Bezdrátová Bluetooth technologie

Ivo Penn

Katedra elektroniky a telekomunikační techniky, FEI, VŠB – Technická Univerzita Ostrava,
17. listopadu 15, 708 33, Ostrava-Poruba
penn.ivo@post.cz

Abstrakt. Trendem poslední doby v informačních a komunikačních technologiích se bezesporu stává mobilita. Proto vzniká řada nových bezdrátových technologií ve snaze zajistit komfortnější využití komplexních služeb, kvalitativně srovnatelných s technologií drátovou Technologie Bluetooth je jednou z nich. Základními požadavkemi je eliminace kabelů, podpora datové i hlasové komunikace, využívání možností ad hoc sítí, malá spotřeba energie a cenová dostupnost. Technologie Bluetooth využívá rádiových kmitočtů v celosvětové bezlicenčně dostupném pásmu 2,4 GHz a pro potlačení rušení používá přenos s rozprostřením signálu metodou FHSS s rychlostí 1600 skoků za sekundu. Přenosová kapacita Bluetooth je 1 Mbit/s a dosah až 100m.

Klíčová slova: Bluetooth, bezdrátové technologie, radiové technologie

1 Specifikace

Systémy Bluetooth se rozdělují podle tří základních funkčních bloků:

- *Bluetooth radio* – vysílač, přijímač, analogová radio-elektronika,
- *Bluetooth link controller* – řízení spojení, komunikace, přístupu, identifikace,
- *Bluetooth link manager* – příprava dat.

1.1 Bluetooth Radio (rádiová vrstva)

Bluetooth [BT] funguje v nelicencovaném frekvenčním pásmu 2,402-2,408 GHz technikou FHSS (frequency hopping system) na 79 kanálech, což je dostačující pro případnou kolizi, například s DECT paketem, který je obsluhován na stejném pásmu. Proti standardním systémům (DECT), kde se frekvence mění jednou za sekundu má fast hopping výhodu ve větší odolnosti proti rušení a větší bezpečnosti přenosu.
Radiový vysílač BT využívá GFSK (Gaussian Frequency Shift Keyng) modulaci. Podle vysílaného výkonu jsou zařízení BT rozdělena do tří pásem. Nominální výkon vysílače je 0 dBm pro dosah 10 cm až 10 m při 1 mW. Vyšší výkon, až 100 mW, což odpovídá 20 dBm, lze použít pro dosah až 100 metrů. Specifikace pro 4 dBm zatím nebyla komerčně uvedena. Celková přenosová kapacita prostřednictvím BT je 1 Mbit/s. Vzhledem k tomu, že se jedná o paketovou technologii, po odečtení dat fyzického protokolu a hlavičky se maximální přenosová rychlost sníží na 723 kbit/s. Tato kapacita může být staticky nebo dynamicky alokována (aplikační vrstva). [1,5]

1.2 Bluetooth Link Controller (Baseband)

Hlavními úkoly procesoru je administrace radiové vrstvy a „hopping“ algoritmu, oprava chyb, příprava dat, datové přenosy, zajištění hlasové a audio komunikace, datová bezpečnost, identifikace a šifrování. Data jsou přenášena duplexně v synchronním módu (SCO) určeném zejména pro hlasovou komunikaci ve třech kanálech s přenosovou rychlostí 64 kbit/s, nebo v asynchronním módu (ACL) s rychlostí pro nesymetrický přenos 721 kbit/s se zpětným kanálem 57,6 kbit/s, nebo 432,6 kbit/s v obou směrech pro symetrický přenos. Každý paket přitom nese informace o odesílateli, příjemci a způsobu komprese. Přenosový kanál je rozdělený do slotů, nominální délka slotu je 625µs. Pakety mohou být jak jednoslotové tak multislotové. Dvě anebo víc (maximálně 8) zařízení používajících stejný fyzický kanál vytvářejí pikosíť. V pikosíti je jedno ze zařízení master a ostatní jsou slave. Hopp-ovací postupnost je unikátní pro každou pikosíť a je daná hardware-ovou adresou (BD_ADDR) master zařízení. Všechna data jsou přenášena prostřednictvím paketů. Standard BT definuje 13 druhů paketů. [1,4,5,6]

Obr. 1. Bluetooth paket.

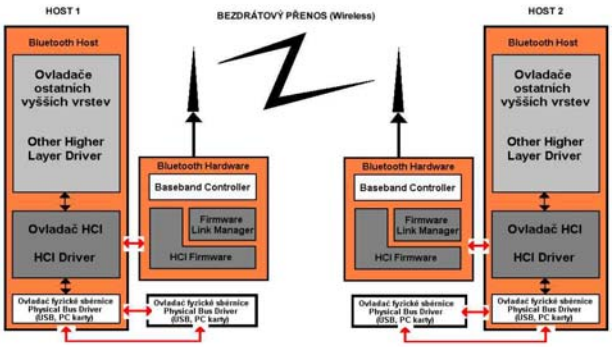
1.3 Link Manager Protocol

Link Manager zabezpečuje konfigurovaní linky, synchronizaci zařízení při vytváření spojení, autentifikaci zařízení na základě privátních klíčů s využitím metody výzva-odezva, šifrování spojení , detekci a korekci chyb a mnohé další funkce. Vyhledává v okolí jiné zařízení a komunikuje s jejich Link Managerem prostřednictvím Link Manager Protocol (LMP) a vytváří spojení . Na vykonávání jím poskytovaných služeb LM používá služby vrstvy Link Controlleru. [1,5]

1.4 Host Controller Interface (HCI)

HCI je rozhraní, které poskytuje uniformní přístup softwarové části protokolového zásobníku k fyzické části zařízení Bluetooth (hardware a firmware).

- *HCI firmware* - Nachází se v časti Bluetooth hardware. Implementuje HCI příkazy prostřednictvím příkazů Baseband a LM vrstvy, přístup k hardwarovým, stavovým a řídícím registrům a k registrům událostí.
- *HCI driver* - Nachází se v části Host (software). Zabezpečuje analýzu přijatých událostí, na základě kterých poskytuje informace vyšším vrstvám.
- *Host Controller Transport Layer (Physical Bus Driver)* - definuje několik různých způsobů komunikace: USB, UART a RS232. Tyto způsoby připojují hardwarové části Bluetooth zařízení k hlavnímu zařízení (HOST).

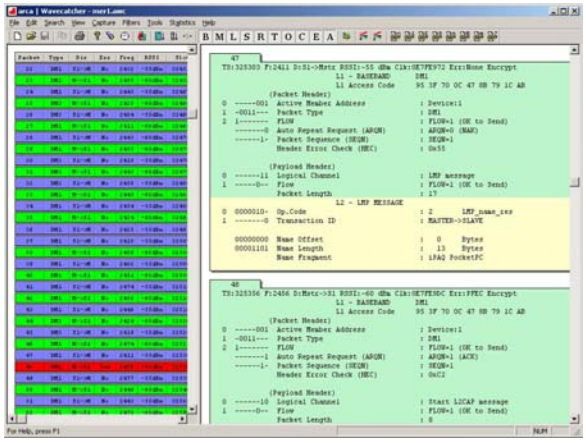


Obr. 2. Architektura HCI.

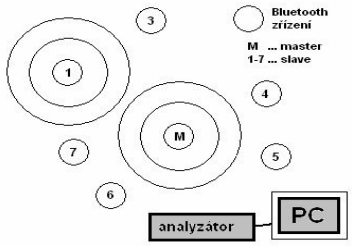
2 Analýza přenosu dat

V letošním roce byla krátkodobě na katedru zapůjčena zařízení, která již umožnila vytvoření modelové pikosítě pro praktické měření a vyhodnocování této technologie. Jednalo se nejenom o běžná koncová zařízení (mobily, PDA), ale také Bluetooth profilový simulátor firmy Arca, který dokáže velmi rychle a jednoduše generovat, testovat a analyzovat Bluetooth provoz (zastoupí i koncové zařízení), a Bluetooth protokolový analyzátor Arca, který zachycuje zprávy poslané mezi Bluetooth zařízeními, stahuje je a poskytuje detailní dekódování přenesených informací. Protokolový analyzátor analyzuje všechny základní Bluetooth protokoly. Tento přístroj se nejprve synchronizuje na zařízení Bluetooth, které je v módu master a pak monitoruje provoz. Je možno sledovat až 7 zařízení v módu slave.
Po aktivaci jednotlivých BT zařízení, je nutné vygenerovat provoz (např.: přenos dat), poté je tento provoz analyzátorem zachycen. Konkrétním výstupem je pak podrobný výpis všech paketů uskutečněné komunikace, které je dále možno zkoumat na základě rozdělení do jednotlivých vrstev či protokolů. Lze vysledovat statické informace přenosu, jako např. počet přenesených paketů, počet paketů různých protokolů nebo počet chybných paketů apod..
Vytvoření spojení mezi dvěmi zařízeními porbíhá pomocí dvou procedur. Procedura *inquiry* zabezpečuje nalezení okolních zařízení a výměnu jejich Bluetooth Device Address [BDA] (fyzická unikátní 48-bitová adresa) a stavu hodinových signálů. Procedura *page* pak slouží pro vytvoření spojení mezi dvěma zařízeními. Zpravidla následuje po proceduře *inquiry*, protože je pro její vykonání třeba znát BDA. Hodina hodinového signálu urychluje vytvoření spojení. Zařízení vyvolávající spojení pomocí procedury *page* se stává masterem.
Zařízení Bluetooth se může vyskytovat ve dvou základných stavech. Standby je počáteční stav zařízení Bluetooth s nízkou spotřebou energie, běží jen interní hodiny, neprobíhá komunikace s okolím. Ve stavu Connection je možné komunikovat s jiným BT zařízením též pikosítě. Zařízení ve stavu Connection může být pak v jednom ze čtyř módů:

- *Active* – V módě Active se zařízení Bluetooth aktivně zúčastňuje komunikace.
- *Hold* – Slave zařízení v tomto módě, udržuje synchronizaci s pikosítí pouze pomocí interních hodin.
- *Sniff* – Slave zařízení v tomto módě se synchronizuje s pikosítí se sníženou intenzitou.
- *Parked* – V tomto módě je slave zařízení stále synchronizované s pikosítí ale nezúčastňuje se aktivně na provozu. [5,6]



Obr. 3. Výpis obsahu paketů analyzátorem.



Obr. 4. Měřící pracoviště.

V letošním byl autorem podán rozvojový záměr Technologie Bluetooth v telekomunikačních systémech na vytvoření vzorové testovací pikosítě Bluetooth. Ta by měla umožnit provádět zkušební provoz a jeho monitoring pro stanovení spolehlivosti přenosu, stability a optimálních podmínek.

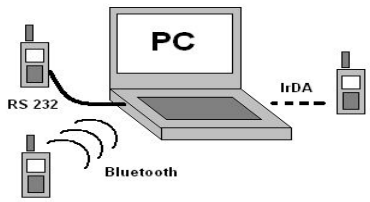
3 Bezpečnost

Nejnižší úroveň ochrany posílaných dat prostřednictvím technologie Bluetooth je její hardwarová specifikace. Z hlediska frekvence jí bezpečnost dostatečně zajišťuje technika „frequency hopping“ s rychlostí 1600 skoků za sekundu a s prodlevou 625 ěs, přičemž počet kanálů je 79. Již z tohoto hlediska je velice těžké tento signál odposlouchávat. Bluetooth zařízení mají navíc zabudovanou vnitřní bezpečnostní ochranu proti odposlechu a falsifikaci originálních dat. Svou roli také hraje udělený rozsah frekvenčního pásma. Aplikační neboli softwarovou ochranu dat je nutno rozdělit podle důležitosti těchto paketů. Aplikační systém je odolný proti vícenásobným cestám šíření a obsahuje korekci chyb až do BER<0,1% a enkrypci. Specifikace Bluetooth definuje 3 různé úrovně softwarového zabezpečení:

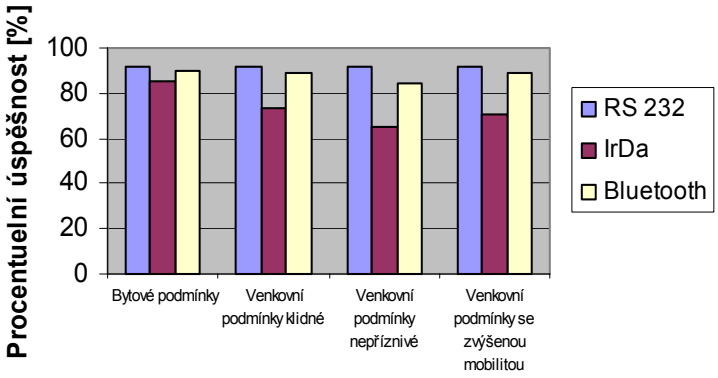
- *nedůležitá data (non-secure)* - nechráněná komunikace.
- *vyšší bezpečnost (autentizace)* - běžný způsob autentizace výzva–odezva zajišťuje, že každá uskutečněná komunikace je přesně adresována. Každý BT chipset má zakódovanou BDA, na základě které komunikuje s jinými přístroji. Jakmile dojde k nesrovnalosti adresy či jakémukoliv přerušení toku dat, komunikační kanál se neotevře a komunikace se přeruší.
- *důležitá data (autentizace + krytování)* - bezpečnost je zaručena vestavěnou podporou 128-bitového šifrovacího kódu. Tento šifrovací kód můžeme dále dělit podle dvou klíčů: *Private user key*, což je tajná entita získaná během inicializace, *Random number* – entita rozdílná pro každou novou transakci, získaná pseudo-náhodným procesem v Bluetooth jednotce. [2,3]

4 Měření GPRS

V měsících srpen a září byly ve spolupráci s firmou T-mobile prováděny testy kvality datových služeb GPRS. Vzhledem k tomu, že koncové zařízení zapůjčené pro provádění těchto testů umožňovalo přenos dat prostřednictvím Bluetooth technologie, bylo provedeno komparační sledování kvalitativních rozdílů využívání GPRS služeb pomocí RS 232 a Bluetooth. Tento test jednoznačně prokázal, že komerční využití technologie Bluetooth v mobilních zařízeních je krokem správným směrem. Stabilita a spolehlivost takto prováděných měření byla naprosto srovnatelná, což při nesrovnatelně větším komfortu využitelnosti technologie Bluetooth mluví jednoznačně v její prospěch.



Obr. 5. Schéma testovacího zapojení GPRS.



Obr. 6. Graf úspěšnosti spojení.

Reference

1. Penn I. Úvod do technologie Bluetooth. *V. Seminář katedry elektroniky a telekomunikační techniky*. Ostrava 2002. ISBN 80-248-0212-0.
2. Penn I. Bluetooth and Security. *ISMOT 2003 (9th Interbational Symposium on Microwave and Optical Technology)*. Ostrava 2003. ISBN 80-248-0355-0 (Book of abstracts). sborník v tisku.
3. Penn I. Security in Bluetooth and 802.11b technologies. *RTT 2003 (Research in Telecommunication Technology)*. Bratislava 2003. ISBN 80-227-1934-X.
4. Penn I. Bezdrátová rádiová technologie Bluetooth. *Workshop Radešín 2003*. sborník v tisku.
5. Bluetooth SIG. http://www.bluetooth.com/pdf/Bluetooth_11_Specifications_Book.pdf.
6. Palowireless. http://www.palowireless.com/bluearticles/softtooth.asp.

Annotation:

Wirelles Bluetooth Technology

Bluetooth is the new emerging technology for wireless communication. It can be used to connect almost any device to another device. Bluetooth uses the radio range of 2.45 GHz. The theoretical maximum bandwidth is 1 Mb/s, which is slowed down by Forward Error Correction (FEC). Bluetooth device (class A) has a range up to 100 meters. Bluetooth specification designates the frequency hopping to be implemented with Gaussian Frequency Shift Keying (GFSK). Bluetooth radio modules avoid interference from other signals by hopping to a new frequency (1600 hops/sec.) after transmitting or receiving a packet. Compared with other systems operating in the same frequency band, the Bluetooth radio typically hops faster and uses shorter packets. It limits the impact of sources of disturbances. Bluetooth has built in sufficient encryption and authentication and is thus very secure in any environment.