

Technologie Bluetooth a BlueJacking

Vložil/a [Profik123](#) [1], 23 Listopad, 2005 - 11:21

- [Networks & Protocols](#) [2]
- [Security](#) [3]
- [WiFi & Wireless](#) [4]

Historie technologie BlueTooth a její základní charakteristika. Dále v článku si ukážeme jak funguje BlueJacking v praxi.

BlueTooth

(dále BT). Každý tohle slovo určitě slyšel, ale znalosti většiny lidí končí tím, že umí přes BT posílat obrázky mezi mobilními telefony. Proto si tuto technologii rozebereme trochu podrobněji. Technologie BT byla původně vyvinutá společností Ericsson v letech 1994-1998 jako nenákladná náhrada kabelového propojení mezi zařízeními výpočetní techniky jako jsou mobily, počítače, notebooky nebo PocketPC. Tato technologie získala název po dánském králi Haraldu I. Blaalandovi ("Modrozubý"), který v 10. století sjednotil vikingské kmeny, což připomíná sjednocení skandinávských firem Nokia a Ericsson při vývoji tohoto standardu. Technologie slouží k bezdrátovému přenosu dat na krátké vzdálenosti (maximálně 100m podle výkonu vysílače). BT využívá technologii **FFHSS CDMA (Fast Frequency Hopping Spread Spectrum, Code Division Multiple Access)**. Nyní si zkusíme ve zkratce vysvětlit, co to znamená.

Technologie **CDMA** je založena na principu, že dostupné spektrum o dané šířce (v případě BT je to 1 MHz) můžeme ve stejný čas přidělit více účastníkům dané mobilní sítě. Z toho vyplývá, že můžete mít u sebe třeba 10 notebooků a 10 telefonů s BT, a přesto se nebudou navzájem rušit. Aby se poznalo, od kterého zařízení ten který datový tok pochází, identifikují se jednotlivá zařízení unikátními kódy - proto tedy CDMA.

Spread Spectrum značí to, že celá komunikace je širokopásmová neboli že zabírá určité širší spektrum frekvencí (např. 1MHz). BT zařízení pracují konkrétně na frekvencích 2,402 - 2,480 GHz.

Frequency Hopping

je metoda používaná v řadě bezdrátových technologií. Velice často se s ní setkáte třeba u GSM sítí. Hlavní myšlenka spočívá v tom, že máme-li k dispozici určitý počet kanálů (u BT 79), může se snadno stát, že některý z těchto kanálů je rušen a jiný třeba ne, což se ovšem může měnit s časem. Pokud však budeme kanály používané pro komunikaci v čase měnit, zvýšíme tím pravděpodobnost, že se největší možná část komunikace proběhne nerušeně. Konečně slůvko Fast v úvodu celého názvu značí, že přeskokování probíhá opravdu rychle. Konkrétně 1600x za sekundu.

V roce 2003 přinesl standard BlueTooth 1.2 podstatná vylepšení. Jedním z nich je **Adaptive Frequency Hopping**. Tato vlastnost vyloučí z komunikace rušené (již zabrané) frekvence z procesu Frequency Hopping, což výrazně pomáhá tam, kde by byl signál BT jinak rušen. Ostatními vylepšeními se nebudeme dále zabývat.

BlueTooth zařízení můžeme rozdělit do tříd, a to podle vysílacího výkonu (tudíž i dosahu zařízení).

Class 1 (100 mW) má dosah až 100 metrů. Díky své energetické náročnosti se používá spíše pro USB adaptéry pro PC a pro budování BT lokálních sítí.

Class 2 (2,5 mW) je nejrozšířenější variantou s dosahem do 10 metrů.

Class 3 (1 mW) má dosah maximálně 1 metr. Používá se zejména u handsfree sad, kdy od telefonu v kapse ke sluchátku na uchu není velká vzdálenost.

Ačkoli je BT jako taková technologie stará přes 7 let, začíná se prosazovat až v poslední době. Důvodem je cena BT chipu, která klesla pod úroveň 5 USD a začíná se používat v levnějších zařízeních. V každém případě má šanci do budoucnosti výrazně ovlivnit podobu výpočetní techniky.

//Zdroj: Chip 10/2005

BlueJacking

BlueJacking je výborná hra, kterou se můžete bavit, pokud zrovna jedete metrem a nemáte co dělat a nebo vůbec kdekoli, když je okolí vašeho fonu dostatek lidí :-)

Uvedl bych zde jeden malý příklad ze serveru Mobilmania.cz a hned pochopíte o čem BlueJacking je :

Dnes si takhle sedím v bance čekajíc, až na mne přijde řada. Lidí zde bylo požehnaně a tak nezbylo, než si pohrát s mobilem. Provedl jsem průzkum svého modrozubého okolí a na displeji se mi objevil nápis Nokia 7650, což poukazovalo na nějakého chudáčka, který nechal na své Nokii zapnuto Bluetooth.

Rozhlédnu se, ale nevidím nikoho s cihlou...mám na mysli Nokii 7650. Vytvořil jsem tedy kontakt, který měl všechny položky prázdné, jen na místo jména jsem se škodolibým potěšením napsal „Kup si Ericsson!“ a tuto vizitku odeslal přes Bluetooth právě Nokii 7650. O několik kroků vedle začala Nokia řvát přes celou banku, majitel ji vzal a začal hledět na displej se zmateným výrazem. Nemohl jsem se udržet a raději jsem z banky odešel.

A pak bych tady měl ještě jeden, ale tentokrát se šťastným koncem :

Jel jsem od babičky z oběda domů. Sedím zhruba uprostřed a koukám na dvě krásné, zhruba dvacetileté, blondaté slečny. Obě vytáhli mobily (T610 a T630) a já už věděl, že BJ je můj... Připravuji si hlášku DÁMY SE MAJÍ RÁDY??? a poslal jsem to na oba dostupné telefony. Rázem se začali dohadovat, kdo jim to poslal a co si to kdo dovoluje. Jako druhou hlášku jsem poslal COPAK, SNAD SE BUDETE HÁDAT??? . Po chvilce jsem to nevydržel a poslal další zprávu: SEDÍM NAPROTI VÁM!!! :) . Opravdu, naproti nim seděl muž středního věku, který zrovna psal textovou zprávu na svém staříčkém Alcatel One Touch Easy. Obě se na něj tak zadívaly, až mi ho bylo skoro líto. Ale abych to nenechal úplně na něm, tak jsem poslal KDE VYSTUPUJETE? . Po chvilce mi přišlo jméno zastávky. Chtěl jsem jet sice ještě další tři, ale tohle jsem si nemohl nechat ujít. Vystupuji za nimi a posílám KAM JDEME? . Když už si začaly něco šeptat, tak jsem jim poslal OTOČTE SE!!! TO JSEM JÁ :) . Neuplynulo ani 5s a už na mě koukaly jako na vraha... Nejprve jsem ze sebe vypustil něco jako omluvu a potom se hned vyptávaly, jak to pracuje. Chvilku jsme si povídali a zjistil jsem, že obě jsou opravdu stejně zaměřené a bydlí kousek ode mě. Vzal jsem si na ně číslo a jsme domluveni, že někam půjdeme posedět.

Myslím, že tady z toho jste určitě pochopili o čem BlueJacking je. Pochopili jste, že nejde o to "zahltit" někomu phone zprávama (i když je to taky možnost :-D), ale o tom si z někoho vystřelit. Doufám, že je to všem jasné a teď se podíváme, jak na to.

Pro odeslání zprávy si stačí v Kontaktech vytvořit nový a do Jména a Příjmení napsat zprávu, kterou chcete posílat. Pak už stačí jenom daný kontakt normálně odeslat přes BlueTooth a vybrat phone, kam to pojedete. Výhodou posílání vizitek je, že starší telefony s BT nemusejí potvrzovat příjem, takže jim to dojde, ať chtějí a nebo nechtějí. U novějších fonů už se to bohužel (bohudík) ptá.

Na závěr bych chtěl ještě zmínit 2 užitečné programky pro OS Symbian, který trochu možná usnadňují BlueJacking.

Jedním z nich je **BlueJackX**, který je takovým nástrojem All-in pro BlueJacking...

Druhý se jmenuje **MobilLuck**, který má tu výhodu, že se může nechat běžet na pozadí ve Vašem fonu a když se objeví nějaký mobil okolo se zapnutým BT, tak Vám tenhle prográmeček zapípá, což taky docela ulehčuje práci.

Samozřejmě použití těchto softů není nutné a vyhrát si lze i pomocí obyčejných vizitek. :-)

P.S Pokud by jste se o tohle téma zajímali někdo víc, tak se ptejte třeba na foru...

Technologie Bluetooth a BlueJacking

Publikováno na serveru Security-Portal.cz (<https://security-portal.cz>)

URL článku: <https://security-portal.cz/clanky/technologie-bluetooth-bluejacking>

Odkazy:

[1] <https://security-portal.cz/users/profik123>

[2] <https://security-portal.cz/category/tagy/networks-protocols>

[3] <https://security-portal.cz/category/tagy/security>

[4] <https://security-portal.cz/category/tagy/wifi-wireless>