

Bezdrôtová komunikácia v priemysle

Jedným z fenoménov dneška je určite bezdrôtová komunikácia. Každý sa už stretol s nejakou jej formou a drvivá väčšina z nás ju aj vo veľkej miere používa. Mobilný telefón, bezdrôtová klávesnica alebo tlačiareň, GPS prijímač a mnoho iných zariadení sú dnes už samozrejmosťou. Káble sú už záťažou. Ťahúňom vo vývoji sú hlavne kancelárie a domáci používatelia. Ako je to však s bezdrôtovými komunikáciami v priemysle? Medzi najpoužívanejšie bezdrôtové technológie sa dnes radí GSM/GPRS/UMTS, WiFi/WLAN, Bluetooth.

GSM/GPRS/UMTS

GSM (Global System for Mobile communications, pôvodne z francúzskeho Groupe Spécial Mobile) je najpopulárnejší štandard pre mobilné telefóny na celom svete. Od svojich predchodcov sa výrazne líši tým, že signálne aj hlasové kanály sú digitálne. Je to bunková sieť (cellular network), čo znamená, že mobilné telefóny (mobilné zariadenia) sa pripájajú do siete prostredníctvom buniek v najbližšom okolí. Sieť GSM operuje v niekoľkých frekvenčných rozsahoch. Najpoužívanejšie sú pásma 900 a 1 800 MHz. V niektorých krajinách v Amerike vrátane USA a Kanady sa používajú pásma 850 a 1 900 MHz, pretože 900 a 1 800 MHz už boli obsadené. Služby zahrnuté v GSM štandarde sú: CSD, SMS, MMS, FAX, GPRS.

CSD (Circuit Switched Data) slúži na prenos dát rýchlosťou od 2 400 bit/s do 14,4 kbit/s v závislosti od protokolu. Pri spojení prostredníctvom CSD sa vytvorí spojenie, ktoré rezervuje celú šírku pásma na danom spojení, až kým sa spojenie neukončí.

SMS (Short Message Service) je druhou najpoužívanejšou službou hneď po telefonovaní a stala sa populárnou rovnako v súkromnom, ako aj profesionálnom použití.

MMS (Multimedia Messaging Service) pracuje na podobnom princípe ako SMS, ale umožňuje posielat obrázky, animácie, hudbu alebo dlhé textové správy.

GPRS (General Packet Radio Service) je rozšírením GSM, pri ktorom využívajú dátové kanály GSM súbežne viacerí účastníci. V tom je zásadný rozdiel oproti službe CSD. Každý kanál, ktorý nie je obsadený, je k dispozícii na prenos dát. Týmto sa dosiahne lepšie využitie kapacity siete. Teoretická prenosová rýchlosť GPRS je 115,2 kbit/s, skutočná sa však pohybuje v rozsahu od 20 do 50 kbit/s a závisí od viacerých faktorov (operátora, terminálu, počtu používateľov na tej istej bunke, pohybu zariadenia ap.).

Existujú tri triedy GPRS pripojenia, ktoré sa od seba líšia. Sú zadefinované ako trieda A, B a C. Rozdiely medzi jednotlivými triedami opisuje tab. 1. Rýchlosť GPRS priamo závisí od počtu pridelených timeslotov pre uplink a downlink. Mobilné zariadenia sa potom podľa toho, ako sú

| | |
|----------|---|
| Trieda A | podporuje simultánne GSM a GPRS operácie |
| Trieda B | podporuje GSM aj GPRS operácie, ale nie simultánne |
| Trieda C | podporuje iba GPRS alebo GSM. Keď treba prepnúť medzi GPRS a GSM, treba zrušiť spojenie a znovu sa pripojiť |

Tab.1 Triedy GPRS

| Trieda | Downlink sloty | Uplink sloty | Aktívne sloty |
|--------|----------------|--------------|---------------|
| 1 | 1 | 1 | 2 |
| 2 | 2 | 1 | 3 |
| 3 | 2 | 2 | 3 |
| 4 | 3 | 1 | 4 |
| 5 | 2 | 2 | 4 |
| 6 | 3 | 2 | 4 |
| 7 | 3 | 3 | 4 |
| 8 | 4 | 1 | 5 |
| 9 | 3 | 2 | 5 |
| 10 | 4 | 2 | 5 |
| 11 | 4 | 3 | 5 |
| 12 | 4 | 4 | 5 |
| 32 | 5 | 3 | 6 |

Najbežnejšie používanými triedami sú triedy 2, 4, 6, 8, 10

Tab.2 GPRS triedy multislot

| kódovacia schéma | rýchlosť (kbit/s) |
|------------------|-------------------|
| CS-1 | 8,0 |
| CS-2 | 12,0 |
| CS-3 | 14,4 |
| CS-4 | 20,0 |

Tab.3 Kódovacie schémy GPRS

schopné využívať pridelené timesloty radia do niekoľkých tried nazývaných „multislot class“.

Rýchlosť GPRS závisí aj od použitej kódovacej schémy. Používajú sa 4 typy kódovacích schém. Najrýchlejšia kódovacia schéma sa používa v blízkosti prenášača signálu (BTS – Base Transceiver Station). Čím ďalej je mobilné zariadenie od BTS, tým menšia je prenosová rýchlosť a najnižšia je pri kódovacej schéme CS-1. Touto schémou je pokryté najväčšie územie. Nie je podmienkou používať všetky kódovacie schémy, preto to ani všetci operátori nerobia.

UMTS (Universal Mobile Telecommunications System) tiež označované aj ako 3G je štandard tretej generácie mobilnej telefónie. Základný rozdiel medzi 3G a GSM je prenosová kapacita, čo znamená rýchlosť, akou môžu byť dáta posielané a prijímané prostredníctvom telefónu. Čím vyššia je prenosová rýchlosť, tým väčšie využitie získa mobilná sieť. Rýchlosť je mnohonásobne vyššia ako pri GSM a to umožňuje prenos pohyblivých obrázkov, filmov a mnoho iných služieb. UMTS sa stále ďalej rozvíja.

Najdôležitejšími zabezpečovacími mechanizmami v sieťach GSM sú:

- autentifikácia používateľov (sieť autentifikuje SIM kartu, SIM karta autentifikuje používateľa pomocou PIN kódu),
- ochrana proti odpočúvaniu dát a signálu na rádiovom rozhraní,
- kontrola identity jednotky, v prípade straty môže byť zablokovaná.

Rádiokomunikácie

Oproti klasickým drôtovým komunikáciám sa táto technológia veľmi odlišuje v plánovaní, rozsahu a v spôsobe, akým sa musí vyrovnáť s rušením a šumom.

Ide o bezdrôtovú dátovú komunikáciu prostredníctvom rádiomodemu, ktorý prevádza dátový signál na rádiové vlny pre daný kanál s určeným vlnovým rozsahom. Dátový signál môže vyžadovať určitú formu spracovania signálu alebo filtrácie ešte predtým, ako bude prevedený na rádiový signál. Potom je signál modulovaný na potrebnú prenosovú frekvenciu a môže byť prenášaný rádiovou linkou k prijímaču. Bez ohľadu na to, či je zdroj dát analógový alebo digitálny, prenos je takmer vždy analógový. Prijímač prijme signál a potom ho dekoduje do pôvodného stavu. Frekvencie, ktoré sa môžu použiť na tieto účely, sú vyhradené príslušným úradom v každej krajine. Na Slovensku je to Telekomunikačný úrad Slovenskej republiky (TÚSR), v Českej republike Český telekomunikačný úrad (ČTU).

Rádiové vlny sa šíria v atmosfére vo vrstve medzi ionosférou a zemským povrchom. Podmienky na komunikáciu závisia od použitého frekvenčného pásma. Rádiomodemy pracujú v pásme UHF okolo 440 MHz. UHF pásmo medzi 300 a 3 000 MHz používajú aj radary, rádio, TV, NMT, GSM a bezdrôtové telefóny. Rádiové vlny sú ovplyvňované povrchom Zeme a vrstvami vzduchu, cez ktoré prechádzajú. Kopce, budovy a iné objekty tak môžu ovplyvniť kvalitu signálu. Signál, ktorý prijímač prijme, je tak veľmi často redukovaný oproti pôvodne vyslanému signálu, čo však nespôsobuje degradáciu signálu. Čo môže spôsobovať problém, je rušenie mimo našej kontroly, čiže šum, ktorý sa pripojí k signálu. Tento šum nevzniká len v použitých zariadeniach, ale môže ísť aj o tepelný šum, atmosférický šum, kozmický šum, lokálne generovaný šum pochádzajúci z elektrických zariadení v okolí.

Ak potrebujeme realizovať rádiovú sieť na väčšie vzdialenosti, ako nám umožňuje samotný rádiový modem, potrebujeme antény. Anténa je elektromechanické zariadenie, ktorého význam je vyslať, prijímať alebo šíriť signál. Anténa prevádza rádiový signál na elektromagnetické vlny.

Poznáme dva základné typy antén:

1. všesmerové – signál vysielajú všetkými smermi,
2. smerové – signál smerujú jedným smerom, čím sa značne predĺži vzdialenosť, na ktorú je anténa schopná signál preniesť.

Podľa potreby sa dajú antény spájať do takzvaného anténneho poľa, čo umožňuje pokryť signálom špecifickú oblasť územia. Priestorová spolupráca viacerých antén prispieva k smerovosti antény. Je veľa typov antén a ich výber závisí od konkrétnej aplikácie. Rovnako aj kmitočet, ktorý použijeme, musí vychádzať z podmienok konkrétnej aplikácie a požiadaviek zadávateľa.

Wi-Fi/WiMAX

Wi-Fi (WiFi) (najčastejšie sa vysvetľuje ako akronym „wireless fidelity“, ale začalo sa to jednoducho ako hra so skratkou „Hi-Fi“) je licencovaná ochranná známka Wi-Fi Alliance a je to súbor štandardov pre bezdrôtové lokálne siete založených na špecifikácii IEEE 802.11. Pôvodne sa Wi-Fi používalo na vzájomné prepojenie prenosných zariadení a počítačov na miestach, kde sa nedala vybudovať klasická káblová sieť, alebo tam, kde bola sieť len dočasná. Spočiatku boli rýchlosti prenosu dát cez Wi-Fi nízke. Za prudký rozmach a rozšírenie tejto technológie vďačíme aj spoločnosti Intel, ktorá ju integrovala do svojej mobilnej platformy Centrino. Aj vďaka tomu sa tak Wi-Fi stala štandardnou súčasťou prenosných počítačov. Rozšíreniu tiež pomohlo využitie nelicencovaného pásma, čo má však aj negatívne dôsledky hlavne v podobe veľké-

ho rušenia daného frekvenčného spektra. V tomto pásme vysielajú aj hromadné oznamovacie prostriedky a dokonca v ňom fungujú aj mikrovlnné rúry a iné spotrebiče.

Bezdrôtová sieť (WLAN – Wireless Local Area Network) môže byť vybudovaná rôznymi spôsobmi v závislosti od požadovanej funkcie. Kľúčovú úlohu zohráva identifikátor SSID (Service Set Identifier), čo je reťazec až 32 ASCII znakov, ktorými sa jednotlivé siete rozlišujú.

Sieť Ad-hoc je menej používaným spôsobom Wi-Fi. V Ad-hoc sieti sa spájajú dvaja klienti, ktorí sú rovnocenní (klient – klient). Vzájomná identifikácia prebieha pomocou SSID.

Typická Wi-Fi zostava obsahuje jeden alebo viac prístupových bodov (Access Point – AP) a jedného alebo viacerých klientov. AP vysielá svoj SSID každých 100 ms rýchlosťou 1 Mbps. To zaručuje, že klient prijímajúci signál z AP môže komunikovať rýchlosťou najmenej 1 Mbps. Viac AP môže vyslať rovnaký SSID a potom je len na používateľovi, ku ktorému sa pripojí (môže sa prepínať napríklad v závislosti od sily signálu).

Zabezpečenie Wi-Fi sietí je ovplyvnené hlavne tým, že na prenos signálu sa používa bezlicenčné pásmo, a potom aj tým, že signál sa šíri aj mimo zabezpečeného priestoru bez ohľadu na steny. Ako sa vyvíjal štandard Wi-Fi, vyvíjali sa aj spôsoby zabezpečenia. Dnes je možností niekoľko:

- Zablokovanie vysielania SSID. Porušuje to štandard, ale patrí medzi najjednoduchšie spôsoby zabezpečenia siete spôsobom zdanlivého skrytia. Toto zabezpečenie je však nedokonalé. Pri spájaní klienta s AP sa prenáša aj SSID v otvorenej podobe a dá sa zachytiť.
- Kontrola MAC adres. Funguje na princípe zadefinovania MAC adres, ktoré majú povolený prístup k AP. Dá sa to obísť tým, že útočník zistí MAC adresu, ktorá má povolený vstup, a potom sa bude vydávať za tú stanicu.
- WEP (Wired Equivalent Privacy). Šifrovanie komunikácie pomocou statických WEP kľúčov, ktoré treba ručne nastaviť na oboch stranách bezdrôtového spojenia. Vďaka nedostatkom v protokole sa dajú relativne ľahko získať. Existujú programy na tento účel.
- WPA a WPA2 (Wi-Fi Protected Access). Kvôli spätnej kompatibilite WPA využíva WEP kľúče, ktoré sú však dynamicky menené. Autentifikácia prístupu do WPA siete je realizovaná pomocou PSK (Pre-Shared Key – heslová fráza) alebo RADIUS (Remote Authentication Dial User Service – prihlasovanie meno a heslo). Novšia WPA2 prináša šifrovanie pomocou blokovej šifry AES (Advanced Encryption Standard), ktorá implementuje úplný štandard IEEE 802.11i. Tento štandard pozostáva z niekoľkých spôsobov autentifikácie.

V súčasnosti sú vyvinuté a schválené štyri variácie štandardu IEEE 802.11. Stručný prehľad je v tab. 4.

WiMAX (Worldwide Interoperability for Microwave Access) je relatívne nová širokopásmová bezdrôtová technológia založená na štandarde IEEE 802.16. Hlavným dôvodom vzniku tejto technológie je bezdrôtový prenos dát na veľké vzdialenosti. To je základný rozdiel oproti Wi-Fi (WLAN), s ktorou má inak veľmi veľa spoločného. Teoreticky možno dosiahnuť dosah v sieťach WiMAX až 70 km, ale vzhľadom na geografické a topografické podmienky je v praxi možný dosah do 10 km pri vonkajšej inštalácii klientskych antén a do 2 km pri vnútorných anténach.

Ďalšou výhodou oproti WLAN je využívanie výhradne licencovaného pásma a poskytovať takúto službu môže len oprávnený držiteľ licencie. Signál sa šíri pomocou básových staníc. Každá básová stanica má obmedzený počet účastníkov a po jeho dosiahnutí sa musí pridať ďalšia básová stanica. Každý klient má svoje vlastné koncové zariadenie

| špecifikácia | rýchlosť | frekvenčné pásmo | kompatibilita |
|--------------|------------|------------------|---------------|
| 802.11b | 11 Mbit/s | 2,4 GHz | b |
| 802.11a | 54 Mbit/s | 5 GHz | a |
| 802.11g | 54 Mbit/s | 2,4 GHz | b, g |
| 802.11n | 108 Mbit/s | 2,4 GHz | b, g, n |

Tab.4 Špecifikácie Wi-Fi

| trieda | maximálny odber | dosah (približný) |
|----------|-----------------|-------------------|
| Trieda 1 | 100 mW | ~100 metrov |
| Trieda 2 | 2,5 mW | ~10 metrov |
| Trieda 3 | 1 mW | ~1 meter |

Tab.5 Označenie výkonnosti Bluetooth zariadení

a nedochádza k využívaniu jedného pripojenia viacerými užívateľmi. V súčasnosti sú k dispozícii hlavne vonkajšie antény, najmenšia anténa do interiéru má veľkosť knihy. Na integrované antény v notebookoch a v počítačoch si ešte musíme minimálne rok počkať.

Bluetooth

Bluetooth je bezdrôtová komunikačná technológia na bezdrôtové prepojenie medzi dvoma a viacerými elektronickými zariadeniami (PDA, mobilný telefón, klávesnica, osobný počítač a pod.) na krátku vzdialenosť. Bluetooth necháva tieto zariadenia komunikovať medzi sebou, pokiaľ sú v dosahu signálu. Zariadenia nemusia na seba priamo vidieť a môžu sa nachádzať aj v iných miestnostiach tak ďaleko od seba, ako to umožňuje sila signálu. Výkonnosť Bluetooth zariadení sa označuje spôsobom uvedenom v tab. 5.

Technológia Bluetooth je definovaná štandardom IEEE 802.15.1. Spadá do kategórie osobných počítačových sietí, tzv. PAN (Personal Area Network). Operuje na frekvencii nelicencovaného pásma 2,45 GHz. Aby sa zabránilo rušeniu s inými typmi bezdrôtových komunikácií využívajúcich rovnaké pásmo, napríklad Wi-Fi, Bluetooth protokol rozdeľuje pásmo do 79 kanálov (každý so šírkou 1 MHz) a mení kanály až 1 600-krát za sekundu. Táto metóda sa volá Frequency-Hopping Spread-Spectrum (FHSS).

Bluetooth sa vyskytuje v niekoľkých vývojových verziách, z ktorých sa dnes najviac využíva verzia 1.2 implementovaná vo väčšine zariadení. Pred uvedením medzi štandard je verzia 2.1 a očakáva sa od nej zvýšenie prenosovej rýchlosti, možnosť získať viac údajov o pripájanom zariadení ešte skôr, ako sa potvrdí spojenie a zníženie spotreby. Očakáva sa aj zjednodušenie párovania zariadení a vyššia kvalita prenosu.

Bezpečnosť Bluetooth je postavená na autentifikácii a autorizácii pomocou kódu. Rozdielne úrovne zabezpečenia sú pre zariadenia a pre služby. Zariadenie môže byť dôveryhodné alebo nedôveryhodné. Dôveryhodné má prístup k službám v druhom zariadení. Služby majú tri úrovne zabezpečenia: služby vyžadujúce autorizáciu a autentifikáciu, služby vyžadujúce iba autentifikáciu a služby prístupné pre všetky zariadenia.

A ako prišla táto technológia k svojmu zaujímavému menu? Názov je odvodený z anglického mena dánskeho kráľa Haralda Modrozuba (Harald Bluetooth), vládnuceho v 10. storočí. Ten využil svoje diplomatické schopnosti na to, aby bojujúce kmene pristúpili k diskusii a ukončili vzájomné rozpory. Práve táto analógia sa využila pri určovaní názvu technológie Bluetooth, ktorá podobne slúži na zjednodušenie vzájomnej komunikácie medzi zariadeniami.

Využitie bezdrôtovej komunikácie v priemysle

Najväčšie využitie nachádzajú tieto technológie v telemetrii. Telemetria je definovaná ako automatická indikácia a riadenie procesov alebo zber dát zo vzdialene uskutočňovaných meraní.

Aj keď by sa mohlo zdať, že SMS je už dávno prekonané, stále sa používa. Hlavnými dôvodmi sú, že ako terminál môžete použiť akýkoľvek mobilný telefón. V priemysle sa využíva hlavne na diaľkové ovládanie a monitoring v neobsluhovaných technológiách, ako sú kotolne, vodárne, výmenníkové stanice, čerpacie stanice alebo malé elektrárne. V spojení so službou GPRS sa možnosti rozširujú o priame čítanie stavov analógových aj digitálnych vstupov a ovládanie výstupov, z ktorýchkoľvek počítača pripojeného na internet. To znamená, že už potrebujeme inteligentnejšie koncové zariadenie. Príklad konkrétneho využitia môže byť monitorovanie priestoru v nejakom vodnom hospodárstve. V prípade zatopenia sledovaného priestoru operátor na diaľku

dostane SMS správu s textom „zaplavene“. Jeho odpoveďou bude SMS správa s textom „cerpaj“, ktorá spustí čerpadlo. Rovnako môžu byť priebežne alebo ako alarmy v kritických stavoch zasielané informácie o teplote vody, tlaku, hladine a podobne. Pri využití GPRS má operátor možnosť prostredníctvom internetu okamžite zasiahnuť a odsledovať stavy na vstupoch a ihneď nastaviť adekvátne výstupy. Tým sa skraca reakčný čas a operátor má predsa len lepšiu predstavu o aktuálnom stave v monitorovanom priestore.

V spojení s GPS, čo je tiež jeden z ďalších spôsobov bezdrôtovej komunikácie, ale nebudeme ho tu bližšie rozoberať, sa dá GSM využiť aj na okamžité zistenie polohy vozidla alebo osoby. Stačí, aby bol v aute GPS prijímač a GSM terminál (telefón). Po zaslání špecifickej SMS správy na GSM terminál v aute by nám automaticky odpovedal SMS správou s udaním polohy, ktorú by získal z GPS zariadenia.

Ďalšie využitie ponúka Wi-Fi v spojení so zberom dát z mobilných zariadení uložených v autách. Typickým príkladom môže byť zber dát z meracích áut plynárov. Posádka auta vykoná potrebné merania a priebežné výsledky sa uložia do počítača v aute. Tento počítač je vybavený Wi-Fi kartou. V centrále je prístupový Wi-Fi bod, ktorý v okamihu, keď sa auto priblíži, nadviaže spojenie a automaticky stiahne dáta z auta. Možnosti využitia sú ďaleko väčšie. Rozširujú sa hlavne vďaka zvyšovaniu prenosovej rýchlosti Wi-Fi. To nám umožňuje prenášať stále väčšie množstvo dát. Preto už nie je problém preniesť videosegnál z kamery, umiestnenej vo vozidle, prípadne záznam z takejto kamery uložený na disku počítača v aute. Takéto využitie môže nájsť uplatnenie vo vozovom parku polície, zdravotníkov či hasičov.

Počítač vybavený bezdrôtovými technológiami umiestnený vo vozidle, môže byť použitý aj na komunikáciu s inými bezdrôtovými zariadeniami. Napríklad vozidlo hasičskej a záchranej služby by mohlo mať priamo vo vozidle počítač, ktorý by sa správal ako dohľadový systém. Zobrazoval a zaznamenával by obraz z bezdrôtových kamier, ktoré by mali na prilbách alebo na uniforme hasiči v teréne. Všetko by to sledoval veliaci celého zásahu a podľa presného obrazu o situácii každého člena zásahu, by mohol koordinovať celý zásah a tým zvýšiť efektivitu a rýchlosť zásahu. Po príchode na stanicu by takto získaný záznam mohli znovu analyzovať a prípadne vypracovať lepší plán pre ďalší podobný zásah.

Na záver veľmi stručne o ZigBee

Čo nás môže čakať už v blízkej budúcnosti, sú technológie, na ktorých sa už dlhší čas pracuje s väčšími či menšími úspechmi. Pre oblasť priemyslu a priemyselných aplikácií sa asi najviac očakáva skutočný príchod senzorových sietí. Sensory sú stále menšie a výkonnejšie a často musia pracovať na jednu batériu dlhé roky. Z toho vyplýva, že základom pre tieto siete je nízke napájanie. V tomto smere sa vyvíja štandard vychádzajúci z normy IEEE 802.15.4 a dostal názov ZigBee. Prezentuje sa aj ako doplnok k Bluetooth technológii. Hlavnými výhodami majú byť spoľahlivý prenos dát a už spomínaná veľmi nízka spotreba energie. Praktické využitie nájde v riadení budov, v telemetrii, v medicíne, riadení priemyselných procesov a podobne.

Výber vhodnej technológie závisí od aplikácie, ktorú ideme realizovať a od podmienok, ktoré nám dá zadávateľ. Každá technológia má svoje plusy a mínusy, a preto treba pri návrhu riešenia zobrať do úvahy všetky možnosti a zvážením výhod a nevýhod každej vybrať tú najvhodnejšiu.

Rastislav Tonka

e-mail: tonka@fccps.sk