Konečně bez kabelů: Wireless USB

STAČÍ USB ADAPTÉR: Toto zařízení firmy WiQuest propůjčí vašemu PC schopnost podpory WUSB. Cena zatím nebyla stanovena.

Pro počítačové experty je to prostě nový standard IEEE 802.15.3. Pro všechny ostatní znamená bezdrátovou volnost – bez nevýhod provázejících WLAN. *Fabian von Keudell, autor@chip.cz*

Už žádné ošklivé spleti kabelů, žádné klopýtání přes povalující se šňůry – namísto toho bezpečná výměna dat po rádiových vlnách: už brzy to umožní Wireless USB (WUSB). Funguje, podobně jako při propojení bezdrátovou sítí WLAN, jako neviditelný most mezi periferními zařízeními, například digitálními fotoaparáty, tiskárnami nebo externími disky, a počítačem. Odpadá tak mj. i neustálé hledání kdovíkam uloženého kabelu, když je zapotřebí připojit „digiťák" k PC.

Skvělé přitom je, že nedochází ke snížení datové propustnosti. Přenosová rychlost se pohybuje kolem 480 Mb/s, což odpovídá výkonnosti kabelového USB – ovšem pouze tehdy, nejsou-li takto propojené přístroje od sebe vzdáleny více než tři metry. Také na zabezpečení přenosu si vývojáři dali záležet – datový transfer chrání hned tři šifrovací metody. A zvláště vynikající hodnoty vykazuje WUSB v oblasti rádiového vyzařování: s výkonem 0,6 mW se řadí i za adaptér Bluetooth, který vyzařuje 1 mW.

Na nové přístroje s podporou WUSB si však budeme ještě muset počkat minimálně do začátku roku 2008. Důvodem je skutečnost, že nejprve musí úřady povolit frekvence v pásmu Ultra Wide Band (IEEE 802.15.3).

Vysílací výkon zvyšují triky

Kabely jsou odstíněné, a mohou proto přenášet data bez rušení. Naproti tomu rádiové vlny vykazují interference, a proto se WUSB, má-li se rychlostí vyrovnat svému staršímu kabelovému sourozenci, musí uchylovat k několika trikům.

Vylepšený protokol: U kabelového USB realizuje přenos dat mezi dvěma zařízeními tzv. „Transaction Group" (TG), která sestává ze tří paketů: jsou jimi „token" (informace o USB zařízení), vlastní přenášená data a „handshake" (korekce chyb). Jedno ze zařízení vyšle token, potom data a na závěr handshake.

Po potvrzení příjmu pak druhý přístroj zahájí spojení. Dosavadnímu USB umožňuje vysoká rychlost uvnitř vedení krátké pauzy mezi jednotlivými datovými přenosy. Wireless USB je poněkud pomalejší a nic takového si nemůže dovolit: vysílající i přijímající přístroj proto data posílají v definovaných časových úsecích, takže už nemusí čekat na potvrzení protistrany. Pak také stačí jeden handshake namísto dvou pro každé vyslání a příjem. Jen na konci TG vysílá Wireless USB ještě také korekci chyb.

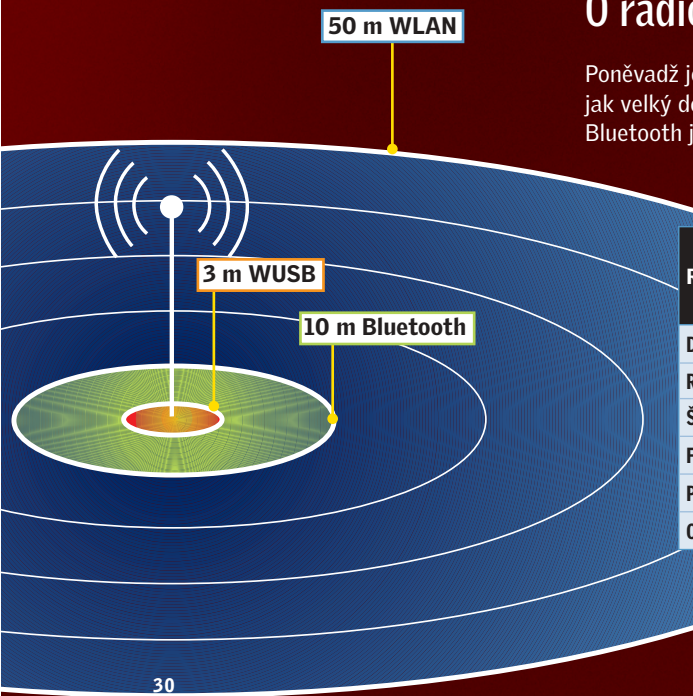
Data Phase Burst: Přístroje si mohou určit počet datových paketů obsažených v Transaction Group. Je-li kvalita rádiového spojení velmi dobrá, lze při jednom vyslání přenést až desetkrát více dat. Pokud je spojení rušeno jiným signálem, hlavní přístroj tomu „burst rate" v reálném čase přizpůsobí. Ke ztrátě dat díky handshaku nedojde.

WUSB je bezpečnější než rádiová síť

Důvodem, proč WUSB dosáhlo tržní zralosti až nyní, je šifrování. Bylo nutno vyvinout koncept, který

O rádiovém standardu rozhoduje oblast nasazení

Poněvadž je Wireless USB určeno pro digitální fotoaparáty a USB zařízení, nepotřebuje nijak velký dosah. Jinak je tomu u WLAN: větší dosah, ovšem na úkor přenosové rychlosti. Bluetooth je ideální pro mobilní telefony, neboť má malou spotřebu.



Rádiový standard	Wireless USB	Bluetooth	Wi Fi CERTIFIED
Dosah	3 m	10 m	50 m
Rychlost	480 Mb/s	2,1 Mb/s	300 Mb/s
Šifrování	128 Bitů	128 Bitů	128 Bitů
Frekvenční pásmo	3,1 – 10,6 GHz *	2,4 GHz	2,4 GHz
Přednosti	mimořádná rychlost	úspornost	velký dosah
Oblasti nasazení	periferie PC	mobily	sítě

* dosud nestanoveno

NOTEBOOK LENOVO: Na cestách oceníte vestavěné WUSB adaptéry.

BELKIN F5U302: USB rozbočovač připojuje zařízení prostřednictvím rádiových vln. Cena: cca 3000 Kč.

Už příští rok na vašem stole

Hardware podporující Wireless USB přijde na trh začátkem roku 2008. Zvenčí na nových přístrojích většinou poznáte jen jeden rozdíl: chybí kabel.

na jedné straně zajišťuje bezpečnost, ale zároveň je uživatelsky přívětivý. Samozřejmě nepřipadalo v úvahu, že by uživatel musel pracně zadávat 20místné klíče, aby třeba mohl jen na chvilku připojit „digiťák" k PC.

WUSB má k dispozici tři šifrovací metody, používané podle výkonu přístrojů a oblasti nasazení. Všechny tři metody ovšem ovládá jen hlavní (řídicí) přístroj – „host", zpravidla počítač. V připojených zařízeních je integrován vždy jen jeden šifrovací postup.

Variabilní šifrovací klíč: Pro zařízení s nevelkým výpočetním výkonem, která však přesto mají být extrémně bezpečná, například NAS systémy, je určena šifrovací metoda s manuální výměnou klíčů. Při ní musí uživatel nejprve na PC („host") zadat tzv. Connection Context (CC). Ten obsahuje kromě šifrovacího klíče (CK) také identifikaci hosta a zařízení. V dalším kroku zadá uživatel CC i na WUSB zařízení („device"). Tím se sestaví spojení k PC – zašifrované klíčem CK. Následuje „4-way-handshake" mezi počítačem a zařízením, přičemž se vytvoří vlastní zašifrovaný spoj.

- Fáze 1: Device z náhodných čísel hosta a device vypočítá tzv. Pairwise Temporal Key (PTK) pro pozdější přenos dat.
- Fáze 2: Klíčem Session Data Key, který znají oba přístroje, zašifrují host a device výměnu dat během handshaku. Kdyby klíč nesouhlasil, host spojení přeruší. Pokud je vše v pořádku, spojení pokračuje.
- Fáze 3: Přístroje zkontrolují, zda je k dispozici správný klíč PTK.
- Fáze 4: Device sdělí hostu, že nyní pracuje s PTK a je připraven přijímat. Tím je spojení zřízeno.

Pevný šifrovací klíč: V tomto případě je šifrovací klíč, tzv. Fixed Symmetric Key (FSK), pevně nastaven. Bývá většinou vytištěn na spodní stěně zařízení, například směrovačů. Tento klíč pak uživatel zadá do PC, načež na počítači i na zařízení stiskne tlačítko „Connect". Tak se zřídí spojení zabezpečené existujícími klíči. V dalším kroku opět proběhne „4-way-handshake" pro výpočet PTK a jeho použití.

Veřejný šifrovací klíč: Nejbezpečnější metoda (viz schéma) je zároveň i nejjednodušší a má být používána pro digitální fotoaparáty a tiskárny. Postup je založen, podobně jako u PGP, na šifrování privátním a veřejným klíčem. Funguje takto: uživatel stiskne tlačítka „Connect" na hostu (PC) i na device (zařízení), načež si přístroje vymění své veřejné klíče. Ty uživatel potvrdí kliknutím myši. V dalším kroku přístroje šifrují spojení příslušným veřejným klíčem. Tak vznikne zabezpečené spojení, Connection Context. Prostřednictvím „4-way-handshake" se pak opět vypočítá PTK.

Info: www.usb.org

Šifrování ve WUSB: Jednoduché, ale bezpečné

Pro WUSB jsou k dispozici tři šifrovací postupy. Která varianta bude použita, to závisí na výkonu CPU klienta. Nejbezpečnější metoda je zároveň nejkomfortnější.