Bluetooth – vrstvy a protokoly

Úvod

V srpnovém čísle ST jsme se začali seznamovat s popisem vrstev systému Bluetooth. Nyní tento popis dokončíme a dále se budeme podrobněji zabývat protokolem správy spojení LMP (Link Manager Protocol), protokolem pro řízení a adaptaci spojení L2CAP (Logical Link Control and Adaptation Protocol), protokolem pro zjišťování služeb SDP (Service Discovery Protocol), protokolem pro řízení telefonie TCS (Telephony Control protocol Specification) a protokolem RFCOMM emulujícím sériové rozhraní RS232 podle specifikace ETSI TS 07.10 včetně dalších aplikací. Tak uzavřeme sérii článků věnovaných technologii Bluetooth.

Logické kanály

V systému Bluetooth je definováno pět logických kanálů. Dva z nich slouží pro řízení a správu spojení, tři pro přenos uživatelských dat. Jednotlivé kanály se podle své funkce nazývají:

- řídicí kanál pro řízení spojení – LC (Link Control),
- řídicí kanál správy spojení – LM (Link Manager),
- uživatelský kanál asynchronních dat – UA (User Asynchronous data),
- uživatelský kanál izochronních dat – UI (User Isochronous data),
- uživatelský kanál synchronních dat – US (User Synchronous data).

Kanál řízení spojení – LC

Kanál řízení spojení je mapován do hlaviček paketů a přenáší řídicí informace nízké úrovně, jako jsou například informace o doručení paketu ARQ, řízení toku FLOW a charakter uživatelských informací v informačním poli. Kanál LC je přenášen ve všech paketech kromě paketu ID, který nemá hlavičku.

Kanál správy spojení – LM

Kanál správy spojení přenáší informace, které si vyměňují správci spojení řídicí a podřízené jednotky. Většinou je pro tento kanál používán paket DM, který má vyšší stupeň zabezpečení. Kanál LM je indikován v hlavičce informačního pole správnou hodnotou v položce *L_CH* (kód 11).

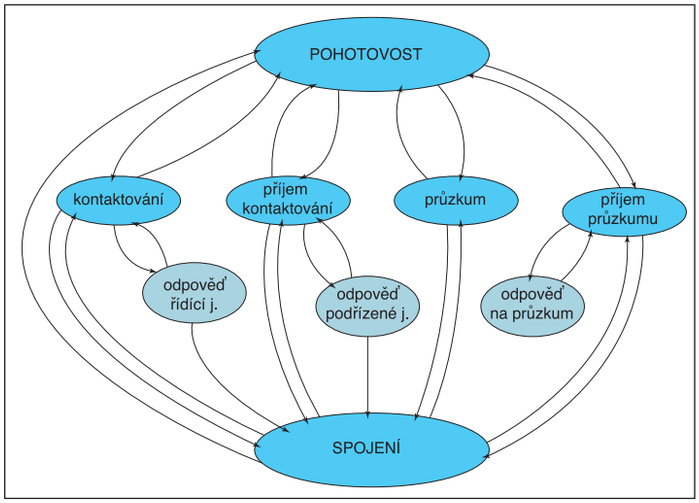
Kanál asynchronních/izochronních dat – UA/UI

Kanál UA transparentně přenáší asynchronní data vyšší vrstvy L2CAP. Pro přenos tohoto logického kanálu slouží pakety provozního kanálu ACL. Tato data mohou být přenášena v jednom nebo více paketech. Pokud je paket vyšší vrstvy přenášen ve více paketech, je první paket označen v hlavičce informačního pole v položce *L_CH* kódem 10, zbylé pakety pak hodnotou 01. Pokud se paket vyšší vrstvy vejde do jednoho paketu vrstvy baseband, pak je tento paket označen hodnotou 10.

Izochronní kanál je podporován vyšší vrstvou správným časováním okamžiků vysílání jednotlivých paketů. Pro ně platí na úrovni vrstvy baseband stejná pravidla jako pro pakety kanálu UA.

Kanál synchronních dat – US

Kanál US transparentně přenáší uživatelská synchronní data. Tento kanál je přenášen pakety provozního kanálu SCO.



Obr. 1 Schéma provozních stavů jednotky Bluetooth

Stavy jednotky Bluetooth

Výchozím stavem pro jednotku Bluetooth je stav pohotovosti (Standby). V tomto stavu fungují pouze vnitřní hodiny a jednotka má minimální spotřebu energie. Z tohoto stavu může přejít do jednoho z následujících stavů: průzkum (Inquiry), příjem průzkumu (Inquiry Scan), kontaktování (Page) a příjem kontaktování (Page Scan) – *obr. 1*.

Průzkum (Inquiry)

Během tohoto stavu prozkoumávající jednotka sbírá adresy a hodnoty vnitřních hodin odpovídajících jednotek, které se nacházejí v jejím okolí. Poté je možno s kteroukoli z takto objevených jednotek navázat spojení pomocí procedury kontaktování. Prozkoumávající jednotka průběžně vysílá průzkumnou zprávu prostřednictvím paketu ID na různých přeskokových frekvencích. Vzhledem k délce paketu ID je možné paket posílat dvakrát v jednom časovém úseku, každý na jiné přeskokové frekvenci podle sekvence pro průzkum. Podle toho, zda je paket adresován všem nebo jen vybraným jednotkám, obsahuje buď obecný přístupový kód GIAC (General Inquiry Access Code), nebo specializovaný přístupový kód DIAC (Dedicated Inquiry Access Code). Prohledá-vající jednotka opakovaně vysílá na šestnácti frekvencích, které tvoří průzkumnou skokovou sekvenci (train). Tyto průzkumné sekvence jsou dvě – A a B. Aby byly zachyceny odpovědi od všech jednotek, je nutné každou z těchto sekvencí projít 256× – za předpokladu, že v daném prostředí nedochází k výskytu chyb. Celkové potřebné množství času pro vykonání průzkumné sekvence je minimálně 10,24 s. Přítomnost provozních kanálů SCO může tento čas prodloužit. Pokud je zachyceno požadované množství odpovědí před koncem průzkumné procedury, může být procedura předčasně ukončena.

Příjem průzkumu (Inquiry Scan)

Pokud zařízení umožňuje identifikaci, periodicky vstupuje do stavu příjem průzkumu. V tomto stavu jednotka naslouchá na jedné vybrané frekvenci, aby z průzkumné skokové sekvence mohla zachytit kód odvozený z její BD-adresy. V tomto stavu zůstává dostatečně dlouho na to, aby nepropásla průzkumnou zprávu, která patří právě jí.

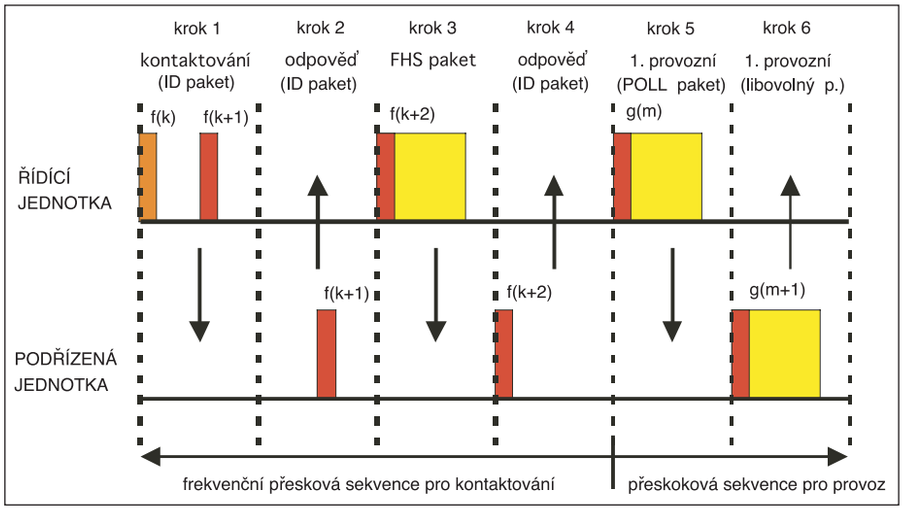
Odpověď na průzkum (Inquiry Response)

Když přijme zařízení, které je ve stavu příjmu průzkumu, průzkumnou zprávu, musí být odvysílána odpověď obsahující adresu jednotky a hodnotu vnitřních hodin. Tato zpráva však není odvysílána bezprostředně po příjmu zprávy, ale s vysíláním se počká náhodný počet časových úseků. To má zabránit případné kolizi s ostatními zařízeními, které přijímaly průzkumnou zprávu na stejné frekvenci. Po uplynutí stanoveného počtu časových úseků je prozkoumávající jednotce vyslán FHS-paket. Ten obsahuje všechny potřebné informace pro případné kontaktování. Po odvysílání FHS-paketu jednotka zůstává ve stavu příjmu průzkumu a nečeká na potvrzení vysla-ného paketu.

Kontaktování (Paging)

Do stavu kontaktování přechází řídicí jednotka tehdy, přeje-li si navázat spojení s jinou

jednotkou Bluetooth. Princip je velice podobný proceduře prohledávání, s tím rozdílem, že ID-paket obsahuje přístupový kód zařízení – DAC (Device Access Code), který je vypočten z adresy kontaktované jednotky. Z této adresy se také řídicí jednotka snaží odhadnout frekvenci, na které kontaktovaná jednotka přijímá. Tento odhad může být přesnější a proces kontaktování může být zkrácen, pokud je známa hodnota vnitřních hodin kontaktované jednotky. Tyto informace jsou získávány z procesu průzkumu, který většinou předchází proceduře kontaktování. Frekvenční skoková sekvence pro kontaktování obsahuje 32 frekvencí a je rozdělena do dvou skupin (trains) po 16 frekvencích. Sekvence *A* obsahuje frekvence z okolí očekávané frekvence a sekvence *B* obsahuje ostatní frekvence. Pokud odhad stavu hodin podřízené jednotky je v rozsahu 7×1,28 až 8×1,28 sekundy, odpoví spuštěním sekvence *A*, jinak odpoví spuštěním sekvence *B*. V prvním případě zabere kontaktování až 1,28 sekundy, v druhém případě až 2,56 sekundy.



Obr. 2 Průběh výměny zpráv při odpovědi podřízené jednotky na druhý kontaktovací paket

Příjem kontaktování (Page scan)

Do tohoto stavu může jednotka přejít buď ze stavu připojení, nebo ze stavu pohotovosti. V tomto stavu podřízená jednotka očekává ID-paket s odpovídajícím přístupovým kódem zařízení – DAC. Při vstupu do tohoto stavu je zvolena frekvence ze sekvence pro příjem kontaktování, na které jednotka poslouchá zvolenou dobu $T_{wpagescan}$. Tato doba by měla být delší než doba potřebná k průzkumu šestnácti frekvencí. Tyto doby jsou odděleny časovým intervalem $T_{wpagescan}$. Definovány jsou tři pevné hodnoty intervalu $T_{wpagescan}$. V případě nulové hodnoty se jedná o kontinuální příjem. Mohou být použity i jiné hodnoty než předdefinované, ale řídicí jednotka o tom musí být informována. To znamená, že při navazování prvního spojení musí být použita jedna ze standardních hodnot $T_{wpagescan}$.

Odpověď na kontaktování (Page response)

Při příjmu kontaktního ID-paketu podřízená jednotka přejde do stavu „odpověď na kontaktování“. V tomto stavu podřízená jednotka odešle ID-paket se svým přístupovým kódem DAC na stejné frekvenci v následujícím časovém úseku přesně 625 µs po přijetí kontaktního ID-paketu. Řídicí jednotka po příjmu této odpovědi přejde do stavu odpověď na kontaktování. V této chvíli již je řídicí jednotce známa frekvence, na které podřízená jednotka přijímala. V dalším kroku řídicí jednotka pošle podřízené jednotce pomocí paketu FHS informace o hodinách řídicí jednotky na frekvenci, která byla určena z předchozí odpovědi s použitím přístupového kódu DAC podřízené jednotky. Paket FHS také přiřazuje tříbitovou adresu aktivního člena *AM_ADDR*. Podřízená jednotka potvrdí příjem FHS-paketu paketem ID a použije přijatý FHS-paket pro určení přístupového kódu pikosítě, která byla právě vytvořena nebo do které podřízená jednotka právě vstoupila, a spočtení posunu vnitřních hodin pro správnou synchronizaci s frekvenční skokovou sekvencí řídicí jednotky. Další paket, zaslaný řídicí jednotkou podřízené jednotce, je paket POLL, který je již adresován pomocí adresy aktivního člena a je opatřen přístupovým kódem pro danou pikosíť na frekvenci skokové sekvence pro fyzický kanál. Podřízená jednotka musí na tento paket odpovědět jakýmkoli paketem (třeba paketem NULL, který obsahuje pouze hlavičku). Pokud všechny zmíněné procedury proběhnou bezchybně, jednotky přejdou do stavu připojení. Po vstupu do tohoto stavu si jednotky začnou vyměňovat informace pomocí protokolu pro správu spojení – LMP (Link Manager Protocol) za účelem vytvoření spojení. Uvedený postup je zobrazen na *obr. 2*.

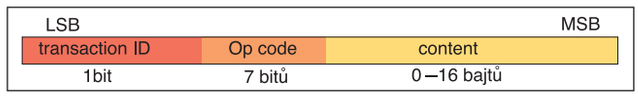
Režimy jednotky ve stavu připojení

Aktivní režim (Active mode)

Jednotka v aktivním režimu obsadí daný kanál. Řídicí jednotka plánuje jedno či obousměrný přenos dat podle požadavků různých podřízených jednotek, dále plánuje pravidelné přenosy pro udržení synchronizace podřízených jednotek s fyzickým kanálem. Aktivní podřízené jednotky poslouchají v časových úsecích určených pro provoz od řídicí jednotky, zda není pro ně přenášen paket. Pokud tomu tak není, nemusí neadresované jednotky naslouchat až do dalšího časového úseku vyhrazeného pro přenos ve směru od řídicí jednotky. Počet časových úseků se určí pomocí položky TYPE v hlavičce paketu. Periodický přenos za účelem synchronizace podřízené jednotky může být proveden pomocí libovolného paketu, protože podřízená jednotka k tomuto účelu potřebuje pouze přístupový kód kanálu.

Režim Sniff (Sniff mode)

V tomto režimu podřízená jednotka omezuje činnost naslouchání v časových štěrbinách podle aktivit řídicí jednotky. Toto opatření umožňuje snížit spotřebu energie dané podřízené jednotky. Podřízená jednotka, která se podílí na provozním kanálu ACL, musí naslouchat v každém časovém úseku, ve kterém začíná přenos od řídicí jednotky. V režimu sniff je množství časových úseků, ve kterých může řídicí jednotka komunikovat s danou podřízenou jednotkou, omezeno. A to tak, že řídicí jednotka může zahájit přenos pouze v určitých časových úsecích. Tyto časové úseky jsou rozmístěny pravidelně v intervalu T_{sniff}. Vstup a dohadování parametrů režimu sniff je zajištěno pomocí příkazů protokolu LMP.



Obr. 3 Informační pole paketu, ve kterém je přenášena zpráva LMP

Režim přidržení (Hold mode)

Během stavu připojení může být provozní kanál ACL uveden do režimu přidržení. To znamená, že daná podřízená jednotka dočasně nepodporuje pakety na provozním kanále ACL (provozní kanály SCO jsou i nadále podporovány). V režimu přidržení může být uvolněná kapacita využita pro jiné věci, jako je například průzkum, kontaktování a jejich příjem, či pro účast v jiné pikosíti. Tento režim může být využit i jako režim s nízkou spotřebou energie. Před vstupem do režimu přidržení se řídicí a podřízená jednotka dohodnou na délce jeho trvání. Po skončení dohodnutého časového intervalu podřízená jednotka přejde do aktivního režimu, syn-

chronizuje se na fyzický kanál a očekává instrukce od řídicí jednotky. Během režimu přidržení zůstává podřízené jednotce její *AM_ADDR*.

Režim parkování (Park mode)

Režim parkování je režim s nejnižší spotřebou energie a s nejmenší aktivitou podřízené jednotky. Kromě toho je tento režim použit k tomu, aby k jedné řídicí jednotce mohlo být připojeno více než sedm podřízených jednotek (počet je limitován velikostí *AM_ADDR*). Při vstupu do tohoto režimu odevzdá podřízená jednotka adresu aktivního člena *AM_ADDR* a dostane přiděleny dvě osmibitové adresy. Jednak je to adresa zaparkovaného člena *PM_ADDR* (Parked Member Address), která je použita řídicí jednotkou pro změnu režimu, a jednak adresa žádosti o přístup *AR_ADDR* (Access Request Address), která je použita podřízenou jednotkou pro žádost o změnu režimu. Podřízená jednotka v pravidelných intervalech poslouchá fyzický kanál za účelem synchronizace a sledování případných žádostí o změnu režimu.

Protokol správy spojení – LMP (Link Manager Protocol)

Zprávy protokolu správy spojení LMP slouží pro konfiguraci a řízení spojení i zabezpečení. Tyto zprávy jsou odfiltrovány a interpretovány správcem spojení na přijímací straně, takže se nešíří do vyšších vrstev.

Funkce LMP se dají rozdělit do několika oblastí:

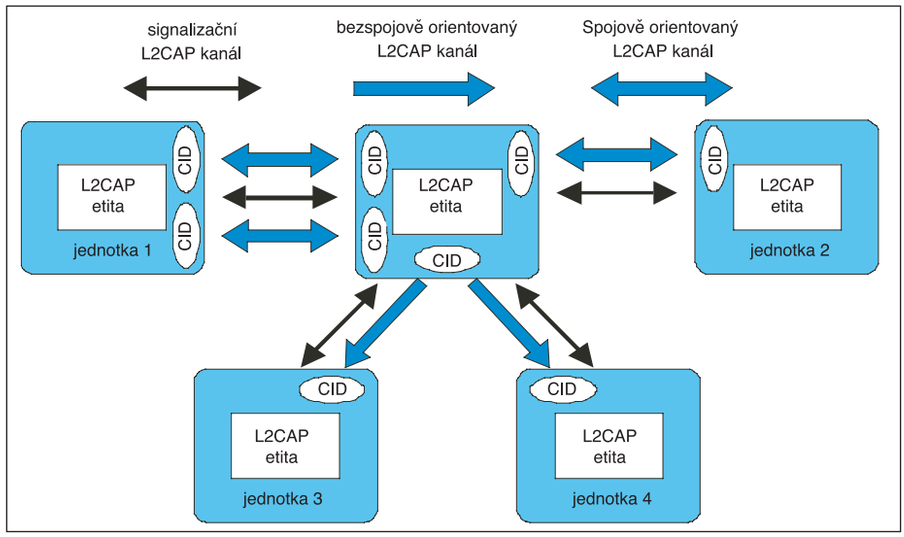
- správa spojení – množina funkcí, které mají za úkol sestavovat, spravovat a rušit spojení (ať již s provozem ACL či SCO),
- bezpečnostní management – řízení párování, výměna klíčů, autentizace, šifrování,
- management pikosítě – parametry časování, požadavky na jméno,
- konfigurace spojení – kontrola kvality spojení, volba vhodných typů paketů, řízení vysílacího výkonu – RSSI.

Pakety protokolu LMP jsou přenášeny v informačním poli místo paketů vrstvy L2CAP. Pakety LMP mají délku jednoho časového úseku a oproti paketům L2CAP mají vyšší prioritu, takže nejsou brzděny běžným provozem na kanálu. V rámci základní vrstvy jsou pakety LMP a L2CAP odlišeny jinou hodnotou položky *L_CH* v hlavičce informačního pole (pakety LMP mají hodnotu 11 b). Vlastní paket LMP se skládá ze tří částí (*obr. 3*):

- Transaction ID – jednobitová položka, která přenáší informaci o původu transakce (0 – transakci zahájila řídicí jednotka; 1 – transakci zahájila podřízená jednotka),
- operační znak (OpCode) – sedmibitová hodnota určující druh konkrétní zprávy,
- obsah (Content) – obsahuje parametry konkrétní zprávy, délka pole je závislá na tom, kolik parametrů má daná zpráva.

Protokol pro řízení a adaptaci logických spojení – L2CAP

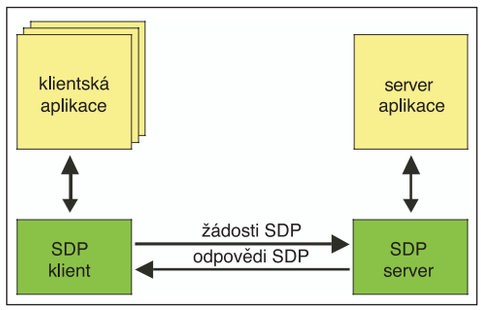
Protokol L2CAP (Logical Link Control and Adaptation Protocol) definuje spojení pouze pro provozní kanály ACL, kanály jsou určeny identifikátorem kanálu CID (Channel Identifier). Tyto kanály jsou analogií portů u protokolu TCP/IP, které tvoří společně s IP adresou socket. U L2CAP je kanál jednoznačně identifikován adresou zařízení, ke kterému je kanál veden, a právě identifikátorem kanálu, který je přidělen pro potřeby jedné aplikace. Každý z kanálů je plně duplexní s možností specifikace QoS pro každý směr přenosu. Dále je možné sestavovat spojení buď spojově orientované (tj. bod – bod), nebo nespojově orientované (čili bod – mnoho bodů) jak je vidět na *obr. 4*.



Obr. 4 L2CAP kanály mezi jednotkami

Spoj je datagramový, proto data pro provozní kanály SCO tohoto protokolu nevyužívají, ale jsou posílána přímo základní vrstvě. Pro žádost o spojení, konfiguraci, odpojení a testování je vždy sestaven zvláštní signalizační kanál, který má pevně přidělenu hodnotu identifikátoru kanálu. Pakety protokolu LCAP mají poměrně malý podíl služebních informací a neposkytují žádný mechanismus pro kontrolu a opravu chyb, protože tyto funkce jsou zajištěny nižšími vrstvami. Pro vyšší vrstvy protokol L2CAP poskytuje tyto funkce:

- rozdělování a spojování paketů vyšší vrstvy: velikost paketů základní vrstvy je limitována (např. pro paket DH5 je to 341 bajtů). L2CAP umožňuje přenos paketů o délce až 64 kB,
- multiplexování protokolů vyšších vrstev: L2CAP musí tuto funkci podporovat, protože nižší vrstvy neobsahují žádné identifikátory protokolu vyšší vrstvy (SDP, TCS, RFCOMM),
- kvalitu služby: při navazování spojení ve vrstvě L2CAP může být vyměněna informace o požadované kvalitě služby; protokol pak monitoruje prostředky a zajišťuje dodržení dohodnutých parametrů.



Obr. 5 Interakce mezi SDP-serverem a klientem

Protokol pro zjišťování služeb – SDP

Protokol pro zjišťování služeb SDP (Service Discovery Protocol) poskytuje aplikacím prostředky pro zjištění, jaké funkce jsou dostupné, a určení charakteristik těchto dostupných služeb. Jednotka Bluetooth, která dovoluje zjistit poskytované služby, se nazývá SDP-server, naopak jednotka zjišťující poskytované služby je SDP-klient. Na jedné jednotce může být provozováno několika aplikacemi několik SDP-klientů, avšak jen jeden SDP-server (*obr. 5*).

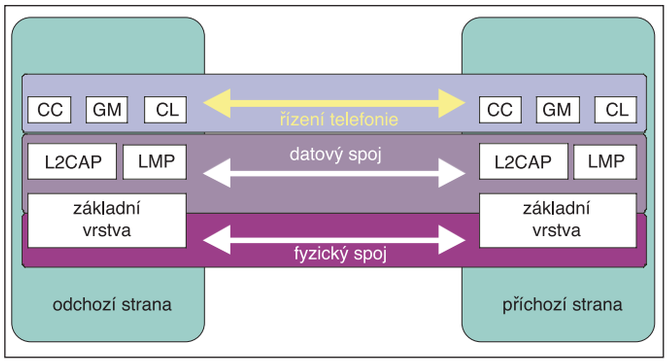
Server spravuje seznam záznamů o službách (service record), tyto záznamy popisují služby spojené se serverem. Každý záznam o službě obsahuje informace o jediné službě. Jednotlivé záznamy o službě jsou rozděleny na atributy služby (service attribute). Každý atribut služby popisuje jednu charakteristiku služby. Atribut služby je rozdělen na dvě části. První část je identifikátor atributu určující, o jaký atribut se jedná včetně jeho délky, druhá část je

vlastní hodnota atributu, která může podle potřeby nabývat libovolné délky.

Klient, který chce využívat nějakou ze služeb, nejprve vytvoří zvláštní spojení k poskytovateli služby a prohledává jeho záznamy o službách. Prohledávat lze jen v určitých záznamech odpovídajících požadovanému charakteru služby, nebo může být procházena celá databáze.

Protokol pro řízení telefonie – TCS

Protokol pro řízení telefonie TCS (Telephony Control protocol Specification) vychází z doporučení ITU-T Q.931 – Digital Subscriber Signaling System No. 1 (DSS 1). Umožňuje realizaci terminálů s funkcemi normálního telefonního přístroje, které umožňují přístup do různých sítí (například PSTN či GSM). Protokol je co do vztahu řídicí-podřízená jednotka symetrický, nerozděluje stranu uživatele a stranu sítě, ale stranu příchozí a odchozí podle toho, která ze stran zahájila hovor. Signalizace mezi jednotkami může být buď bod-bod nebo bod-body. Signalizace bod-bod je použita v tom případě, kdy je známa konkrétní jednotka, ke které je směrováno spojení. Signalizaci bod-body je možné použít tehdy, když existuje více zařízení, ke kterým může být směrováno spojení. Příkladem signalizace bod – body je případ jedné základnové stanice a několika bezšňůrových telefonů, které mají začít vyzvánět v případě příchozího hovoru. Signalizace bod – bod je přenášena spojově orientovanými pakety L2CAP, signalizace bod-body pomocí bezspojově orientovaných L2CAP-paketů.



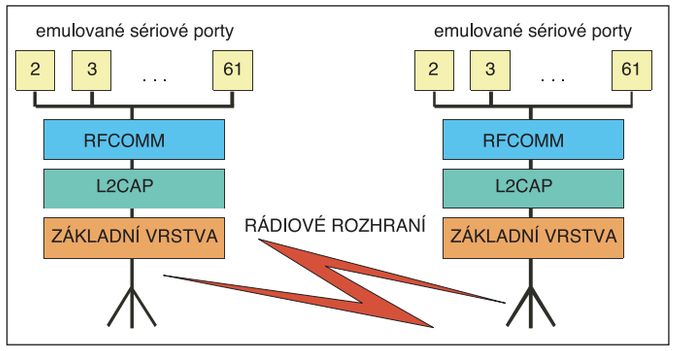
Obr. 6 TCS v rámci Bluetooth protokolů

Funkce protokolu TCS můžeme rozdělit do tří skupin: *(obr. 6)*

- řízení volání – CC (Call Control): signalizace nutná pro sestavení a rušení hlasových a datových spojenímezi jednotkami Bluetooth,
- správa skupiny – GM (Group Ma-nagement): signalizace usnadňu-jící obsluhování skupiny jedntek,
- nespojová TSC – CL (Connection Less TCS): určená pro výměnu signalizačních informací nevztahujících se k právě probíhajícímu spojení.

Protokol RFCOMM

Tento protokol slouží jako nosný protokol pro různé aplikační protokoly, jako například protokol OBEX pro výměny elektronických vizitek, kontaktů a souborů, či protokol TCP/IP pro přístup do počítačových sítí a sítě Internet. Protokol RFCOMM (Radio Frequency Communications port) je protokol emulující sériové rozhraní RS232, definovaný ve specifikaci ETSI TS 07.10 s drobnými úpravami vyplývajícími z vlastností technologie Bluetooth. RCOMM podporuje až 60 simultánních spojení mezi Bluetooth jednotkamia přenos stavů signalizačních obvodů pro každé spojení *(obr. 7)*.



Obr. 7 Zjednodušený vrstvový model

V TS 07.10 jsou tři možné pracovní režimy: základní, rozšířený bez opravy chyb a rozšířený s opravou chyb. Protokol RFCOMM byl odvozen ze základního režimu, který vychází z protokolu HDLC, ale na rozdíl od něj neužívá princip transparentnosti dat, nýbrž indikátor délky. RFCOMM pak na rozdíl od TS 07.10 nepoužívá návěstí začátku a konce rámce.

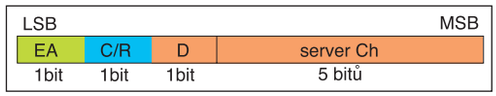
Obr. 8 Struktura rámce protokolu RFCOMM

Struktura rámce

Rámec protokolu RFCOMM se skládá z adresového, řídicího a informačního pole, a dále z indikátoru délky a zabezpečovacího pole (*obr. 8*).

Adresové pole

Adresové pole je dlouhé jeden bajt. Obsahuje pole EA, C/R, D a Server-kanál (*obr. 9*). Pole D (Direction bit) a Server-kanál (Server channel) udávají identifikátor datového kanálu DLCI (Data Link Connection Identifier). Zařízení zahajující spojení používá hodnotu bitu D=1. Aplikace běžící na zařízení, které zahajuje spojení, jsou tedy dostupné na DLCI 3, 5, 7, …, 61. Aplikace běžící na zařízení, které nezahajuje spojení, pak na DLCI 2, 4, 6, …, 60. Bit C/R (Command/Response) určuje, zda je rámec příkaz, nebo odpověď. Jeho hodnota dále závisí na tom, zda je jednotka iniciátorem spojení. Pole EA (Extension Address) označuje konec adresového pole a v případě RFCOMM je tedy vždy rovno 1.



Obr. 9 Formát adresového pole

Řídicí pole

Toto pole určuje typ rámce. Definováno je pět typů rámců:

- SABM (Set Asynchronous Balanced Mode): příkaz pro zahajování komunikace na určeném DLCI,
- UA (Unnumbered Acknowledge-ment): pozitivní odpověď na příkaz,
- DM (Disconnected Mode): negativní odpověď při pokusu o zahájení komunikace,
- DISC (Disconnect): příkaz k ukončení komunikace na určitém DLCI,
- UIH (Unnumbered Information with Header check): používán pro řídicí příkazy a pro přenos dat.

Indikátor délky

Indikátor délky je podle potřeby dlouhý jeden nebo dva bajty. Délku indikátoru určuje první bit. Pokud je jeho hodnota rovna 1, pak délka indikátoru je jeden bajt.

Zabezpečovací pole FCS

FCS slouží k zabezpečení rámce pomocí cyklického kódu. Hodnota tohoto pole se počítá pro různé typy rámců z různých položek, pro rámce SABM, DISC, UA a DM z adresového a řídicího pole a indikátoru délky. Pro rámec typu UIH se počítá z adresového a řídicího pole.

Ing. Jiří Svoboda ml.
Ing. Jiří Svoboda
Katedra telekomunikační techniky
ČVUT FEL

LITERATURA

[1] http://www.bluetooth.org
[2] http://www.bluetooth.org/foundry/specification/document/Bluetooth_V1._Core_Specifications.pdf
[3] http://www.ericsson.com/