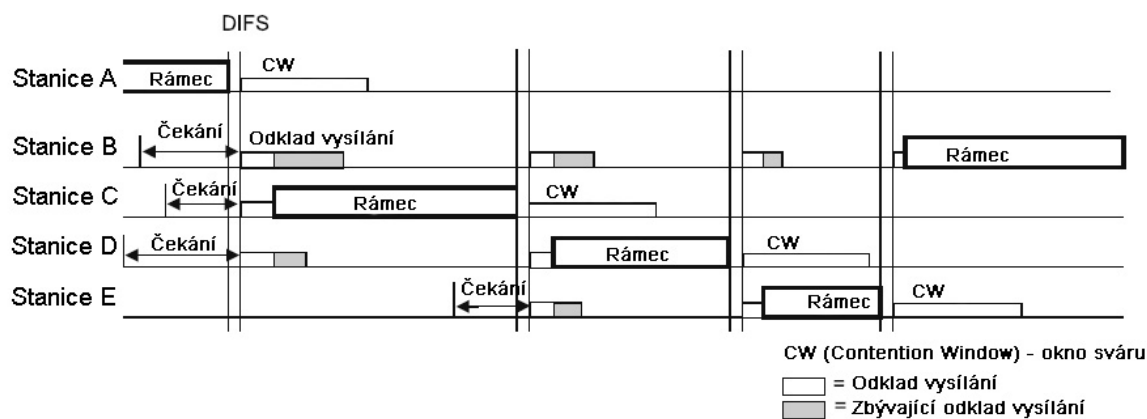
WiFi sítě mají v podstatě dvě základní možnosti konfigurace či topologie sítě. V prvním případě jsou sítě spojeny **ad-hoc** neboli **p2p** (peer-to-peer). Zde jsou zařízení spojena přímými spoji a komunikují každý s každým. Většinou se takto spojují dvě zařízení, ale je možné jich takto spojit i více. Druhou možností jsou sítě **infrastrukturní**. Zde jedno zařízení představuje vysílač (AP, Access Point – přístupový bod) a ostatní zařízení jsou jako klienti připojeny na tento vysílač. Tato konfigurace se využívá při větším počtu připojených zařízení. Vysílač je připojen na distribuční systém často pevným připojením, většinou Ethernetem.

Media Access Control (MAC) podvrstva linkové vrstvy WiFi sítí

Standard 802.11 definuje dvě přístupové metody k médiu – **DCF** (Distributed Coordination Function – Funkce rozložené koordinace) a **PCF** (Point Coordination Function – Funkce bodové koordinace).

Základ tvoří metoda **DCF**, která je založena na CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance – mnohonásobné metodě přístupu s nasloucháním nosné a zabráněním kolizí) a volitelně na RTS/CTS (Request To Send / Clear To Send). Klient naslouchá sdílené médium, zda nevysílá nějaký jiný klient, pokud je volno, začne vysílat a tím se vyhne kolizím. To ovšem vyžaduje, aby měli všichni klienti informace o všech ostatních klientech, aby na sebe „viděli“, což u většiny venkovních bezdrátových sítí nelze. Proto se používá RTS/CTS metoda, kde je každé vysílání zahájeno žádostí (RTS),

to je potvrzeno ze strany centrálního bodu (CTS) a tím je zabráněno ostatním ve vysílání. Vše je pak potvrzeno potvrzovacím paketem ACK. Takto se minimalizuje ztrátovost paketů, ovšem za cenu zvýšené režie provozu. Pro ochranu před kolizemi používá DCF dále dvě techniky. Vkládání mezery mezi vysílanými rámci (IFS, InterFrame Space) a odklad vysílání (backoff). Interval DIFS (DCF IFS) odpovídá době povinného čekání po zjištění volného vysílacího kanálu, než může stanice sama začít vysílat. Pokud v této době začne vysílat jiná stanice, musí se vysílání odložit. Interval odkladu si každá stanice generuje sama z intervalu mezi nulou a velikostí tzv. okna sváru (CW, Content Window). Velikost okna sváru se při každé kolizi zdvojnásobuje (exponential backoff). Jakmile interval odkladu vyprchá a médium je volné, může stanice začít vysílat. Příjemce po obdržení paketu čeká po dobu SIFS (Short IFS), a pak vyšle potvrzení přijetí paketu. Mechanismus je naznačen na obr. 5.



zdroj: www.ieee802.org

Obr. 5 - Režim DCF ve WLAN

Jeden z problémů, kromě kolizí a absence QoS, je stav, kdy jeden klient „vyhraje“ přístup k médiu. Nemusí jej opustit, jak jen dlouho chce. Pokud má nízkou rychlost připojení (1 Mbit/s), bude mu trvat podstatně déle, než svůj paket odešle. Tím se zpomaluje celá komunikace a celý přenos dat od všech klientů.

Druhou metodu **PCF** lze použít pouze v infrastrukturní konfiguraci sítě. Tato funkce je volitelná a je velmi zřídka implementována. Přístupové body posílají tzv. „beacon“ rámce v pevně stanovených intervalech (obvykle 0,1 s), které specifikují parametry PCF. Dobu mezi těmito rámci PCF dělí na dva časové úseky. V jednom se používá DCF metoda, tento bývá označován jako CP (Contention Period), a ve druhém přístupový bod posílá

klientům signál, který klient má právo dále vysílat. Tento úsek je označován jako CFP (Contention Free Period). Ostatní klienti mají zakázáno snažit se o vysílání. Toto je vhodné pro real-time aplikace, bohužel PCF není dostatečně podporován a má značné limitace (například zde není jakákoliv možnost volby priorit provozu) [13], [23].

2.3.1. WiFi 5 – 802.11a

Standard označovaný jako 802.11a, schválený v roce 1999, pracuje v bezlicenčním pásmu 5 GHz, jehož bezlicenční využití bylo ČTÚ schváleno od 1.9.2005 [16]. Jedná se o pásmo 5,470 – 5,725 GHz, kde je k dispozici 11 nepřekrývajících se kanálů s odstupem 20 MHz. Vyzářený výkon je omezen na 1 W střední e.i.r.p. (equivalent isotropically radiated power – střední ekvivalentní izotropicky vyzářený výkon je výkon po dobu vysílání, který odpovídá nejvyššímu výkonu, pokud je použita regulace výkonu) pokud zařízení umožňuje automatickou regulaci výkonu nejméně o 3dB, jinak je výkon omezen na 500 mW e.i.r.p. Teoretická rychlost je 54 Mbit/s, skutečná rychlost pak závisí na mnoha parametrech konkrétní radiové trasy, průměrně se pohybuje mezi 30–36 Mbit/s. Norma podporuje rychlosti 54, 48, 36, 24, 18, 12, 9 a 6 Mbit/s a v případě zhoršující se kvality spoje se rychlost patřičně snižuje, případně naopak při lepších podmínkách se při zvyšující se kvalitě spoje rychlost zvyšuje.

Pro dosažení těchto rychlostí se používá ortogonální multiplex s kmitočtovým dělením (OFDM, Orthogonal Frequency Division Multiplexing). Přesně vzato OFDM není modulace, jedná se o metodu používanou pro generování a modulaci signálu na více nosných současně. Jedná se o multiplex pracující s rozprostřeným spektrem (spread spectrum), kde je signál vysílán na více nezávislých frekvencích, což zvyšuje odolnost vůči interferenci. Jednotlivé subkanály se přitom vzájemně překrývají, čímž se dosáhne mnohem efektivnějšího využití frekvenčního pásma. OFDM je rychlý multiplex, ovšem na druhou stranu jej není možné použít na větší vzdálenosti a v členitém terénu, kde vykazuje horší výsledky než DSSS, které je použito u IEEE 802.11b. Jako skutečnou modulaci lze použít jakýkoliv typ modulace včetně BPSK, QPSK, 16-QAM či 64-QAM [23],[25],[35]

2.3.2. WiFi – 802.11b

Tento standard patří mezi základní nejrozšířenější standardy z rodiny IEEE 802.11. WiFi 802.11b pracuje v bezlicenčním pásmu 2,4 GHz. Toto pásmo bylo ČTÚ schváleno k bezlicenčnímu využití v roce 2000. K dispozici je 13 kanálů, a to od 2,412 GHz do 2,472 GHz s odstupem 5 MHz. Bohužel jeden kanál má šířku ideálně 20 MHz (až 24 MHz), z čehož můžeme usoudit, že jednotlivé kanály se překrývají. V praxi existují tedy pouze tři kanály, které se nepřekrývají. Vyzářený výkon je omezen na 100 mW e.i.r.p.

Norma 802.11b dosahuje rychlosti až 11 Mbit/s pomocí tzv. doplňkového klíčového kódování (CCK, Complementary Code Keying) v rámci DSSS (DSSS, Direct Sequence Spread Spectrum – přímá posloupnost rozprostřeného spektra) modulace na fyzické vrstvě. DSSS je modulace používající matematické kódování. Signál je rozprostřen do širšího spektra, tím je zavedena redundance, která vede ke zvýšení spolehlivosti přenosu dat. Při zhoršení parametrů rychlost klesá z 11 Mbit/s na 5,5, 2 případně až na 1 Mbit/s. Poměrně značnou část teoretické kapacity tvoří rezie – 30 až 40 %, takže průměrná skutečná rychlost se pak pohybuje kolem 5 – 6 Mbit/s [26], [28].

2.3.3. WiFi – 802.11g

V roce 2003 byla přijata norma pod označením IEEE 802.11g. Hlavní důvod pro vznik této normy byla nedostatečná rychlost normy IEEE 802.11b. WiFi 802.11g pracuje ve stejném pásmu se stejnými kanály jako 802.11b a je s ní zpětně kompatibilní.

Maximální rychlost dle standardu je 54 Mbit/s. Aby bylo možné dosáhnout vyšší rychlosti a zároveň kompatibility, používá norma 802.11g DSSS modulaci pro komptabilitu a OFDM pro dosažení vysoké rychlosti. V podstatě spojuje metody ze standardů 802.11a a 802.11b. Podporované rychlosti jsou v závislosti na modulaci. Dostupné podporované rychlosti pomocí OFDM jsou následující: 54, 48, 36 a 24 Mbit/s s pomocí 16-QAM, 18 a 12 Mbit/s s pomocí QPSK, 9 a 6 Mbit/s s pomocí BPSK. Další rychlosti jsou v souladu s 802.11b a používají DSSS: 11, 5,5 , 2 a 1 Mbit/s.

Skutečná rychlost opět závisí na parametrech radiové trasy a pohybuje se do 30 Mbit/s. Zde navíc záleží i na tom, zda do sítě nejsou připojeni i klienti s pomocí standardu

802.11b, jelikož se tím snižuje výkonnost systému a tím i podstatně přenosová rychlost. Systém je nucen přejít na systém požadavků o vysílání, aby se předešlo kolizím na fyzické vrstvě, tím se podstatně zvyšuje režie [14].

2.3.4. WiFi – využití pro ITS

	IEEE označení	Kmitočet	Dosah	Max. rychlost	Skut. rychlost	Vznik IEEE normy
WiFi 5	802.11a	5 GHz	do 8000 m	54 Mbit/s	do 36 Mbit/s	1999
WiFi	802.11b	2,4 GHz	do 8000 m	11 Mbit/s	do 6 Mbit/s	1999
WiFi	802.11g	2,4 GHz	do 8000 m	54 Mbit/s	do 30 Mbit/s	2003

Tab. 2 - Přehled WLAN technologií

Tímto jsem představil základní standardy z rodiny IEEE 802.11 používající se pro přenos dat. Jejich využití v ITS má velký potenciál, který je ovšem snižován faktem, že provoz se odehrává s bezlicenčním pásmu, kde může nastat rušení a dojít tím tak ke ztrátě informace. Bez dalších doplňků, jako jsou například standardy 802.11e a 802.11i není možné použít tyto technologie pro profesionální aplikace.

2.4. Bezdrátové metropolitní sítě (WMAN)

2.4.1. WiMAX – 802.16

Pracovní skupina IEEE 802.16, zabývající se metropolitními bezdrátovými systémy, byla založená v roce 1999. Postupně pracuje na vývoji jednotlivých standardů rodiny IEEE 802.16. Nebudu popisovat historii vývoje standardů a přejdu ke stručnému popisu dvou pro nás důležitých standardů.

2.4.1.1. 802.16d

Standard 802.16d je poslední dostupný standard z rodiny 802.16. Je již implementován do mnoha zařízení. Je navržen tak, aby vyhověl požadavkům na spolehlivost a dostupnost sítě v 99,999 % [3].

Pracuje v pásmu 2 – 11 GHz a nabízí přenosovou rychlost až 70 Mbit/s. V současné době je u nás možnost zprovoznění této sítě v pásmu 3,5 GHz. Využívá modulace typu OFDM a dokáže pracovat v režimu NLOS (Non Line Of Sight), tedy že nevyžaduje přímou viditelnost mezi základnovou stanicí a klientem. Dosah sítě je do 50 km v otevřeném terénu a do 10 km v zástavbě. [18]

Standard umožňuje využívat jak frekvenční (FDD, Frequency Division Duplex) tak časové dělení kanálů (TDD, Time Division Duplex). Pro OFDM specifikuje tři možnosti:

- OFDM s jedním kanálem
- OFDM s 256 kanály
- OFDMA s 2048 kanály (OFDMA, Orthogonal Frequency Division Multiple Access)

Specifikace zahrnuje řízení radiového spoje (RLC, Radio Link Control) pro nastavování parametrů při změnách podmínek okolí. Na rozdíl od WiFi kde je použit náhodný přístup k médiu (CSMA/CA) a dochází ke kolizím, je zde použit systém časového multiplexu (TDM / TDMA, Time Division Multiplex / Time Division Multiple Access), který plánuje využívání pásma s ohledem na priority jednotlivých přenášených dat. Řízení kvality služeb je (QoS) velmi propracované a nabízí mnoho úrovní pro bezproblémové nasazení náročných aplikací [14], [18], [37].

2.4.1.2. 802.16e

Standard IEEE 802.16e, označován jako „mobilní WiMax“, vychází ze standardu IEEE 802.16d a v současné době je ve fázi implementace. První zařízení podporující tuto normu se očekávají koncem tohoto roku (2007). Pracuje v pásmu 2 – 6 GHz a nabízí přenosovou rychlost přibližně 3 – 5 Mbit/s, maximálně 15 Mbit/s. Mobilita je garantována

až do rychlosti 120 km/h. Při rychlostech nad 60 km/h dochází k postupnému snižování kapacity z důvodů bezproblémového předávání spojení mezi základnovými stanicemi.

Standard IEEE 802.16e využívá novější typ OFDMA modulace, a to škálovatelné OFDMA (S-OFDMA, Scalable Orthogonal Frequency Division Multiple Access). S-OFDMA má lepší přenosové parametry, subnosné frekvence volí dle okolního prostředí, a tak funguje velmi dobře i při nepřímé viditelnosti, kolem budov, v prostředí s rušením apod. [14],[18].

2.4.2. MBWA – 802.20

Standard IEEE 802.20 je sice stále ve vývoji, přesto se o něm krátce zmíním. Standard má umožnit mobilním uživatelům pohybujícím se rychlostí až 250 km/h připojení s maximální kapacitou nejméně 1 Mbit/s download a minimálně 300 kbit/s upload. Buňka má mít průměr kolem 15 km a má v ní být agregována rychlost 4 Mbit/s / 800 kbit/s. Standard bude pracovat v licenčních kmitočtových pásmech pod 3,5 GHz [14].

2.4.3. WMAN – využití pro ITS

Ve skupině WMAN jednoznačně dominuje standard 802.16 – WiMax. Pro profesionální ITS aplikace je tento velmi vhodný, jelikož pracuje v licencovaných pásmech, kde by nemělo docházet k okolnímu rušení, navíc má tento standard velmi vhodné přenosové parametry zaručující kvalitu služeb. Umožňuje stanovit kvalitu služeb a poskytuje tak potřebné garance pro provoz služeb. S očekáváním se čeká na mobilní verzi WiMaxu 802.16e, která má nabídnout plnou podporu mobilních uživatelů.

2.5. Bezdrátové rozlehlé sítě (WWAN)

Zástupcem rozlehlých bezdrátových sítí jsou bezesporu sítě mobilních operátorů založené na standardu GSM. Pro přenos dat lze v těchto mobilních sítích využít poměrně mnoho systémů a služeb. Pokusím se stručně představit většinu z nich.

2.5.1. DTMF (Dual Tone Multiple Frequency)

Mezi základní schopnosti mobilních sítí patří sestavení hlasového spojení. DTMF – tónová volba nabízí přenos dat po takto sestaveném hlasovém spojení, jedná se o přenos na principu přepojování okruhů. Jednotlivé DTMF tóny se skládají ze dvou amplitudově složených sinusových signálů. V hlasovém kanále je možno přenášet vždy pouze jeden tón, doba přenosu tónu je minimálně 50ms a po každém tónu musí následovat minimálně 50 ms „ticha“. Z tohoto nám vyjde přenosová rychlost 5 byte/s. Generování tónů je snadné, detekce tónů je složitější. DTMF se dnes masově používá pro telefonní volbu a v radiotechnice [27].

2.5.2. CSD (Circuit Switched Data)

CSD nebo-li přepojování okruhů je technologie přenosu dat realizovaná po hlasovém kanálu. Kapacita jednoho hlasového kanálu je 33,8 kbit/s, ovšem od toho je nutné odečíst režii (zajištění funkčnosti sítě, zajištění spolehlivosti). Zbývající kapacita pro čistý datový tok je 9,6 kbit/s. Data není nutno kódovat tak důkladně jako hlas, takže po odstranění dodatečného kódování se lze dostat na rychlost 14,4 kbit/s [24], [27].

2.5.3. HSCSD (High Speed Circuit Switched Data)

HSCSD nebo-li vysokorychlostní přepínání okruhů je v podstatě stejný systém jako CSD, pouze zde dochází ke sdružování více kanálů (okruhů), čímž je docílena vyšší rychlost. Typicky jsou spojovány 4 kanály s možností spojení buď symetricky (2 kanály pro download, 2 kanály pro upload) nebo asymetricky (3 kanály pro download a 1 kanál pro upload). Nejčastěji se používá asymetrická možnost, kde se pak rychlostně jedná o 43,2 kbit/s download / 14,4 kbit/s upload. Existují i další možnosti jak spojovat kanály, teoreticky lze docílit až rychlosti 115,2 kbit/s oběma směry současně [24].

2.5.4. SMS (Short Message Service)

Jedná se o službu poskytovanou v sítích GSM. SMS nebo-li krátké textové zprávy lze také využít pro přenos dat. Přenos využívá kontrolní (signalizační) kanály, nikoliv hovorové. Nabízí nám délku 160 znaků. Při přenosu se může vyskytnout problém, že příjemce není schopen vyzvednout zprávu. V tomto případě se zprávy skladují v SMS centru a doručí se při první další příležitosti. Často při přenosu vznikají velké časové prodlevy. K dispozici je navíc možnost získat automaticky notifikaci o doručení zpráv.

2.5.5. GPRS (General Packet Radio Service)

GPRS je paketově orientovaný přenos dat v síti GSM. Opět pro zvýšení rychlosti sdružuje jednotlivé hlasové kanály, je možno jedinému uživateli rezervovat všech osm kanálů jednoho TDMA rámce. Rychlost závisí na schématu kódování, které se volí samo ze čtyř dostupných možností podle síly signálu GSM a vzdálenosti od vysílače. Rychlost dále závisí na počtu využitých kanálů. Pro IP komunikaci je tedy k dispozici maximální rychlost pod 160 kbit/s, skutečná rychlost se pak pohybuje mezi 22 – 40 kbit/s. Standardně se při přenosu využívá 5 kanálů, většinou v konfiguraci 4+1 (4 pro download a 1 pro upload). Přenos má poměrně velké zpoždění, pohybující se kolem 500 ms [23], [27]

2.5.6. EDGE (Enhanced Data Rates for GSM Evolution)

EDGE je v podstatě totéž co GPRS. Hlavní rozdíl je v použité modulaci. U EDGE je použita modulace 8-PSK, která dokáže přenést tři informační bity pomocí jednoho symbolu na rádiové vrstvě, na rozdíl od GPRS, kde je použita modulace GMSK, která dokáže přenést pouze jeden informační bit na jeden informační symbol. Tím lze dosáhnout při ideálních podmínkách a použití všech osmi kanálů maximální rychlosti 473,6 kbit/s. Při použití kanálů 4+1 a nejvyššího schématu kódování MCS-9 lze dosáhnout rychlosti až 236,8 kbit/s. Skutečná rychlost pak dosahuje rychlostí kolem 200 kbit/s pro download a 100 kbit/s pro upload, při konfiguraci kanálů 3+2. Aby bylo možné využít technologii

EDGE, je třeba, aby byla implementována jak v telekomunikačním zařízení, tak ve vysílací základnové stanici [23], [30], [31], [32].

2.5.7. CDMA 2000 (Code Division Multiple Access)

Technologie CDMA 2000 využívá metodu CDMA, která využívá relativně široké kanály (CDMA 2000 konkrétně 1,25 MHz). Užitečný signál je v tomto případě kódován unikátním kódem, který rozprostře signál po celé šíři spektra přenosového kanálu. Díky tomu je možné, že na jednom kanále v jednom okamžiku komunikuje více uživatelů najednou.

Technologie CDMA 2000 zahrnuje standardy CDMA 2000 1xRTT (1 x Radio Transmission Technology), CDMA 2000 1xEV-DO (1 x Evolution Data Optimized) a CDMA 2000 1xEV-DV (1 x Evolution Data/Voice).

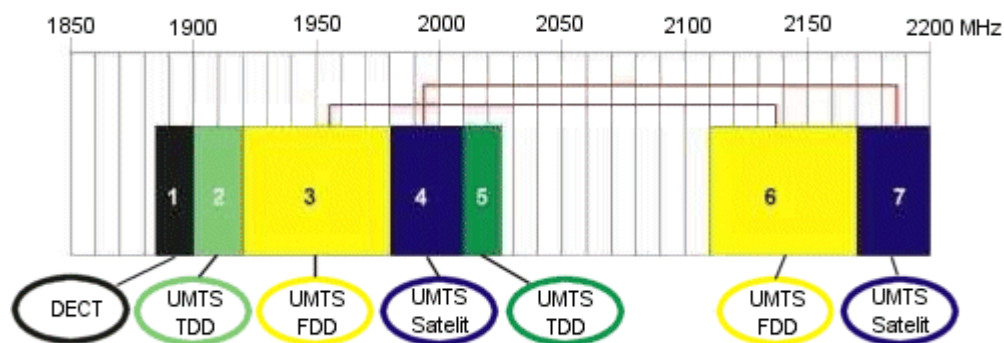
Stručně popsáno, standard RTT je starší a nabízí dvojnásobnou kapacitu pro přenos hlasu a pro data nabízí maximální rychlost 614 kbit/s. Standard EV-DO je orientován čistě na datové přenosy, hovor na této technologii lze uskutečnit nanejvýše pomocí VoIP. Teoretické přenosové maximum je 2,4 Mbit/s při modulaci 16-QAM a ideálních podmínkách. Skutečná přenosová rychlost se pak pohybuje mezi 500 – 700 kbit/s se zpožděním okolo 200 ms. Třetí standard EV-DV nabízí maximální rychlost 3,1 Mbit/s pro download a 1,8 Mbit/s pro upload. Zároveň podporuje současné využívání jak hlasových tak datových služeb.

K dispozici je i modifikace CDMA 450, která je založena na CDMA EV-DO a umožňuje využití této technologie na pásmu 450 MHz, na kterém u nás provozuje Telefonica O2 síť T!P [14], [23], [33], [34].

2.5.8. UMTS (Universal Mobile Telecommunication System)

Síť UMTS používá metodu W-CDMA (Wideband Code Division Multiple Access) s kanály o šířce 5 MHz, která používá pro přenos frekvenční duplex (FDD, Frequency Division Duplex). Toto řešení, označované jako UMTS FDD, u nás provozuje Telefonica

O2 a nabízí paketové datové přenosy a hlasové služby na bázi přepojování okruhů. Další variantou je metoda TD-CDMA (Time Division CDMA), která využívá časový duplex (TDD, Time Division Duplex). UMTS TDD u nás provozuje T-Mobile a poskytuje pouze paketové datové přenosy.



Zdroj: tomas.richtr.cz

Obr. 6 - Frekvenční spektrum UMTS

Na obr. 6 je naznačeno využití frekvenčního spektra UMTS. To se skládá z jednoho párového pásma (1920 – 1980 MHz + 2110 – 2170 MHz) a jednoho nepárového pásma (1910 – 1920 + 2010 – 2025 MHz). V roce 2000 byla přidána ještě 3 další pásma, ale v Evropě použitelné je pouze jedno z nich, a to 2500 – 2690 MHz.

UMTS existuje v několika verzích. Starší verze měli poměrně malé přenosové rychlosti, první varianta UMTS R99 (R3) v praxi dosahovala rychlostí 120 / 50 kbit/s. Dnešní UMTS je nabízené ve verzi R5, ta je velmi často označována spíše podle jedné z technologií, které tento standard obsahuje – HSDPA (High Speed Downlink Packet Access). S touto verzí je možné dosahovat rychlosti až 14,4 Mbit/s. HSDPA v současné době existuje ve 4 variantách. V rámci R5 se jedná o HSDPA Phase I ve verzích SoC I (rychlost do 1,8 Mbit/s – verze kterou u nás nabízí Telefonica O2) a SoC II (rychlost do 3,6 Mbit/s). V novější verzi R6 je pak standardizováno i HSDPA Phase II ve verzích SoC I (rychlost do 7,2 Mbit/s) a SoC II (rychlost do 14,4 Mbit/s). Verze R6 přinese snížení zpoždění přenosu z 100 – 200 ms pod hranici 50 ms a navyšuje kromě rychlostí pro download i rychlosti pro upload, a to pro SoC I na 1,8 Mbit/s a SoC II na 3,6 Mbit/s. Toto zvýšení je dosaženo úpravou radiového rozhraní a nese název HSUPA (High Speed Uplink Packet Access) [14],[31],[33],[34].

2.5.9. WWAN – využití pro ITS

Jelikož jsou přenosové rychlosti většiny služeb z této oblasti malé a odezva je poměrně vysoká, jsou tyto technologie vhodné pouze pro aplikace nenáročné na tyto parametry. Velkou výhodou těchto systémů je fakt, že jsou dostupné téměř po celém území naší republiky, a proto je použití těchto systémů jednoduchým nástrojem, jak zajistit komunikaci na co největším území. Systémy jsou vhodné například pro sledování pohyblivých vozidel v rámci velkého území. K dispozici je komunikační linka a zároveň díky buňkovému uspořádání těchto systémů je známé i přibližné umístění vozidla v prostoru.

2.6. Porovnání jednotlivých technologií

Jednotlivé technologie mají rozdílné parametry. Jak už samo říká jejich dělení, mají rozdílnou především oblast působnosti a dosahu sítě. Proto použití jednotlivých technologií závisí na konkrétním typu aplikace. Pokud specifikujeme oblast použitelnosti, můžeme se dále zabírat výběrem vhodné technologie z dané kategorie. Každá uvedená technologie je specifická a jde pouze o nalezení aplikace, pro kterou je vhodná.

3. Performační indikátory

Performační indikátory jsou v podstatě indikátory, s jejichž pomocí je možno definovat požadavky na telematické a jiné aplikace. Dají se s nimi kvantifikovat a kvalifikovat procesy a jejich parametry. Cílem je hledat parametry v telematickém a telekomunikačním subsystému a jejich vzájemné vazby. Sledované procesy musí splňovat předem danou množinu parametrů, které matematicky vyjadřují kvality analyzovaného systému. Takto se dají kvalifikovat i jednotlivé součásti systému, jako jsou bezdrátová telekomunikační síť, software systému, atd. Všechny tyto parametry tvoří množinu analyticky uchopitelných vlastností systému. Tyto parametry nám, spolu s nástroji složitých matematických analýz, umožní korektně zhodnotit použitelnost systému.

3.1. Telematické performační indikátory

Systémové parametry lze stanovit k funkci, telekomunikační vazbě, jednotlivým procesům v dopravně-telematickém systému a jednotlivým parametrům např. polohová informace. V následujících definicích je uveden obecný popis těchto telematických parametrů dle [5],[6],[7],[8].

3.1.1. Přesnost

Přesnost je definována jako stupeň shody mezi měřenou a definovanou hodnotou parametru / procesu / funkce:

$$P(|p_i - p_{m,i}| \leq \varepsilon_1) \geq \gamma_1 \quad (1)$$

tj. že rozdíl mezi požadovaným parametrem p_i a měřeným parametrem $p_{m,i}$ nepřesáhne hodnotu ε_1 na hladině pravděpodobnosti γ_1 . Uvedený vztah platí i pro vektory parametrů.

Pro ilustraci uveďme, že v případě pilotního projektu systému monitorování pohyblivých objektů po pohybové ploše letiště je požadavek daný příslušnými letištními předpisy tak, že chyba polohové informace nesmí překročit v horizontální rovině 7,5m na hladině pravděpodobnosti 99%.

3.1.2. Spolehlivost

Spolehlivost je schopnost systému plnit požadované funkce bez přerušení během daného postupu v průběhu definovaného časového intervalu:

$$P(|\vec{v}_t - \vec{v}_{m,t}| \leq \varepsilon_2) \geq \gamma_2, t \in \langle 0, T \rangle \quad (2)$$

tj. že rozdíl mezi požadovanými parametry (vektory parametrů) $\vec{v}_t$ a měřenými parametry $\vec{v}_{m,t}$ nepřesáhne hodnotu ε_2 na hladině pravděpodobnosti γ_2 v libovolném čase t časového intervalu $\langle 0, T \rangle$.

U polohové informace je spolehlivost chápána jako podíl dostupnosti lokalizační služby vzhledem k celkové době T sledování této informace. Čas sledování se typicky určuje jako jedna hodina pro hodnocení pozemních dopravních systémů na stanovené hladině pravděpodobnosti. Pokud je požadavek spolehlivosti systému 99% na hladině pravděpodobnosti 99% v čase 1 hodina, znamená to, že v 99 pokusech ze sta pokusů je 99% z 1 hodiny služba funkční, tj. služba není funkční 36 s z jedné hodiny.

3.1.3. Dostupnost

Dostupnost je schopnost systému plnit požadované funkce při inicializaci (spuštění) systému/procesu dle daného postupu:

$$P((q_{m,i} - q_i) \leq \varepsilon_3) \geq \gamma_3 \quad (3)$$

tj. rozdíl požadované hodnoty úspěšného spuštění i -té funkce/procesu q_i a naměřené hodnoty $q_{m,i}$ nepřekročí hodnotu ε_3 na hladině pravděpodobnosti γ_3 .

V případě telematických služeb na letišti je požadováno, aby po aktivaci lokační služby včetně komunikace k serveru byla služba dostupná do 30 sekund po zahájení aktivace na hladině pravděpodobnosti 99% (u GPS lokalizace je tento čas známý jako TTFF – Time To First Fix, nebo-li čas spuštění služby). Tento požadavek znamená, že provedeme-li 100 náhodných spuštění lokalizační služby, pouze v jednom případě naběhnutí lokalizační služby trvá déle než 30 s.

3.1.4. Kontinuita (spojitost)

Kontinuita je schopnost systému plnit požadované funkce/procesy bez (neplánovaného) přerušení (maximální povolená délka přerušení je předem definována) během daného postupu (nebo definovaného časového intervalu):

$$P(|r_t - r_{m,t}| \leq \varepsilon_4) \geq \gamma_4, t \in \langle 0, T \rangle \quad (4)$$

tj. rozdíl mezi požadovaným maximálním přerušením r_t a měřenou hodnotou $r_{m,t}$ nepřesáhne v každém čase t v intervalu $\langle 0, T \rangle$ hodnotu ε_4 na hladině pravděpodobnosti γ_4 . Kontinuita má blízko ke spolehlivosti, ale hlavním rozdílem je sledování délky výpadku. Jde tedy o možnost kvantifikace rozložení výpadků – u spolehlivosti můžeme zaznamenat jeden dlouhý výpadek a nebo mnoho krátkodobých výpadků. Právě kontinuita dokáže mezi těmito dvěma případy rozlišit a definovat, jaká maximální délka výpadku je povolena.

Na letišti je požadavek maximální délky výpadku lokalizační služby 5 sekund na hladině pravděpodobnosti 99% v časovém intervalu 3 minuty. Znamená to, že v intervalu 3 minuty jsou možné výpadky pouze s maximální délkou 5 sekund. Provedeme-li 100 měření, pouze v jednom případě se stane, že v 3 minutovém intervalu nalezneme výpadek delší než 5 sekund. Kontinuita má velký vztah ke kritickým aplikacím pracujícím v reálném čase.

3.1.5. Integrita

Integrita je schopnost systému včasné a bezchybně informovat uživatele, že systém nemůže být použit pro operace daného postupu

$$P(|s_i - s_{m,i}| \leq \varepsilon_5) \geq \gamma_5 \quad (5)$$

tj. rozdíl mezi požadovanou dobou nahlášení poruchy s_i , tj. např. zpráva o překročení daného limitu (AL – Alert Limit) a naměřenou hodnotou doby hlášení poruchy $s_{m,i}$ nepřekročí hodnotu ε_5 na hladině pravděpodobnosti γ_5 .

Integrita vyjadřuje schopnost systému včas diagnostikovat překročení předdefinovaných parametrů a za požadovaný časový interval o této skutečnosti informovat uživatele/obsluhu.

V případě lokalizačních funkcí je požadavek, že pokud přesnost určení polohy překročí hranici 10 metrů, uživatel musí být o této změně přesnosti informován do 5 sekund na hladině pravděpodobnosti 99%.

3.1.6. Bezpečnost

Bezpečnost je schopnost systému, že v případě vzniku poruchy nedojde k poškození systému nebo k materiálním ztrátám či ztrátám na lidském životě. Kvantifikace vychází z provedené analýzy a klasifikace rizik:

$$P(|W_i - W_{m,i}| \leq \varepsilon_6) \geq \gamma_6 \quad (6)$$

tj. rozdíl mezi požadovanou rizikovou situací W_i a skutečnou rizikovou situací $W_{m,i}$ nepřekročí hodnotu ε_6 na hladině pravděpodobnosti γ_6 .

Bezpečnost, jako systémový parametr, rozděluje chyby/poruchy, které se vyvíjí bezpečným směrem, pak jde o výpadky, které jsou charakterizovány spolehlivostí, kontinuitou, integritou, atd. a chyby/poruchy, které se vyvíjí nebezpečným směrem. Zjištění bezpečných a nebezpečných stavů systému je součástí klasifikace a analýz rizik.

Nebezpečným stavem je např. situace, kdy jsou třetí stranou vysílány falešné GNSS signály. Pokud existuje možnost, že zdroj signálu není přijímacím lokalizačním systémem identifikován jako neautorizovaný, pak tento případ může skončit i fatální nehodou. Chceme-li zvýšit bezpečnost této typicky kritické aplikace, je nutno využít dostatečně zabezpečených signálů, tj. např. vyšší kategorie služeb nového systému Galileo, kdy signály již nebudou volně aplikovatelné, ale distribuované za zvláštních bezpečnostních podmínek. Tímto přístupem vzroste významným způsobem bezpečnost služby založená na takto zabezpečených GNSS službách, protože pravděpodobnost vyrobit a vysílat falešné signály tak, aby byly zaměnitelné za signály originálních zdrojů, bude podstatně méně pravděpodobné. Je možné pouze systém rušit šumem, ale to je identifikovatelný stav jednotkou ve vozidle s diagnostickou reakcí. Další možností zajištění odpovídající bezpečnosti je využít paralelních zdrojů polohových informací,

např. majáky na dopravní infrastruktuře, inerciální systém ve vozidle a jejich kombinace a porovnání s cílem zachytit nebezpečné stavy systému.

3.2. Telekomunikační performační indikátory

Telekomunikační performační indikátory v podstatě zastupují systémové parametry přenosových systémů. V následujících definicích je uveden obecný popis těchto telekomunikačních performačních indikátorů dle [5],[6],[7],[8].

3.2.1. Aktivační doba dostupnosti služby

Aktivační doba dostupnosti služby je definovaná jako čas potřebný pro aktivaci systému z nefunkčního stavu (např. vypnutý přístroj) do jeho plně funkčního stavu.

$$P(|a_i - a_{m,i}| \leq \varepsilon_1) \geq \gamma_1 \quad (7)$$

tj., rozdíl požadovaného času úspěšného i -té aktivace systému a_i a naměřeného aktivačního času $a_{m,i}$ nepřekročí hodnotu ε_1 na hladině pravděpodobnosti γ_1 .

3.2.2. Dostupnost služby (např. virtuálního okruhu)

Dostupnost služby je schopnost okruhu plnit požadované funkce bez přerušení během daného postupu v průběhu definovaného časového intervalu:

$$P(|ca_t - ca_{m,t}| \leq \varepsilon_2) \geq \gamma_2, t \in \langle 0, T \rangle \quad (8)$$

tj. že rozdíl mezi požadovanými parametry ca_t a měřenými (skutečnými) parametry $ca_{m,t}$ nepřesáhne hodnotu ε_2 na hladině pravděpodobnosti γ_2 v každém čase t v intervalu $\langle 0, T \rangle$.

Dostupnost virtuálního okruhu je chápána jako podíl dostupnosti okruhu v daném čase sledování. V telekomunikacích se obvykle uvádí hodnotami dostupnosti služby v období 1 roku. Např. roční dostupnost 99,95% reprezentuje nedostupnost okruhu cca. 4 hodiny

v průběhu jednoho roku s tím, že v 99 pokusech ze 100 pokusů je v 99 případech dostupnost splněna. S ohledem na paritní definici spolehlivosti telematických služeb je takto stanovená hodnota nesouměřitelná a je nutno ji kombinovat s veličinami MTBF a MTTR, jejichž definice následuje.

3.2.3. Doba mezi dvěma poruchami – MTBF

MTBF – Mean Time Between Failure, nebo-li střední doba bezporuchového provozu, je definována jako čas mezi dvěma neočekávanými poruchami na jisté pravděpodobnostní úrovni.

$$P(|f_i - f_{m,i}| \leq \varepsilon_3) \geq \gamma_3 \quad (9)$$

tj. i -tý rozdíl vzorku požadované doby mezi dvěma poruchami f_i a skutečné hodnoty tohoto parametru $f_{m,i}$, který je menší než ε_3 na hladině pravděpodobnosti γ_3 .

Pokud je interval MTBF na dané hladině pravděpodobnosti řádově větší než interval $\langle 0, T \rangle$ definice (2), lze tento parametr, tj. dobu mezi dvěma poruchami, považovat na dané hladině pravděpodobnosti za nevýznamný. Tento stav ale není dosažitelný zejména u mobilních komunikačních systémů aplikovaných v členitém terénu, kde je nutné vzít v úvahu, že nosná telekomunikační služba nebude všude dostupná, a proto je nutné řešit doplňkové pokrytí prostor další technologií. Je proto nezbytné v komplikovanějších aplikacích co nejpřesněji specifikovat území s různou úrovní (rozptylem) požadavků na performační parametry.

3.2.4. Doba obnovení služby – MTTR

MTTR – Mean Time To Recover, nebo-li doba obnovení služby, je definována jako čas potřebný k obnovení služby z neočekávané poruchy na jisté pravděpodobnostní úrovni.

$$P(|rc_i - rc_{m,i}| \leq \varepsilon_4) \geq \gamma_4 \quad (10)$$

tj. rozdíl požadované rc_i a skutečné hodnoty $rc_{m,i}$ i-tého obnovení funkcionality po poruše sítě je menší než ε_4 na hladině pravděpodobnosti γ_4 .

Tato hodnota je samozřejmě vázaná na redundantní síťová telekomunikačních řešení s automatickou obnovou. Tato veličina je interpretovatelná jako (dominantní) součást parametru kontinuita (4), tj. maximální doba výpadku služby v daném intervalu na dané hladině pravděpodobnosti. S ohledem na možnost způsobení výpadku třetí stranou (poškození kabelu, úder blesku apod.) považujeme za vhodné s touto hodnotou vždy počítat – tedy alespoň při stanovování kritických časových prodlev způsobených kumulací zpoždění signálu komunikačním zařízením. Je ale třeba poznamenat, že tyto hodnoty se liší i o několik řádů podle použitého síťového řešení (např. IP VPN/L2 vs. MPLS/L3).

3.2.5. Zpoždění

Zpoždění (latence) je definováno jako časová prodleva doručení rámce/paketu mezi zdrojem a cílem komunikace během určité definované doby na jisté pravděpodobnostní úrovni.

$$P(|d_t - d_{t,m}| \leq \varepsilon_5) \geq \gamma_5, t \in \langle 0, T \rangle \quad (11)$$

tj. rozdíl požadované hodnoty zpoždění d_t a měřené hodnoty zpoždění $d_{t,m}$ nepřesáhne hodnotu ε_5 na hladině pravděpodobnosti γ_5 .

Zpoždění má akumulární charakter a je mj. ovlivněno:

- přenosovou rychlostí rozhraní
- velikostí paketu/rámce/buňky
- zatížením každého z uzlů, kterými spojení prochází

Zatímco přenosová rychlost rozhraní a velikost paketu jsou veličiny statické (za předpokladu konstantní délky paketu/rámce), je zatížení uzlu veličinou pravděpodobnostní svou příslušností patřící do kategorie „měkkých“ systémů. Důvodem je skutečnost, že existují nástroje řízení sítě, které mohou snížit pravděpodobnost vlivu zatížení uzlů sítě zejména u nejvyšší třídy služby na hodnotu blízkou nule. Pokud není přetížení sítě způsobené třetí stranou, tj. jev z kategorie bezpečnosti sítě, je v možnostech

správce sítě (je-li k tomu vůle z ekonomických důvodů využití sítě) udržet stupeň vytížení uzlů pod kritickou hodnotou především korektní konfigurací sítě, tj. jejích jednotlivých uzlů a příslušných rozhraní.

V kompetenci řešitele telematického systému je volba spolehlivého poskytovatele služby a příslušné třídy služby, která mj. i obsahuje toleranční pásmo zpoždění přeneseného paketu každým uzlem a kumulativně celou sítí.

3.2.6. Ztráta paketů

Ztráta paketů (packet loss) je definována jako procento nedodaných paketů z celkového počtu odeslaných paketů uvnitř definované doby na jisté pravděpodobnostní úrovni.

$$P((pl_{t,d} / pl_t) \geq \varepsilon_\gamma) \geq \gamma_\gamma, t \in \langle 0, T \rangle \quad (12)$$

tj. podíl počtu dodaných paketů $pl_{t,d}$ a celkového počtu odeslaných paketů pl_t je roven anebo větší než ε_γ na hladině pravděpodobnosti γ_γ pro každý čas t z intervalu $\langle 0, T \rangle$.

Problematika ztráty paketů souvisí s korektností konfigurace sítě a volbě odpovídající třídy služby. Významnou úlohu má i relevantně navržená aplikační vrstva, případně v kombinaci s TCP anebo RTP/UDP transportními protokoly. Vysoké procento ztracených paketů ve svém důsledku vyvolává změnu průchodnosti sítě – v případě jednoduché aplikace protokolu TCP může mít lokální přetížení sítě důsledek v možnosti až patologického nárůstu zpoždění přenosu paketů. Proto jsou často užívány např. pro multimediální aplikace právě kombinace protokolů RTP/UDP, které s ohledem na typ aplikace spíše tolerují ztrátu jednotlivého paketu, než narůstající zpoždění generované měnicími se časovými podmínkami odesílání paketů protokolem TCP. Opět i zde platí důležitost volby adekvátní třídy služby, která je svými parametry relevantní dané aplikaci.

3.2.7. Bezpečnost

Bezpečnost je schopnost systému, že v případě vzniku poruchy nedojde k poškození vlastní funkcionality komunikačního systému:

$$P(|Wc_i - Wc_{m,i}| \leq \varepsilon_6) \geq \gamma_6 \quad (13)$$

tj. že rozdíl mezi i -tou požadovanou hodnotou rizikové situace Wc_i a skutečnou hodnotou rizikovou situací $Wc_{m,i}$ nepřekročí hodnotu ε_6 na hladině pravděpodobnosti γ_6 .

Nebezpečným stavem je, pokud jsou třetí stranou poškozovány přenášené informace, tj. bezpečnostním rizikem je odstranění/modifikace anebo zaslání falešné informace jiným zdrojem, než je vlastní relevantní zdroj informace. Významu identifikaci bezpečnostních rizik a tvorbě bezpečnostní politiky bude věnována samostatná kapitola.

3.3. Vztah mezi telematickými a telekomunikačními performančními indikátory

Při tvorbě komunikačních řešení pro telematické aplikace jsou kladeny nemalé požadavky na tato řešení. Je třeba docílit garantované funkčnosti systému ve všech požadovaných parametrech za cenu nejmenších nákladů. Performanční indikátory nám pomohou definovat jednotlivé parametry řešení. Z vazeb je nutno určit závislost jednotlivých indikátorů a snažit se minimalizovat jejich negativní vliv na celý řetězec.

Performanční indikátory popisující telekomunikační aplikace musí být dány do vazeb na telematické performanční indikátory a naopak. Takovéto propojení pak dovoluje systémovou analýzu. Konečný přidaný efekt vektoru telekomunikačních performančních indikátorů $\vec{tci}$ na vektoru telematických performančních indikátorů $\vec{tmi}$ může být vyjádřen rovnicí (14), nicméně pouze za podmínek, že pravděpodobnostní úrovně všech ukazatelů jsou nastaveny na stejnou hladinu a že mají stejný fyzikální rozměr (čas).

$$\Delta \vec{tmi} = TM \cdot \vec{tci} \quad (14)$$

TM představuje transformační matici. Identifikace TM představuje iterativní proces a může být provedena ve čtyřech iterativních krocích. Tento proces začíná s maticí TM_0 v základní podobě. Transformační matice TM_0 bere v úvahu všechny možné vazby mezi telematickými a telekomunikačními indikátory. Stavba matice je závislá na detailním komunikačním řešení pro daný případ a jeho integraci do telematického systému. Každý prvek matice je v několika krocích ohodnocen na základě detailní analýzy specifické

telekomunikační a telematické konfiguraci systému a má přiřazenu pravděpodobnost výskytu v kontextu celého systému. Toto se odehrává v již zmiňovaných čtyřech krocích, které vedou k cíli, kde jsou veškeré méně významné vztahy (ukazatelé) vyřazeny a naopak více významné vztahy (ukazatelé) jsou identifikovány pod podmínkou stejného tolerančního rozsahu telematických indikátorů.

Čtyři iterativní kroky vedoucí ke koncovému stupni jsou:

1. **Primární vyloučení telekomunikačních ukazatelů** založených na implementaci vhodného komunikačního řešení nebo jeho nastavení (například garantované pokrytí definované oblasti).
2. **Primární ignorování telekomunikačních ukazatelů**, pokud jejich váha může být stanovena jako bezvýznamná.
3. **Identifikace a vyloučení ukazatelů** s podstatně nižší úrovní jejich pravděpodobnosti výskytu.
4. **Poslední iterativní identifikace dominantních ukazatelů** je založena na nastavení parametrů virtuálního telekomunikačního řešení. Modifikace řešení může vést opět ke kroku č. 1.

Tento postup může být úspěšně aplikován i pro CALM identifikaci kritérií. Správné výsledky popisovaného iterativního procesu jsou získány na základě detailní znalosti konkrétního řešení a jeho korektní analýzy. Lze kvantifikovat, jaké parametry má telekomunikační řešení v dané oblasti z hlediska telematického zadání. Máme tedy nástroj, jak optimalizovat telekomunikační řešení podle telematického zadání.

4. Stav implementace standardů 802.11

4.1. Základ – 802.11a/b/g

Standardy IEEE 802.11a/b/g označovány jako WiFi jsou již několik let k dispozici, jsou velmi populární a poměrně hodně rozšířené. V současné době existuje 836 poskytovatelů bezdrátového připojení přes technologii WiFi a ti nabízejí své služby dohromady v 6297 obcích a městech. [15, 5.8.2007] Do oblíby se WiFi dostala především díky faktu, že je provozována v bezlicenčním pásmu pouze na základě veřejného oprávnění. Díky hromadné výrobě stojí zařízení pro WiFi dnes pouze zlomek ceny, za kterou bylo možné technologii sehnat před několika lety a zařízení je volně dostupné. Díky těmto faktům je WiFi velmi úspěšné a poměrně hodně rozšířené. Celosvětově je certifikováno přes 3000 produktů podporujících Wi-Fi [19].

WiFi 2,4 (802.11b/g) je v ČR od roku 2000. V té době byli pevné přípojky do internetu pomalé a poměrně drahé. WiFi měla tedy poměrně dobrou startovní pozici, které opravdu využila. Kromě komerčních subjektů se objevily i nekomerční neziskové subjekty „czfree.net“, které šíří myšlenku připojení se do sítě czfree.net, potažmo do sítě Internet, za minimální náklady pro co největší množství lidí. Technologie WiFi se tak rozšířila opravdu téměř do všech koutů republiky. Dnes díky velkému rozšíření lze tuto technologii nalézt běžně integrovanou v přenosných počítačích a dokonce i v mobilních telefonech.

Z výše uvedených je zatím nejméně rozšířena technologie označována jako WiFi 5, neboli síť založená na standardu IEEE 802.11a. Nejméně je rozšířena z důvodů, že využití pásma 5 GHz bylo k bezlicenčnímu využití schváleno ČTÚ v září roku 2005, takže oproti WiFi 2,4 má pět let zpoždění. To ovšem poměrně svižně dohání jako doplněk pro již stávající síť WiFi, kde nabízí lepší kvality připojení. Ceny zařízení jsou opět poměrně příznivé.

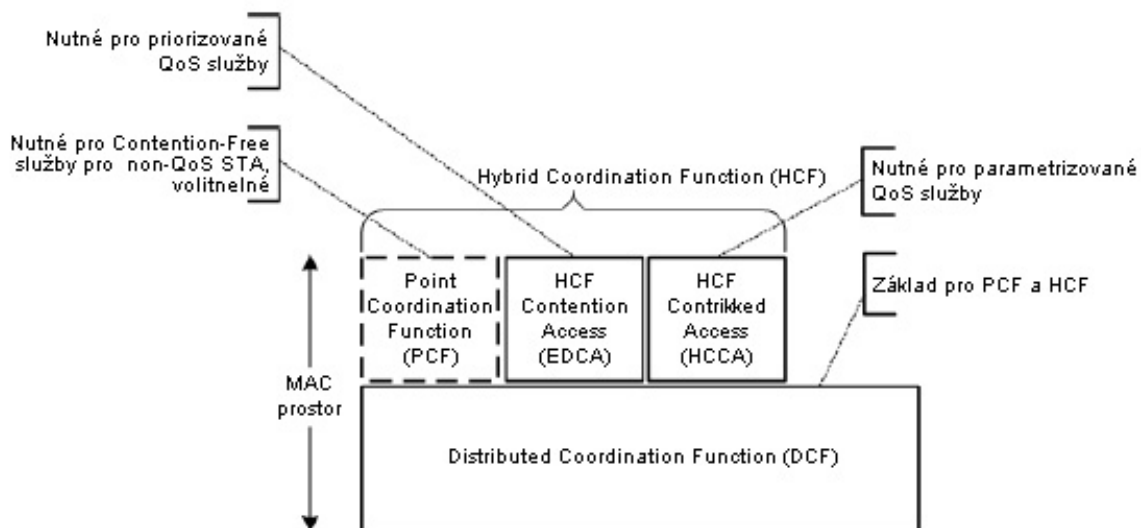
Rozšíření technologie WiFi má bohužel i negativní dopady, a to sice na profesionální použití této technologie. Na přeplněném bezlicenčním pásmu není možné garantovat kvalitu služby, a proto se tato technologie hodí pouze na některé nenáročné ITS aplikace. Například pro off-line výměnu dat vozidel při zastávkách na cestách, přenos fotografií nebo videa s malým rozlišením z kamer pro sledování dopravního provozu na komunikacích nebo podobné nenáročné aplikace [36].

4.2. Doplněk 802.11e – Wireless QoS

Standard IEEE 802.11e, dokončený v září 2005, představuje doplněk pro IEEE 802.11. Doplnjuje podporu pro kvalitu služeb (QoS – Quality of Service) a opravuje chyby v podvrstvě MAC (MAC – Media Access Control) pro podporu všech fyzických vrstev používaných v IEEE 802.11 sítích. Standard je důležitý pro aplikace citlivé na koncové zpoždění, kolísání zpoždění a šířku pásma jako je například přenos hlasu (VoIP, Voice over WLAN – VoWLAN, VoWiFi, VoFi) nebo přenos videa [20], [22], [23].

Mezi hlavní funkce patří mapování QoS, kde se sleduje provoz a určuje se, s jakou prioritou má být daná část přenesena, dále řízení přístupu k médiu, kde se stanoví, zda je možné požadavkům vyhovět, a naposled přidělování síťových prostředků, které se realizuje buď rezervací, nebo upřednostněním provozu.

IEEE 802.11e vylepšuje MAC metody DCF a PCF novou hybridní koordinační funkcí HCF (Hybrid Coordination Function). HCF má dvě metody přístupu k médiu, podobné původním metodám. Jedná se o HCCA (HCF Controlled Channel Access – přístupová metoda ke kanálům řízená HCF) a EDCA (Enhanced DCF – vylepšená DCF přístupová metoda ke kanálům). Obě definují třídy provozu (TC, Traffic Classes). Architektura MAC vrstvy standardu je zobrazena na následujícím obrázku.



zdroj: www.ieee802.org

Obr. 7 - IEEE 802.11e MAC architektura

EDCA

Při použití EDCA dochází k prioritizaci provozu a data s vyšší prioritou jsou upřednostňována před daty s nižší prioritou a čekají kratší dobu na odeslání. Každá úroveň provozu má přiřazenu přenášecí příležitost (TXOP, Transmit Opportunity), to je ohraničený časový interval, během kterého může stanice poslat tolik rámců/paketů, kolik je schopna. Pokud je rámec/paket příliš velký na to, aby byl přenesen v jednotlivé TXOP, je fragmentován do menších rámců/paketů. Tím se redukuje problém přenosu informací od stanic s nízkou rychlostí přenosu.

HCCA

Metoda HCCA pracuje velmi podobně jako PCF. Na rozdíl od PCF, kde se interval dělil pevně na dvě periody, u HCCA je možné zahájit úsek CFP kdykoliv. Tento druh CFP je označován jako CAP (Controlled Access Phase) a je iniciován přístupovým bodem, kdykoliv je potřeba přijmout nebo odeslat data okamžitě. Během úseku CP je používána metoda EDCA. Dalším rozdílem oproti původnímu PCF je přítomnost tříd provozu (TC, Traffic Class) a proudů provozu (TS, Traffic Streams). Provoz a řazení do front může tedy probíhat dle požadavků jednotlivých spojení s různými klienty. Klienti navíc poskytují informaci o délkách jejich front pro každou provozní třídu, čímž je umožněno dosažení lepších výsledků při plánování provozu.

HCCA je obecně považováno za nejpokročilejší a nejkomplexnější koordinační funkci. QoS může být nakonfigurován velmi precizně. Stanice tak mají možnost specifikovat konkrétní požadavky na přenos (rychlost, kolísání zpoždění,...), což vede k umožnění používání náročnějších aplikací, jako jsou například VoIP, video streaming atd.

IEEE 802.11e přináší ještě další vylepšení v MAC vrstvě:

APSD – Automatic Power Save Delivery (Automatická úspora energie)

APSD je účinnější metoda řízení výkonu než původní metoda v IEEE 802.11.

BA – Block Acknowledgments (Blokované potvrzování)

BA umožňuje potvrdit celý TXOP v jediném rámci, což snižuje režii protokolu zejména při delších TXOP.

NoAck – Not Acknowledged (Žádné potvrzování)

Služba pro posílání rámců v QoS může nabývat dvou hodnot: QoSAck a QoSNoAck. Rámce s QoSNoAck nejsou potvrzovány, což zamezí znovuposílání dat, které mají být s malým zpožděním.

Standard stanovuje čtyři kategorie provozu pro osm úrovní priority stejných jako v 802.1d viz tab. 3. [13]

Priorita	802.1d Priorita	802.1d Označení	802.11e Označení
nejnižší ↓ nejvyšší	1	Background	Background
	2		
	0	Best Effort	Best Effort
	3	Excellent Effort	
	4	Controlled Load	Video
	5	Video	
	6	Voice	Voice
	7	Network Control	

Tab. 3 - 802.11e/802.1d priority

zdroj: www.ieee802.org

Při základní metodě EDCA se upravují doby čekání mezi jednotlivými pokusy o vysílání. Jeden z upravovaných parametrů je AIFS (Arbitration Interframe Space). AIFS se prodlužuje se snižující se prioritou provozu. To znamená, že provoz s vysokou prioritou bude čekat méně než provoz s nízkou prioritou. Celkovou dobu čekání ještě doplňuje náhodné okno sváru (CW, Contention Window), jehož hlavním účelem je zamezit kolizím paketů stejné kategorie.

kategorie	charakteristika přenosu	AIFS	CW	celková doba čekání
hlas (7,6)	VoIP s nejvyšší kvalitou – minimální zpoždění	2	0 – 3	2 – 5
video (5,4)	video toky (běžné i vysoké rozlišení)	2	0 – 7	2 – 9
best effort (0,3)	interaktivní aplikace necitlivé na zpoždění	3	0 – 15	3 – 18
pozadí (2,1)	datové soubory	7	0 – 15	7 – 22

Tab. 4 - Doba čekání na vysílání

zdroj: www.lupa.cz

Z architektury MAC vrstvy standardu na obr. 7 lze vysledovat kompatibilitu s WiFi zařízeními, které nemají implementován tento standard. Tyto zařízení pak komunikují

bez jakékoliv možnosti stanovit priority provozu, s těmi se operuje pouze se zařízeními podporující standard IEEE 802.11e.

4.3. Další doplňkové standardy 802.11

V současné době se pracuje na dalších přírůstcích do rodiny IEEE 802.11, které by měly zvýšit komfort a potenciál již stávajících řešení a přispět tak k využití 802.11 v profesionální oblasti [14], [20], [23], [28], [34].

4.3.1. IEEE 802.11i

Standard IEEE 802.11i, označovaný jako WPA2, byl IEEE schválen v červnu roku 2004. Upravuje bezpečnostní opatření pro WLAN sítě. Pomocí účinných šifrovacích metod a autentizačních algoritmů tento standard zajišťuje lepší ochranu sítě i přenášených dat, což je velmi podstatné pro profesionální aplikace. WPA2 používá blokovou šifru AES (Advanced Encryption Standard), zatímco dřívější WEP a WPA používají proudovou šifru RC4.

802.11i architektura obsahuje následující komponenty: IEEE 802.1x pro autentizaci (používá se tedy EAP (Extensible Authentication Protocol) a autentizační server), RSN (Robust Security Network) pro udržování záznamu asociací, na AES založený CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), který poskytuje utajení, integritu a autentizaci, a nebo protokol TKIP (Temporal Key Integrity Protocol), který zajišťuje kombinování klíčů pro pakety, kontrolu integrity zprávy a mechanismu překlíčování.

4.3.2. IEEE 802.11n

Tato norma 802.11n „Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Enhancements for Higher Effective Throughput“ modifikuje

stávající fyzickou vrstvu a MAC vrstvu tak, aby se na úrovni MAC docílilo propustnosti minimálně 100 Mbit/s. Udávaná rychlost má být reálná, v teoretických číslech se uvažuje o rychlostech až do 600 Mbit/s.

Standard by dle IEEE měl být dokončen v září 2008. V současné době existují výrobky postavené na draftech tohoto standardu. Využívají technologie MIMO (Multiple Input – Multiple Output), která spočívá ve využití více antén jak na přijímači, tak na vysílači. Původní návrhy počítaly s šířkou pásma 40 MHz, ale z důvodů zpětné kompatibility se nakonec rozhodlo pro šířku 20 MHz.

4.3.3. IEEE 802.11p

Standard 802.11p se týká bezdrátového přístupu pro mobilní zařízení (WAVE, Wireless Access for the Vehicular Environment). Norma představuje rozšíření standardů 802.11 pro podporu ITS aplikací. To zahrnuje komunikaci mezi vozidly ve vysokých rychlostech (do 200 km/h) a mezi vozidly a pevnou infrastrukturou v licencovaném pásmu 5,9 GHz.

Standard má mimo jiné představovat základ pro DSRC (Dedicated Short Range Communications), má spolupracovat se systémem CALM a podporovat aplikace typu jako výběr mýtného, informování servisů o stavu vozidla z hlediska bezpečnosti, peněžní transakce prostřednictvím automobilů. Vzdálenou vizí je jednotná celostátní (celosvětová) síť umožňující komunikaci mezi vozidly a přístupovými body v okolí silnic nebo přímo mezi jednotlivými vozidly.

Pracovní skupina je stále aktivní, dle posledních informací by standard měl být dokončen v březnu 2009 [20].

4.3.4. IEEE 802.11r

Současné předávání spojení založené na doplňku IEEE 802.11f je příliš pomalé pro aplikace v reálném čase, proto se pracuje na vývoji doplňku rychlého roamingu IEEE 802.11r. Ten by měl zajistit bezproblémové předání spojení mezi stanicemi

s nepoznatelným přechodem (handover) včetně zajištění nepřetržitého šifrování spojení pomocí 802.11i.

V současné době je vytvářeno tělo standardu ze dvou zbývajících návrhů, TAP (Transition Acceleration Protocol) a Just-In-Time 2 Phase Association. Dokončení standardu se dle IEEE očekává v březnu 2008 [20].

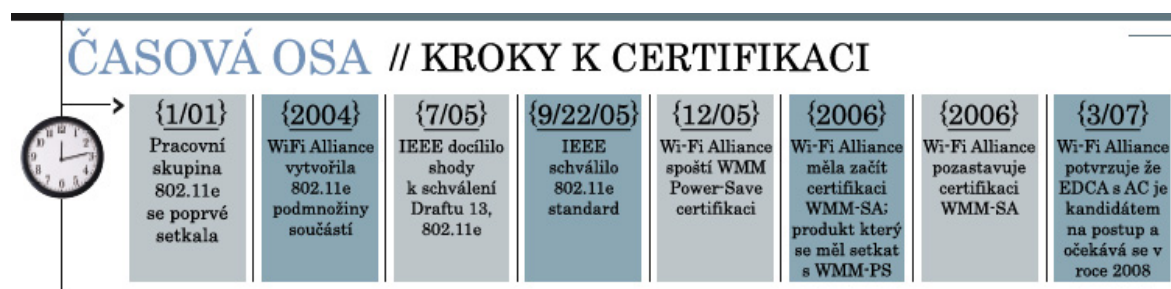
4.4. Certifikace a přínos standardu 802.11e

Standard IEEE 802.11e má tři stupně certifikace. První stupeň pod označením WMM (Wireless MultiMedia), dříve WME (Wireless Multimedia Extensions), byl vytvořen v roce 2004 jako draft standardu. WMM tedy podporuje pouze některé prvky z normy. Certifikované WMM zařízení musí podporovat EDCA přístup, ostatní rozšíření jsou volitelná.

Druhým stupeň certifikace představuje WMM Power Save (WMM-PS), které obsahuje všechny prvky z WMM a přidává rozšíření pro úsporu energie zařízení, což je vhodné především pro mobilní zařízení, jako jsou mobilní telefony, PDA a podobně.

Třetí konečný stupeň certifikace nese označení WMM Scheduled Access (WMM-SA) a obsahuje všechny prvky z normy 802.11e, včetně HCCA metody.

Na následujícím obrázku jsou uvedeny důležité kroky v postupu certifikace standardu IEEE 802.11e.



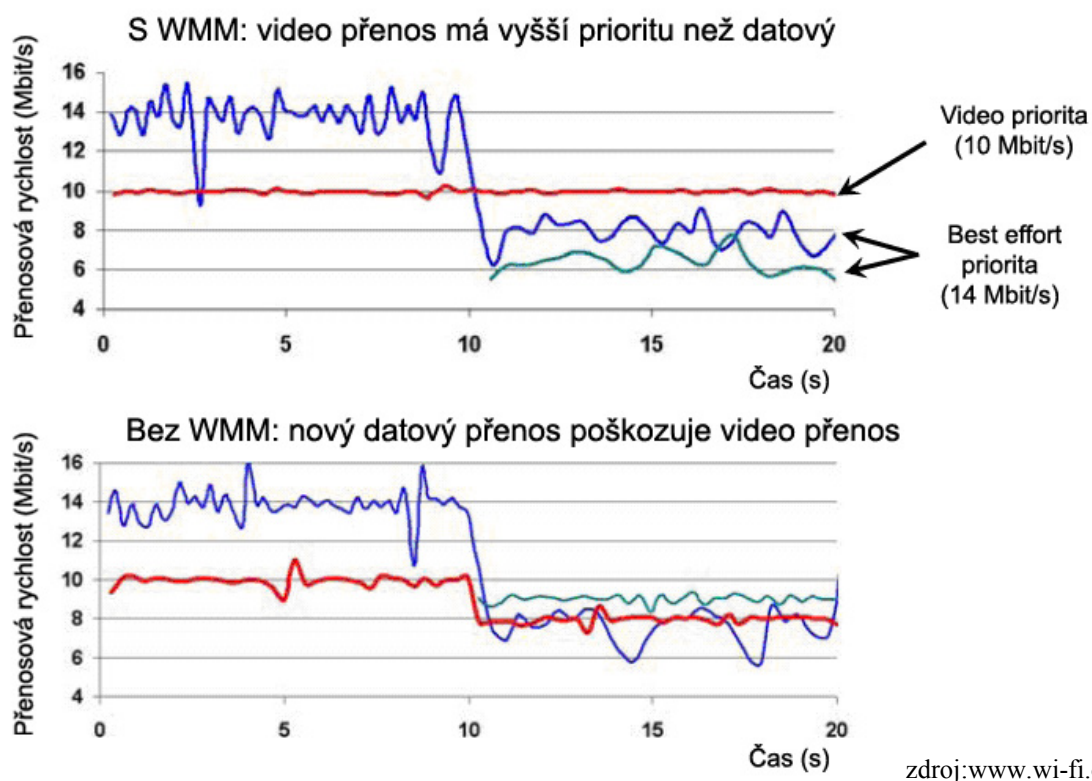
Obr. 8 - Certifikace IEEE 802.11e

zdroj: www.networkcomputing.com

Jak lze z obrázku vyčíst, třetí finální verze certifikace WMM-SA standardu 802.11e není dosud dostupná. Wi-Fi Alliance stále odsouvá certifikaci této verze a místo toho se v roce 2007 zaměřila na rozšíření EDCA pomocí řízení přístupu (AC, Admission Control), které má umožnit podporu většího množství souběžných spojení vyžadujících vyhrazenou

rychlost. V současné době (5.8.2007) dle [19] má WMM certifikaci uděleno 499 produktů a WMM-PS celkem 91 produktů. Konkrétní aktuální seznam certifikovaných zařízení je možno nalézt na stránkách Wi-Fi Alliance [19].

Wi-Fi Alliance provedla několik testů WMM technologie, které prokázali její schopnost vyhovět požadavkům přenosu. Na následujícím obrázku je vidět výsledek testu.



Obr. 9 - Test WMM priorizace

Na obrázku je vidět, jak probíhá přenos videa s videoprioritou, u něhož je požadována přenosová rychlost 10 Mbit/s. Zároveň probíhá stahování souboru rychlostí cca 14 Mbit/s. Celkově máme k dispozici cca 24 Mbit/s. Po deseti vteřinách přijde požadavek na stahování dalšího souboru. U horního grafu je zapnuta volba WMM, tím pádem nedochází ke zhoršení kvality přenosu videa, ale přenosu s nižší prioritou, což je právě přenos souborů, který se rozdělí o zbylých 14 Mbit/s. U spodního grafu není zapnuta volba WMM a po požadavku na stahování druhého souboru tedy dojde k rovnoměrnému rozložení dostupné rychlosti mezi všechny právě probíhající přenosy, což má za následek snížení rychlosti u přenosu videa a tím dochází k nekvalitnímu příjmu videa [38].

Standard IEEE 802.11e tedy zavádí priority provozu do stávající WiFi technologie. Verze WMM-SA dává navíc možnost detailního nastavení QoS systému. Ta bohužel stále není

dostupná, a tak není možné otestovat tuto variantu. WMM prošla testem Wi-Fi Alliance výborně, ovšem je otázka, jak by se osvědčila v reálném provozu, kde existuje mnoho dalších faktorů ovlivňujících přenos. Z principu funkce EDCA je evidentní, že se stále jedná o provoz založený na CSMA/CA a jako takový nedokáže poskytnout opravdové garance QoS. Očekávaná verze WMM-SA podporující funkci HCCA by již měla nabídnout jisté záruky kvality. Je teoreticky možné, aby produkty podporující WMM byly pomocí upgrade software upraveny na WMM-SA, ovšem je otázkou, zda bude tato možnost využita. Výrobci by se tím připravili o možnost donutit nás k nákupu nového zařízení [14].

5. Zhodnocení standardu 802.11 pro ITS

Abychom mohli hodnotit využití WiFi pro ITS aplikace, je nutné definovat ještě několik dalších vlastností a otázek týkajících se WiFi.

5.1. Vlastnosti 802.11

5.1.1. Otázka sdíleného pásma

Prvním velmi podstatným faktem je to, že 802.11 operuje v bezlicenčním pásmu, kde z podstaty přístupu k němu není možné vyloučit případné interference s okolními zařízeními. Všeobecné ohlášení řeší problém interference na stejném kanálu systémem, kdo začne vysílat první, má na kanál právo. Pokud ovšem začne někdo vysílat na vedlejším kanále, interference se vyskytne taktéž a problém již není řešen. Vše je doporučováno řešit domluvou mezi provozovateli přístupových bodů, nicméně pásmo je poměrně omezené a WiFi dosti rozšířená, takže ne vždy je možné vyloučit interference.

Pokud ovšem budeme síť provozovat v uzavřeném prostoru, kam jen stěží pronikne signál z vnějšku, nemusíme se obávat interference s okolními zařízeními. Příkladem takovýchto prostorů mohou být podzemní garáže, různé kovové haly, hangáry a podobné objekty.

Provoz v bezlicenčním pásmu může být považován i za značnou výhodu, jelikož zprovoznění takového systému je otázka pouze samotného nákupu a instalace zařízení. Pokud chceme zprovoznit systém založený na licencovaných pásmech, je nutné poměrně zdlouhavé vyřizování licencí.

5.1.2. Otázka bezpečnosti

Bezpečnost WiFi řeší doplněk IEEE 802.11i diskutovaný v kapitole 4.3.1. Kromě tohoto doplněku lze zvýšit bezpečnost sítě zavedením MAC access listu. Ten definuje, které zařízení s danými MAC adresami se mohou připojit na vysílač, případně které nemohou. Další dodatečnou bezpečnostní vlastností je možnost zamezení vysílání SSID

identifikátoru sítě. Vysílač potom nelze při procházení éteru nalézt, a pokud cizí zařízení nezná používaný konkrétní název sítě, nedokáže se k vysílači připojit. Toto je ovšem nebezpečná vlastnost, protože ostatní provozovatelé sítě nemohou detekovat vysílač se skrytým identifikátorem a klamně se tak domnívají, že kanál je volný. Jeho obsazení se pak projeví až při provozu sítě.

5.1.3. Otázka handoveru

Handover, nebo-li předání spojení, u WiFi označované jako roaming, představuje pro systém další problém. Roaming probíhá na druhé nebo třetí vrstvě síťové architektury. WiFi řeší pomocí interních protokolů roaming na druhé vrstvě v rámci jedné IP sítě. Pro roaming v rámci třetí vrstvy se musí zapojit Mobile IP protokol. Roaming je možný na základě doplňku IEEE 802.11f, který řeší komunikaci mezi přístupovými body různých výrobců protokolem IAPP. (Inter Access Point Protocol).

Při předání spojení po WiFi je třeba provést následující kroky:

- Získat seznam dostupných vysílačů, ke kterým se lze přepojit
- Získat status řízení přístupu (AC) nového vysílače
- Rozhodnout se, zda je čas pro přepnutí
- Přepnutí na nový vysílač:
 - o Autentifikovat se s novým vysílačem
 - o Vyměnit si klíče pro spojení s novým vysílačem
 - o Získat nové IP adresy, pokud je to nutné
 - o Obnovit přenos dat

Celý tento proces je poměrně pomalý a v extrémních případech může být systém rozpojen až v řádech vteřin. Pro zrychlení roamingu ovšem existuje několik metod [14],[30],[39].

Key-caching je metoda, kde si přístupový bod ukládá klíče jednotlivých spojení, takže při opětovném připojení není nutné znovu zadávat všechny údaje a celé připojení se zjednoduší na výměnu čtyř zpráv (ohledně bezpečnostní relace spojení). Tato metoda dokáže snížit zpoždění při předávání klienta z 800 ms až na 25 ms, což je velmi znatelné, a hodnota 25 ms je již přijatelná i pro aplikace pracující v reálném čase.

Pre-authentication je další podpůrná metoda redukující zpoždění. Key-caching redukuje zpoždění na základě informací o klientovi, které má z posledního spojení, pokud se ovšem jedná o první připojení, tento systém nám zpoždění nesníží. Pre-authentication tedy zajišťuje předání informací o klientovi okolním kooperujícím vysílačům, aby bylo možné později vytvořit spojení pomocí key-caching metody.

Další problém nastává, pokud je spojení šifrováno pomocí WPA. Zde je třeba stávající šifrovaný tunel zrušit a vytvořit nový tunel přes nový vysílač. Doba zpoždění s použitím výše uvedených metod se pak prodlužuje až na 70 ms, což už není zanedbatelné.

SyncScan je softwarová metoda, která dokáže zredukovat zpoždění při předání spojení až na 5 ms. Jedná se o algoritmus vyvinutý na univerzitě Jacobs School of Engineering v San Diegu, USA. Podstatou je načasování jednotlivých akcí při handoveru, skenování okolních vysílačů probíhá průběžně na pozadí. Metoda je jednoduchá, není třeba žádná změna na vysílačích. Redukce zpoždění lze dosáhnout i při použití software pouze na jedné straně spoje [40].

Pro zlepšení celého procesu je vyvíjen doplněk IEEE 802.11r diskutovaný v kapitole 4.3.4., který má nabídnout plnou podporu rychlého handoveru zabezpečeného spojení se zpožděním v jednotkách ms.

5.1.4. Diskuse

WiFi má tedy vlastnosti vhodné pro ITS systémy, nicméně stále se jedná o systém založený na komunikaci v bezlicenčním pásmu kolizním protokolem. Jak bylo uvedeno, WiFi je poměrně hodně rozšířené, takže je velká možnost interference s okolím a zároveň to stanovuje jistou bezpečnostní hrozbu, proto je použití omezené.

WiFi má tedy své výhody a nevýhody, pokusíme se je zhodnotit pomocí SWOT analýzy.

Silné stránky (Strengths)	Slabé stránky (Weaknesses)
- levná technologie - jednoduchá instalace - bezlicenční pásmo - možnost QoS díky 802.11e - bezpečnost díky 802.11i	- bezlicenční pásmo - vysoká dostupnost technologie - komunikace založená na kolizním protokolu

(Příležitosti) Opportunities	Hrozby (Threats)
- další rozšíření standardu - možnost okamžitého použití	- bezpečnostní rizika - nedostatečná kvalita komunikace - nedostatečná funkčnost systému

Tab. 5 - SWOT analýza standardu IEEE 802.11

Po představení základních vlastností systémů založených na standardu 802.11 přistoupím k jejich zhodnocení v rámci použitelnosti pro ITS aplikace.

5.2. Srovnání 802.11 vs. 802.16

Základní parametry obou systémů vynesu do přehledné tabulky.

	802.11a	802.11b	802.11g	802.16d	802.16e
frekvenční pásmo	sdílené 5 GHz	sdílené 2,4 GHz	sdílené 2,4 GHz	licencované 3,5 GHz	licencované 3,5 GHz
rychlost přenosu	do 36 Mbit/s	do 6 Mbit/s	do 30 Mbit/s	do 70 Mbit/s	do 15 Mbit/s
dosah	až 8 km	až 8 km	až 8 km	až 50 km	až 50 km
modulace	OFDM	DSSS	DSSS, OFDM	OFDM	SOFDMA
bezpečnostní nástroje	WEP, WPA, WPA2	WEP, WPA, WPA2	WEP, WPA, WPA2	DES3, (AES)	DES3, (AES)
priority paketů	ANO (s 802.11e)	ANO (s 802.11e)	ANO (s 802.11e)	ANO	ANO
IP roaming	ANO	ANO	ANO	ANO	ANO
dynamické předání (handover)	ANO (s doplňkem)	ANO (s doplňkem)	ANO (s doplňkem)	ANO	ANO
QoS	ANO (s 802.11e)	ANO (s 802.11e)	ANO (s 802.11e)	ANO	ANO
tolerance pohybu	–	–	–	–	150 km/h
dostupnost standardu	1999	1999	2003	2004	2005

Tab. 6 - Parametry IEEE 802.11 a 802.16

Systémy na bázi IEEE 802.16 jsou stavěné jako profesionální bezdrátové systémy nabízející kromě vyšší kapacity přenosu a většího dosahu především plnou podporu QoS,

garance přenosu a ve verzi 802.16e podporuje systém taky plně mobilitu klientů. Nejbližší WiMaxu se přibližuje WiFi 5, které má vyšší kapacitu než ostatní verze WiFi, zároveň nabízí větší počet nekolidních kanálů a díky implementaci doplňků standardu dokáže podporovat i QoS a rychlý handover. Oproti ostatním systémům ale pracuje v nejvyšším frekvenčním pásmu – 5 GHz, kde jsou požadovány větší nároky na přímou viditelnost mezi vysílačem a klientem. WiMax pracující na frekvenci 3,5 GHz dokáže pracovat v režimu NLOS a nevyžaduje přímou viditelnost mezi vysílačem a klientem.

Abychom mohli doporučit jednotlivé technologie pro různé ITS aplikace, je nutné znát aplikace konkrétně a analyzovat je. Uvedené technologie jsou všechny použitelné, mají specifické vlastnosti a záleží na typu aplikace. Někde může být na první pohled nevýhoda výhodou a naopak. Obecně je tedy nutno řešit otázky bezpečnosti systému, spolehlivosti a dalších pro aplikaci důležitých parametrů.

Použití 802.11 pro inteligentní dopravní aplikace závisí především na dané konkrétní aplikaci a na tom, jak specificky má stanovené jednotlivé požadované parametry.

5.3. Volba alternativního řešení

Při návrhu alternativního či doplňkového telekomunikačního řešení pro komplexní systém je nutné zajistit vlastní předání spojení mezi buňkami jedné technologie, označované jako handover, a předání spojení mezi jednotlivými komunikačními technologiemi, toto předání bývá označováno jako vertikální handover.

U handoveru rozeznáváme tři druhy přepínání z pohledu přepínacího procesu. Tvrdý handover (Hard Handover), kde je nejprve stanice odpojena od původní sítě a poté je teprve připojena do sítě nové. Dále bezešvý handover (Seamless Handover), kde se nejdříve vytvoří spojení do nové sítě a teprve poté je zrušeno spojení do původní sítě. Poslední je měkký handover (Soft Handover), kde se využívá faktu, že stanice je neustále připojena alespoň do dvou sítí. Při pohybu jsou tak průběžně některá spojení rušena a zároveň vznikají nové. Poslední jmenovaný způsob handoveru v kombinaci s vertikálním handoverem je vhodný pro potřeby zajištění komunikace u ITS aplikací, nicméně způsobuje větší nároky na kapacitu a zahuštění sítě.

Předání spojení musí splňovat jisté předem definované parametry. Je nutné definovat, jaký typ handoveru má proběhnout, do jaké rychlosti má proběhnout, případně do jaké doby má dojít k obnovení služby po rozpojení. Pro volbu alternativního řešení lze využít několik systémů, stručně představím dva z nich.

5.3.1. CALM

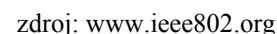
CALM (Communications Air-interface for Long and Medium range) je rodina standardů TCO TC204 WG 16.1 a ETSI ERM TG37, která utváří jednotnou vrstvu síťového rozhraní pro různé bezdrátové technologie, např. DSRC, WiMax, WiFi, GSM, IrDA. [9]

V podstatě se jedná o systém, který zajišťuje výběr „nejlepšího“ komunikačního řešení z právě dostupných řešení na základě stanovených kritérií pro různé konkrétní ITS aplikace. Dá se říct, že systém zajišťuje jakýsi vertikální i běžný handover, ovšem podstatně rozšířený. Kritéria pro výběr „nejlepšího řešení“ mohou být technického rázu, jako např. chybovost, doba zpoždění, tolerance rychlosti pohyb atd., ale mohou být i ekonomického a bezpečnostního rázu. Jednotlivá kritéria mohou být navíc vzájemně provázaná. Změnu komunikačního řešení tedy nemusí vyvolat pouze nedostatečná úroveň signálu nebo velká chybovost spoje, ale například i drahý provoz spoje nebo nízká priorita aplikace.

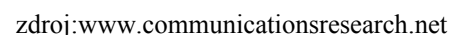
Při použití komunikačních systémů vyšší systémové úrovně („carrier grade“), jako například WiMax, je třeba zohlednit fakt, že již technologie samotná má implementován optimalizační algoritmus a díky vnitřní regulaci parametrů systémem CALM může dojít ke kolizi obou optimalizací. Proto je nutné nastavení parametrů a referenčních hladin tak, aby nedocházelo ke kontraproduktivní interakci obou řídicích procesů.

Nejvýznamnějším použitím systému CALM je komunikace pevné infrastruktury s pohybujícím se vozidlem. Systém ale dokáže zajistit i komunikaci typu vozidlo-vozdlo nebo infrastruktura-infrastruktura, což může být někdy velmi vhodné.

Na obr. 10 je znázorněna architektura systému CALM. Každé komunikační rozhraní má svoji vlastní management vrstvu a adaptační vrstvu. Mezi jednotlivými oblastmi



je zaveden SAP (Service Access Point) pro správu služeb. Lze vidět, že systém má mnoho vrstev pro detailní management systému. Jádrem CALM tvoří IPv6 (adresování, směrování), CME (CALM Management Entity) entita a další podpůrné nástroje. Systém nabízí podporu pro aplikace vyžadující systém CALM (CALM aware) i pro aplikace, které CALM nevyžadují a přenos je pro ně zcela transparentní (Non-CALM-aware).



Obr. 11 - CALM management entita (CME)

CME je zodpovědná za správný a nejvhodnější výběr komunikačního média podle požadavků aplikací. CME porovnává vlastnosti dostupných médií a požadavky spuštěných aplikací. Požadavky aplikací a hlavní charakteristiky médií jsou předem definovány a uloženy v paměti entity jako statické charakteristiky. Kromě těchto statistik porovnává CME také vlastnosti dynamické, získané při registraci média a jeho monitorování.

5.3.2. L2/L3 switching

Tato metoda je založená na IEEE 802.3, 802.1d a 802.1q aplikované na druhé vrstvě síťové architektury. Principiálně přepínání funguje tak, že jednotlivá rozhraní, jak klientské zařízení tak vysílače, jsou jednoznačně určena MAC adresou. Na těchto rozhraních mají zařízení přiděleny IP adresy, pomocí kterých probíhá směrování jednotlivých paketů. Na rozhraní lze vložit několik různých statických IP adres a vhodně vytvořit pomocí 802.1q VLAN spojení s požadovanou prioritou přenosu. Pomocí diagnostických nástrojů na L3 je zjišťován stav jednotlivých spojení a při překročení předem definovaných hranic spoje je přesměrována komunikace z jedné VLAN do jiné, resp. z jedné IP na jinou. Standardy obsahují několik podporujících protokolů, které urychlují obnovení sítě po výpadku.

Toto řešení má potenciál dosáhnout vhodných parametrů rychlého nekonfliktního přepínání pro většinu aplikací a má velmi výhodný poměr mezi výkonem a cenou. [4],[8]

5.3.3. Kritéria volby alternativy

Jednotlivá kritéria volby alternativních řešení jsou úzce spojena s konkrétní aplikací. Kritéria korespondují s performačními indikátory, ale pro volbu alternativního řešení se systém může rozhodnout i na základě dalších parametrů, jako například v systému CALM podle ekonomických hledisek. Na základě dostupných informací a blíže specifikovaných požadavků na aplikaci se stanoví významné parametry, jejichž hodnoty budou východiskem ke konkrétní volbě alternativních technologií a jejich nastavení. Nejčastěji se jedná o technické zajištění požadované služby, a proto se stanovují kritéria jako maximální doba zpoždění přenosu, maximální procento ztracených paketů, minimální přenosová rychlost, maximální doba výpadku systému a další provozní parametry. Při překročení některého z parametrů dojde ke změně používané technologie na vhodnější. Cílem je vždy dodržení spojení na základě dohody o kvalitě poskytovaných služeb (SLA – Service Level Agreement) se snahou minimalizovat náklady.

6. Návrh alternativního řešení pro Letiště Praha

Na základě výsledků testování technologií z minulých let v rámci projektu Monitorování a řízení pohybu objektů po ploše letiště pomocí GNSS (Grant MDS 802/210/112) v rámci účasti České republiky v projektu Galileo, byla zvolena nosná komunikační technologie pro tento projekt. Tou se stala mobilní verze technologie WiMax – IEEE 802.16e pro vlastnosti vhodné pro tento projekt (licencované pásmo, zabezpečení přenosu dat, handover, garance kvality služby QoS,...).

V projektu byla testována i technologie WiFi ve verzi 802.11b v roce 2003. Výsledky testů nebyli špatné a bylo doporučeno test zopakovat, k tomu bohužel nedošlo. Dnes je k dispozici i méně problémová verze WiFi – 802.11a, kterou by bylo vhodné otestovat v provozu na Letišti Praha.

6.1. Systémové požadavky řešení pro Letiště Praha

Letiště Praha má poměrně vysoké požadavky na jednotlivé parametry telekomunikačního řešení systému.

Přenosová kapacita

Je třeba zajistit dostatečnou přenosovou kapacitu systému pro několik desítek klientských zařízení. V systému se přenáší především polohové informace, a to celkem 3 druhy (poloha jednotky se přenáší na server, server přenáší polohy všech zařízení všem zařízením a zároveň server přenáší i polohy jednotek ze systému A-SMGCS). Podle potřeby jsou přenášeny i servisní zprávy spojené s autentifikací klientů a s řízením provozu na letišti. Servisní zprávy lze vzhledem k rozdílu mezi jednotlivými typy přenosu zanedbat. Polohová informace z jednoho klienta představuje včetně režie v průměru 70 bitů. Pokud budeme uvažovat n klientů, m objektů ze systému A-SMGCS a aktualizaci s frekvencí f Hz, lze požadovaný bitový tok pro distribuci polohových dat dle [10] vyjádřit takto

$$C = f \cdot n \cdot (m + n - 1) \cdot 70 \cdot 8 \quad (15)$$

Jedná se o datový tok směrem ke klientům, tedy download, který je potřeba zajistit, aby bylo umožněno zásobování klientů dostatečně aktuálními polohovými daty o všech objektech v systému. V rovnici je bohužel kvadratická závislost C na n , což představuje

určitou neoptimalitu v komunikaci. Pro 50 klientů systému, spolu s 20 objekty aktuálně přítomnými v A-SMGCS s frekvencí distribuce 5 MHz dostaneme

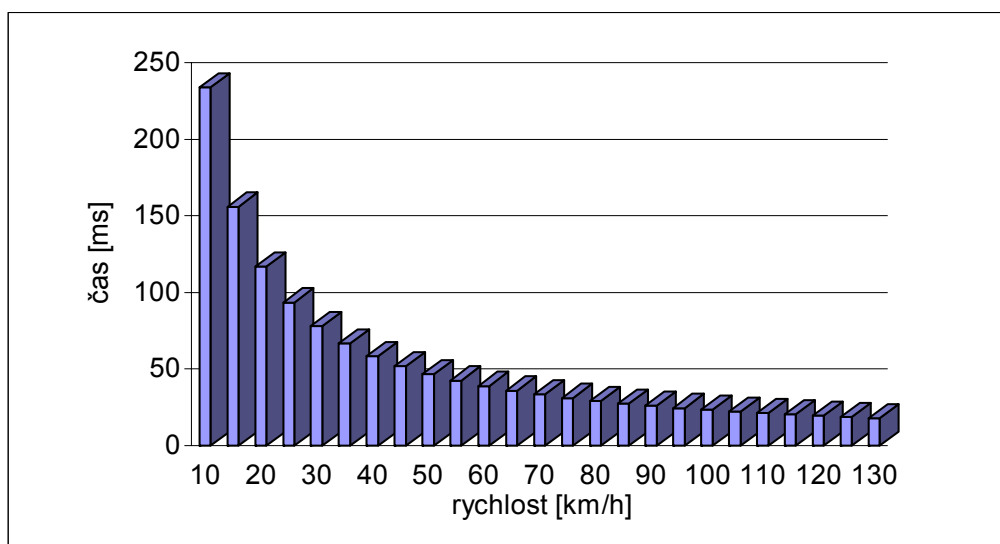
$$C = 5 \cdot 50 \cdot (20 + 50 - 1) \cdot 70 \cdot 8 = 9,66 \text{ Mbit/s} \quad (16)$$

Přenosová kapacita v takové konfiguraci je téměř 10 Mbit/s. Při dvojnásobném počtu klientů a objektů z A-SMGCS s frekvencí 5 MHz se pak jedná o přenosovou kapacitu až téměř 39 Mbit/s. Je nutno vzít v potaz fakt, že uvedené výpočty počítají se stoprocentní spolehlivostí přenosu paketů. Je nutné započítat určitou chybovost paketů, nicméně kdyby protistrana polohovou informaci o některém klientu nedostala, není důvod se ji snažit odeslat znova. Server v dalším „kole“ posílá opět aktuální pozici o klientech, původní informace je již neaktuální.

Mobilita ve vazbě na přesnost určení polohy

V případě lokalizačních funkcí je dán předpisem požadavek, že pokud přesnost určení polohy překročí hranici 10 m, musí být uživatel o této změně přesnosti informován do 5 s na hladině pravděpodobnosti 99%. Jedná se tedy spíše o otázku integrity systému. Přesnost určení polohy přímo souvisí s aktuálností polohových dat, potažmo s rychlostí pohybujících se objektů. Směrnice Eurocontrol Op_Perf-06 a EUROCAE 3.2.3 stanovuje, že u služby monitorování pohyblivých objektů na pohybové ploše letiště nesmí chyba předané polohové informace překročit v horizontální rovině 12 m na hladině pravděpodobnosti 99,9%. Pokud se však jedná o službu řízení a navigování, je přípustná maximální horizontální chyba 7,5 m na hladině pravděpodobnosti 99,9%. Tato přesnost činí poměrně velké problémy systému GPS i u nepohyblivých objektů. S moderními multikanálovými vysoce citlivými přijímači je sice možné dosáhnout požadované přesnosti, nicméně stále je řeč o určení vlastní polohy. Jakmile uvedeme objekt do pohybu a chceme polohovou informaci přenést z objektu na server a následně zpět do ostatních klientů, může být chyba 7,5 m dosažena už jen z podstaty mobility a nenulové přenosové doby.

Navigační systém Galileo by měl v rámci svých garantovaných služeb přinést přesnost určení polohy lepší než 1 m a v kombinaci s pozemními stanicemi dokonce 0,1 m. Budeme-li tedy dále uvažovat maximální chybu budoucího systému Galileo 1m, zbývá 6,5 m na chybu spojenou s mobilitou. Tuto chybu lze pro různé rychlosti převést na čas podle vztahu $t = \frac{s}{v}$. (obr. 12)



Obr. 12 - Disponibilní časy pro přenos a zpracování polohy při chybě 6,5 m pro různé rychlosti

Disponibilní čas představuje čas, který uplyne od náhodně zvoleného okamžiku do zobrazení polohy klienta na obrazovce jiného klienta. Za tento čas musí proběhnout následující procesy:

- čekání na odeslání polohy na server
Low-endové přijímače svoji polohu počítají jednou za sekundu, specializované přístroje s periodou 100 ms a kratší. Spíše než čekání na odeslání je to nejhorší možný čas, představující stáří poslední známé polohy v okamžiku jejího odeslání.
- odeslání poslední vypočtené vlastní polohy telekomunikačním prostředím z klienta na server
- zpracování dat na straně serveru
- rozeslání polohové informace ze serveru všem klientům (odesílání probíhá se zmíněnou frekvencí f)
- zpracování dat na straně klienta (interpretace a prezentace polohové informace)

Prostorové zajištění služby

V prostorách letiště je nutno specifikovat území s různou úrovní požadavků na performační parametry. Není příliš efektivní řešit prostory, které nemají tak vysoké nároky hlavní komunikační službou, a to jak z ekonomického, tak ze systémového hlediska. Příkladem

mohou být letištní hangáry, kam stěží pronikne signál hlavní komunikační služby. Oblast vnitřku hangáru nepatří mezi kritické oblasti pro sledování objektů, a proto není ekonomicky vhodné řešit pokrytí vnitřku hangáru opět nosnou telekomunikační službou. Uvnitř hangáru navíc musí dojít ke změně na alternativní zdroje polohové informace, jelikož uvnitř hangáru není dostupný signál pozičních GNSS služeb.

Rozdělení na zóny letiště bylo navrženo takto [4]:

	Typ	Popis
1.	Kritická	Oblast přistávacích a startovacích drah letadel a jejich okolí
2.	Významná	Oblast pojížděcích drah letadel
3.	Ostatní	Oblasti mimo dosah pohybujících se letadel

Tab. 7 - Oblasti letištní plochy podle nároků na performační indikátory

- V kritické oblasti je nutno řešit pokrytí území hlavní komunikační službou tak, aby nedocházelo k jakýmkoliv změnám, a to ani k předávání spojení. Doba obnovy spojení musí být zajištěna s dostatečnou rezervou. Je vyžadována plná redundance všech prvků telekomunikačního řetězce.
- Ve významné oblasti se počítá s přepínáním mezi buňkami a se změnami přenosových parametrů jednotlivých přenosových systémů. Pro zajištění garance kvality poskytované služby je možné například omezit maximální rychlost objektů v určité oblasti.
- V ostatních oblastech se počítá s hybridním řešením s maximálním stupněm automatického obnovení v případě výpadku služby. Počítá se zde s automatickou volbou alternativního komunikačního média a případným přepínáním na alternativní zdroje polohové informace.

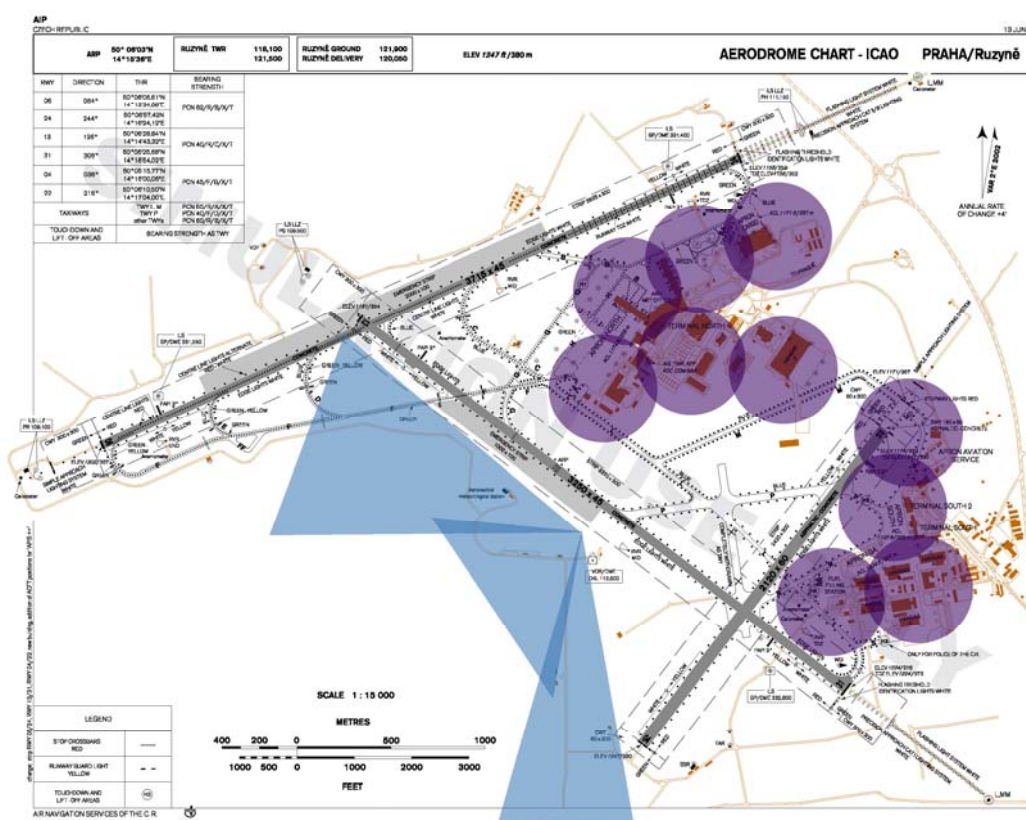
6.2. Návrh vlastního doplňkového řešení

Na základě uvedených požadavků v minulé kapitole se jeví jako nejlepší možnost použití technologie WiFi5 (802.11a), jelikož nabízí větší množství bezkolizních kanálů, větší přenosovou rychlost, je méně rozšířená a v kombinaci s implementací WMM-PS a WPA2 je schopna nabídnout požadovanou úroveň přenosu dat v nesnížené kvalitě.

6.2.1. Plánování pokrytí

Vzhledem k požadavkům Letiště Praha je technologie WiFi vhodná pouze pro oblasti s označením jako „ostatní“, kde nehrozí kolize vozidla s letadlem a nejsou zde tak vysoké požadavky. Technologie je vhodná i pro prostory, kde existuje limitace prostředí, jako jsou hangáry, podzemní parkoviště a podobné objekty. Je zbytečné pokrývat území, kde bez jakýchkoliv problémů funguje hlavní nosná technologie. U ní je očekáváno plné pokrytí přistávacích, vzletových a pojezdových drah a jejich okolí. Problém může nastat v blízkosti objektů letiště.

Bez testu nelze stanovit dosah technologie v reálné situaci. Na základě předchozích testů [11] byl dosah WiFi 802.11b stanoven na 600 m s všesměrovými anténami. Předpokládáme tedy, že dosah bude opět cca 600 m a v případě potřeby je zde možnost použít sektorové antény s větším ziskem a docílit tak delšího dosahu. Na základě rozboru prostorů letiště s odborníky z firmy Telematix byly nalezeny vhodné oblasti pro pokrytí touto technologií.



zdroj: www.prg.aero

Obr. 13 - Umístění a očekávané pokrytí AP

Na obr. 13 je zakresleno teoretické umístění několika venkovních AP s všesměrovými anténami (fialová barva) v okolí budov letiště, kde technologie může nahradit nosnou technologii při výpadku nebo nedostatku signálu. Dále se jedná o 6 AP umístěných uvnitř 6-ti hangárů v prostorách letiště, která na obrázku nejsou naznačena. Mezi „ostatní“ oblasti patří i komunikace v okolí drah, v mapce zakreslené hnědou barvou. U nich je zakresleno jedno AP se třemi sektorovými anténami většího dosahu (modrá barva). V této oblasti se pravděpodobně vzhledem k přítomnosti nosné technologie nevyplatí stavět AP alternativní technologie, jelikož nosná technologie je pečlivě zálohována. Jedná se pouze o teoretický náznak řešení. Na zvážení je i navržený počet a umístění jednotlivých AP. Navrhované řešení je nutné sladit s pokrytím nosné technologie, které bohužel zatím není realizované vzhledem k nedostupnosti zařízení. Konkrétní návrh by měl vycházet z dostupnosti, resp. nedostupnosti signálu v jistých oblastech, především okolo budov. Jedním z míst, kde by mohl pravděpodobně nastat problém, je okolí hangárů u terminálu jih. Zde se pokusím navrhnout konkrétní řešení. Na následujícím obrázku je naznačeno pokrytí zmiňované oblasti.

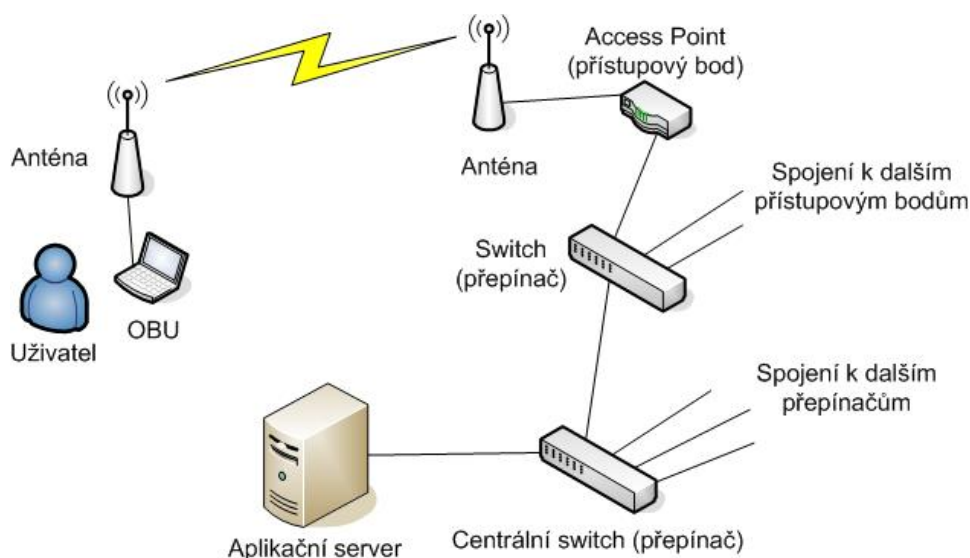


Obr. 14 - Detail pokrytí oblasti v okolí hangárů u terminálu jih zdroj: earth.google.com

Pro pokrytí je zapotřebí vybudovat 5 přístupových bodů. Tyto body budou osazeny několika směrovými anténami tak, aby se dosáhlo rovnoměrného pokrytí na všech pojezdových plochách v okolí budov, aniž by některá z nich stínila. Při návrhu je použito 8 antén s úhlem vyzařování 90° a 5 antén s vyzařovacím úhlem 120°. Pro pokrytí vnitřku hangáru postačuje jedna anténa s vyzařovacím úhlem 90° umístěná v rohu budovy. Celkově je tedy použito 13 antén s úhlem 90° a 5 antén s úhlem 120° pro pásmo 5 GHz. Vzhledem k počtu antén je nutno vhodně rozvrhnout i využití kanálů, což ovšem není problém, jelikož je k dispozici 13 kanálů a antény jsou směrové, takže je možné vícenásobné využití kanálů v různých oblastech.

6.2.2. Architektura

Pro každou anténu je třeba jeden access point. V přístupových bodech jsou umístěny říditelné přepínače podporující L2/L3 switching, ve kterých jsou napojeny jednotlivé access pointy. Přepínače jsou napojeny na místní síťovou infrastrukturu letiště a cesty končí v serverovně u centrálního přepínače a serverů aplikací, kde se do databáze zaznamenávají všechny pohyby vozidel a jejich akce, informace se poskytují ostatním uživatelům sítě. Je zde spuštěn server RADIUS, který slouží pro řízení přístupu pouze autorizovaných klientů do sítě a zajišťuje například distribuci sdílených klíčů pro šifrování komunikace.



Obr. 15 - Architektura návrhu

6.2.3. Hardware

Na trhu se objevují přístupové body podporující funkci WMM i v kategorii low-end zařízení vhodné pro domácí nenáročnou síť. Pro použití v naší aplikaci je nicméně nutné zaměřit se na výrobky profesionální. Po prostudování udělených certifikací a současného trhu se nám nabízí výrobky od několika firem. Pro návrh jsem zvolil zařízení firmy Cisco s označením Aironet 1240AG Serie.



zdroj: www.cisco.com

Obr. 16 - Cisco Aironet 1240AG Serie

Toto zařízení podporuje všechny tři standardy WiFi – IEEE 802.11a/b/g. Má velmi propracované bezpečnostní funkce, podporuje IEEE 802.11i. Samozřejmostí je podpora standardu IEEE 802.11e – v podobě WMM-PS.

Parametry přístupového bodu Cisco Aironet 1240AG Serie:

Rozhraní	IEEE 802.11a, 802.11b a 802.11g
Podporované rychlosti přenosu	802.11a: 6, 9, 12, 18, 24, 36, 48 a 54 Mbit/s 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 a 54 Mbit/s
Bezpečnost	802.11i, WPA2, WPA 802.1X AES, TKIP
Paměť	32 MB RAM 16 MB flash
Anténní konektory	Duální RP-TNC konektory
Teplota prostředí	Neprovozní (skladovací) teplota: –40 až 85°C Provozní teplota: –20 až 55°C Provozní vlhkost: 10 až 90 procent (nekondenzující)

Napájení	Místní napájení 802.3 AF Cisco vysokonapěťové přepínače schopné nabídnout 13W nebo více Cisco Aironet napájecí injektory (PWRINJ3 a PWRINJ-FIB) Cizí PoE zařízení s odpovídajícími parametry
Rozměry	16,76 x 21,59 x 2,79 cm

Tab. 8 - Parametry přístupového bodu Cisco Aironet 1240AG Serie

Tento access point je určen pro indoor použití, ale lze jej použít i ve venkovním prostředí. Na následujícím obrázku je ukázána možnost jeho instalace pro venkovní prostředí do plastového boxu.



zdroj: www.hyperlinktech.com

Obr. 17 - Instalace Cisco Aironet 1240AG Serie do plastového boxu pro venkovní použití

Již jsem zmiňoval použití sektorových antén. Mezi vhodné přichází například profesionální antény firmy Pacific Wireless (PW) SA58-90-17-WB a SA58-120-16-WB.

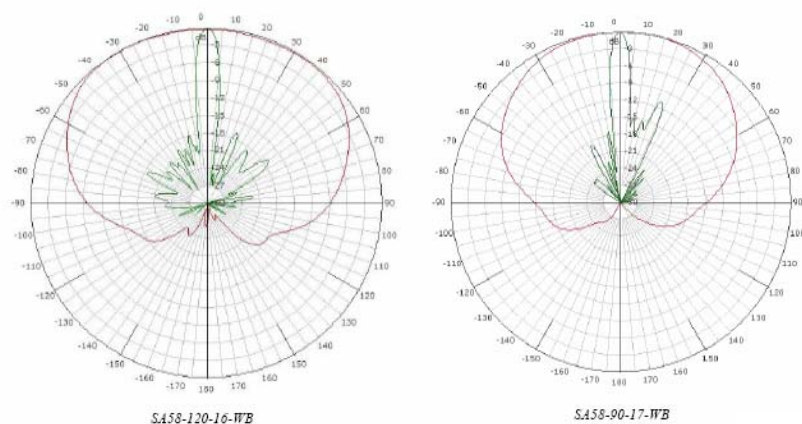
Frekvenční rozsah	5470 – 5850 MHz	
Hmotnost	1,2 kg	
Polarizace	Vertikální	
Rozměr	545 x 125 x 71 mm	
Provozní teplota	– 40 až + 70 °C	
VSWR	1,5:1	
Zisk antény	17 dBi	16 dBi
Vyzařovací úhel horizontální	90°	120°
Vyzařovací úhel vertikální	7°	7°

Tab. 9 - Parametry antén PW SA58-90-17-WB a SA58-120-16-WB



zdroj: www.pacwireless.com

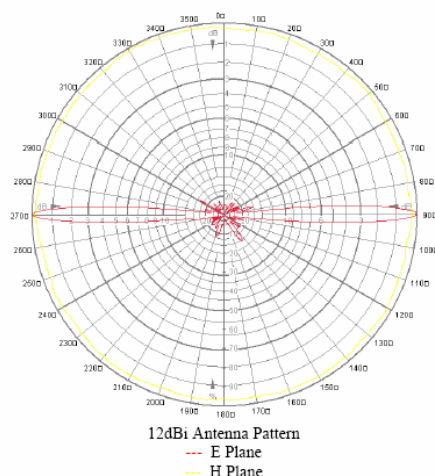
Obr. 18 - Anténa PW SA58-120-16



zdroj: www.pacwireless.com

Obr. 19 - Vyzářovací diagramy antén PW SA58-120-16WB a SA58-90-17-WB

Pro vozidlo je nutná všesměrová anténa, případně vhodná kombinace několika sektorových antén. Je třeba zajistit, aby vozidlo mělo signál při všech možných úhlech jeho natočení od vysílače. K dispozici je opět profesionální anténa značky Pacific Wireless, konkrétně PW OD58-12 s vertikální polarizací a ziskem 12 dB.



zdroj: www.pacwireless.com

Obr. 20 - Všeměrová anténa PW OD58-12 a její vyzářovací diagram

Jako OBU jednotka do vozidel je použito zařízení typu CarPC, které nemá možnosti rozšíření pomocí Mini-PCI nebo PCMCIA karty. Proto je nutné zvolit systém, který bude komunikovat přes rozhraní, které CarPC obsahuje, a to tedy přes USB nebo LAN. Jelikož není USB adaptér podporující zároveň standard 802.11a, WMM a možnost připojení externí antény, je nutno zvolit mezi variantou access pointu umístěného ve vozidle, nebo je zde případně ještě možnost osadit vozidlo další jednotkou, a to sice zařízením typu WRAP či MIKROTIK a toto zařízení vybavit kompatibilní Mini-PCI kartou,

kteřá je dostupná a poměrně levná. Tato varianta je složitější, nicméně nabízí větší prostor pro nastavení parametrů WiFi karty a je ekonomicky výhodnější než použití stejných access pointů na vysílače i přijímače. Bylo by vhodné otestovat i levnější access pointy pro funkci klienta ve vozidlech.

6.3. Zhodnocení návrhu

6.3.1. Ekonomické zhodnocení

Návrh byl poměrně konkrétní a tak lze stanovit náklady spojené s vybudováním tohoto systému. Ceny jsou získány z internetových obchodů nalezených vyhledávačem Google. Ceny profesionálních access pointů se pohybují od 22 000 Kč do 32 000 Kč. Cena zvoleného access pointu Cisco Aironet 1240AG Serie se pohybuje kolem 25 000 Kč. Ceny sektorových antén jsou stejné, jedna stojí přibližně 4400 Kč. Teď máme základní informace nutné pro výpočet nákladů na vysílací část řešení. Náklady na technické vybavení tedy budou následující.

$$n_{tech} = 18 \cdot 4400 + 18 \cdot 25000 + 18 \cdot 1500 = \underline{556200Kč} \quad (17)$$

1500 Kč je cena za konektory, kabely, izolaci, přepěťovou ochranu atd. připadající na jeden vysílač. K těmto nákladům je nutno připočítat náklady na samotné vybudování sítě, především spojené se samotnou instalací a konfigurací zařízení. Dále je třeba započíst řízené přepínače, které bude třeba pořídit (orientační cena jednoho řízeného přepínače s 12/13 se pohybuje kolem 20 000 Kč) a případné dobudování síťové infrastruktury letiště. Dostáváme se na částku blížíci se 1 000 000 Kč.

Jako částečně proměnné jsou náklady na technické vybavení vozidel, nebo-li klientskou část řešení, kde by záleželo na výsledcích testů zařízení. Pro příjem lze použít stejný access point jako vysílací (25 000Kč), lze použít low-end access point (například Compex WP-54AG-A13ER – 3 700Kč), nebo lze použít WRAP s Mini-PCI kartou (WRAP/ALIX 1B2 LX800/256 MB s Intel PRO/Wireless 3945ABG – 5 600 Kč). Všeměřová anténa PW OD58-12 stojí 2300Kč. Dále záleží na počtu vozidel vybavených tímto systémem. Pokud budeme předpokládat 50 vozidel, dostaneme se k následujícím nákladům.

$$n_{k \min} = 50 \cdot 3700 + 50 \cdot 2300 + 50 \cdot 1500 = \underline{375000Kč} \quad (18)$$

$$n_{k \max} = 50 \cdot 25000 + 50 \cdot 2300 + 50 \cdot 1500 = \underline{1440000Kč} \quad (19)$$

Pokud by systém pracoval korektně i s low-endovými zařízeními, je možno ušetřit přes 1 000 000 Kč a celkové náklady by činily cca **1 400 000 Kč**. Pokud by naopak systém fungoval pouze s profesionálním zařízením typu Cisco Aironet 1240AG Serie, cena celého projektu by se dostala na částku téměř **2 400 000 Kč**. Je možné snažit se hledat kompromis s celkovými náklady kolem **1 700 000 Kč**.

Pokud bychom se ohlédli na technologii WiMax a chtěli bychom s ní realizovat stejné pokrytí, dostáváme se do neurčitých čísel, jelikož WiMax bude na letišti vybudován jako nosná služba a OBU jednotky budou na příjem jeho signálu vybaveny. Pro „doplňkové“ pokrytí oblasti v okolí hangáru na terminálu jih tak není nutno počítat s klientskou částí nákladů. Dále vzhledem k možnosti technologie WiMax NLOS by pravděpodobně nebylo zapotřebí takového počtu přístupových bodů ani tolik vysílačů. Nicméně i tak jsou náklady na WiMax stále vyšší než na WiFi alternativu. Kompletní základnové stanice pro srovnatelné pokrytí by nás vyšly přibližně na podobnou částku jako kompromisní řešení návrhu WiFi systému, tedy kolem **1 700 000 Kč**. Bohužel by ovšem nebyl pokryt vnitřek hangárů. U WiMaxu se navíc platí i za licencované pásmo, tato částka je ročně kolem 30 000 Kč za jeden kanál. Nesmíme zapomenout, že není započítána klientská část zařízení, která naopak ve WiFi návrhu započítána je. Cena WiFi řešení bez klientské části se pohybovala kolem **1 000 000 Kč**. Zvýšením počtu WiFi přípojných míst v areálu letiště by tak došlo ke snížení procenta nákladů na klientská zařízení a zároveň by došlo i k jejich většímu využití. Ceny jsou pouze orientační, při jednáních s dodavatelskými firmami by se jistě nechal nalézt prostor pro jistou úpravu cen.

6.3.2. Technické zhodnocení

Dostupná technologie WiFi s implementací standardu IEEE 802.11e označenou jako WMM-PS nabízí možnost přenosu dat s prioritou bez další parametrizace přenosu. Stále se jedná o systém založený na kolizním protokolu v bezlicenčním pásmu, tudíž přenos dat nelze dostatečně garantovat. Pokud se v návrhu soustředíme na oblast použití systému v uzavřených objektech typu hangáry, podzemní parkoviště, sklady

a podobně, kam se nedostane vnější signál, můžeme si dovolit garantovat jisté záruky QoS přenosu dat.

K dispozici jsou sofistikované profesionální access pointy, ale zároveň i méně sofistikované access pointy. Podstatný rozdíl je v jejich ceně a v možnostech takovýchto systémů. U méně sofistikovaných systémů může do jisté míry vspělost systému zajistit OBU jednotka, případně další dodatečná vozidlová jednotka.

6.3.3. Bezpečnostní zhodnocení

Z hlediska bezpečnosti systém přináší řadu rizik. Samotná komunikace se dá pohodlně zabezpečit šifrováním dle standardu IEEE 802.11i, který je v podstatě neprolomitelný. Problém nastává díky faktu, že WiFi pracuje na sdíleném pásmu a že patří mezi rozšířené systémy. Rizikem tak může být přítomnost lidí se zřízením umožňující komunikaci tímto standardem. Může tak dojít k rušení, změně přenosových parametrů a to může vést až k selhání systému. Systém je tedy možné snadno zarušit, proto je systém vhodný do oblastí, kam se běžný člověk nedostane a nemůže tak tedy narušit bezpečnost systému. Pokud by se jednalo o úmyslné zarušení, má to narušitel snadnější díky dostupnosti zařízení, nicméně pokud to bude úmysl, je možné zarušit i technologii WiMax.

6.3.4. Diskuse

Doplňkové řešení technologií WiFi je tedy levnější než technologií WiMax, ovšem rozdíl není tak velký jak jsem očekával. Cílem není ovšem porovnávat jednotlivé technologie, ale navrhnout hybridní řešení zajišťující komplexní pokrytí prostor letiště pro zajištění telekomunikační služby pro přenos informací o polohách vozidel.

Nosná technologie WiMax má výborné parametry i v oblasti šíření signálu, přesto ovšem nelze pokrýt všechny prostory. Pro prostory v „ostatní“ oblasti nepokryté nosnou technologií je vhodné realizovat řešení na bázi IEEE 802.11, pokud bude řešení splňovat požadavky jak technické tak bezpečnostní.

7. Závěr

V práci byla zhodnocena technologie WiFi z pohledu aplikovatelnosti v ITS. Jsou zde snahy zajistit parametry potřebné pro většinu profesionálních ITS aplikací. Důležitý je doplněk 802.11e, jehož hlavním přínosem je zajištění garance kvality služeb v technologii WiFi. Implementace WMM-SA má nabídnout komplexní sadu parametrizovaných služeb QoS pro přenos dat. Bohužel tato verze není stále dostupná a tak je k dispozici implementace tohoto standardu s označením WMM a WMM-PS. Tyto implementace podporují pouze upřednostňování provozu dle tříd služeb. Stále se tedy jedná o systém založený na kolizním přístupu a je otázka, jak se systém bude chovat v reálném provozu. Proto by bylo vhodné provést provozní test systému s dostupnou technologií, například dle mého návrhu jako součást řešení projektu monitorování objektů na pohybové ploše letiště.

Systém založený na standardu 802.11 skýtá určitý potenciál, má své výhody i nevýhody a záleží na požadavcích na konkrétní řešení. Pokusil jsem se o návrh řešení pomocí této technologie v rámci projektu Monitorování a řízení pohybu objektů po ploše letiště pomocí GNSS (Grant MDS 802/210/112) v rámci účasti České republiky v projektu Galileo a ve výsledku je vidět, že systém lze pravděpodobně bez komplikací použít v uzavřených prostorách letiště, kde nehrozí narušení přenosu, a za jistých podmínek i v okolí budov. Systém je levnější než obdobný systém založený na technologii WiMax, ovšem stále je poměrně nákladný. Při použití tohoto systému a vybavení všech vozidel kompatibilní jednotkou pro příjem signálu se pak už vyplatí pokrýt co nejvíce prostor s odpovídajícími systémovými požadavky. Jelikož je systém postaven na bezlicenčním pásmu, je možná jeho aplikace téměř okamžitě na rozdíl od WiMaxu, kde je třeba vyřizovat licence pro používání, a systém je tak vhodný jako okamžitá náhrada či záloha za jiný systém.

Své uplatnění může technologie nalézt u jiných ITS aplikací, kde není kladen takový důraz na jednotlivé performační indikátory, nevadí občasné přerušení toku dat, případně vyšší doba zpoždění. U této WiFi technologie lze očekávat výrazný pokles cen na rozdíl od vývoje cen robustnější technologie WiMax. Bylo by vhodné zajímat se touto technologií i nadále a provést několik testů dostupné technologie v rámci některých projektů, které provádí naše fakulta a zhodnotit praktické výsledky testů.

8. Seznam použitých zdrojů

8.1. Literatura

- [1] Vodrážka, J.: *Přenosové systémy v přístupové síti*, ČVUT v Praze, 2006
- [2] Hanus, S.: *Bezdrátové a mobilní komunikace*, VUT Brno a Ústav Radiotechniky, Brno, 2003
- [3] Pužmanová, R.: *Širokopásmový Internet: Přístupové a domácí sítě*, Computer Press, Brno, 2004
- [4] Zelinka, T.: *Komunikační řešení dopravních telematických systémů*, Praha, 2006
- [5] Svítek, M.: *Intelligent Transport Systems – Architecture, Design methodology and Practical Implementation, Key-note lesson, 5th WSEAS/IASME Int. Conf. on systems Theory and Scientific Computation*, Malta, 2005
- [6] Svítek, M. – Zelinka, T.: *Communications Solutions for ITS Telematic Subsystems WSEAS Transactions on Business and Economics Issue 4 (2006), Vol. 3*, ISBN 1109–9526
- [7] Svítek, M. – Zelinka, T.: *Nové směry v telekomunikačních řešeních pro telematiku, Sborník přednášek konference TELEMATIKA pro regionální dopravu 2006*, Brno, 2006
- [8] Svítek, M. – Zelinka, T.: *Communication solution for Vehicles Navigation on the Airport territory. Proceedings of IEEE Intelligent Transport Systems Society Conference*, Istanbul, 2007
- [9] Zelinka, T. – Svítek, M.: *CALM – Telecommunication Environment for Transport Telematics. Technology & Prosperity, 2006, Vol. XI, special edition (11/06)*, ISSN 1213-7162.
- [10] Svítek, M. – Zelinka, T. a další: *WiMax v projektu „Monitorování a řízení pohybu pohyblivých objektů po pohybové ploše letiště“ Závěrečná zpráva*, Praha, 2007
- [11] Svítek, M. – Tvrzký, T. a další: *WiMax v projektu „Monitorování a řízení pohybu pohyblivých objektů po pohybové ploše letiště“ Závěrečná zpráva*, Praha, 2003
- [12] IEEE 802.11e, *IEEE Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements*, 2005

- [13] IEEE 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999

8.2. Internetové odkazy

- [14] www.lupa.cz
[15] www.internetprovsechny.cz
[16] www.ctu.cz
[17] www.automatizace.cz
[18] www.intelek.cz
[19] www.wi-fi.org
[20] www.ieee802.org
[21] www.connect.zive.cz
[22] www.telnet.cz
[23] www.wikipedia.org
[24] www.earchiv.cz
[25] 802.11b.cz
[26] www.svetsiti.cz
[27] www.hw.cz
[28] access.feld.cvut.cz
[29] www.pan.wz.cz
[30] www.comtel.cz
[31] tomas.richtr.cz/mobil
[32] www.mobilmania.cz
[33] www.mobil.cz
[34] www.computerworld.cz
[35] www.klfree.net
[36] www.ikaros.cz
[37] www.wimax.cz
[38] www.marigold.cz
[39] www.wi-fiplanet.com
[40] www.cs.ucsd.edu