Bezpečnost technologie Bluetooth a její využití v PKB

Bluetooth security and its PKB usage

Tomáš Novák

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tomáš NOVÁK**
Osobní číslo:	**A08364**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnost technologie Bluetooth a její využití v průmyslu komerční bezpečnosti**

Zásady pro vypracování:

1. **Proveďte literární rešerši na téma technologie Bluetooth.**
2. **Popište způsob zabezpečení komunikace mezi zařízeními a typy možných útoků na ni.**
3. **Ověřte známé útoky a zhodnoťte jejich rizika.**
4. **Navrhněte způsoby využití této technologie v průmyslu komerční bezpečnosti.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **GEHRMANN, Christian; PERSSON, Joakim; SMEETS, Ben. Bluetooth Security. Norwood : ARTECH HOUSE, 2004. 204 s. ISBN 1-58053-504-6.**
2. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace. Brno : CP Books, a.s., 2005. 184 s. ISBN 80-251-0791-4.**
3. **SVOBODA, J. Principy a perspektivy technologie Bluetooth. Sdělovací technika. 2004, roč. 52, č. 8, s. 3-6. ISSN 0036-9942.**
4. **Wikipedie otevřená encyklopedie online, 2011, Dostupné na WWW: http://cs.wikipedia.org**
5. **The Official Bluetooth SIG Member Website [online], 2011, Dostupné na WWW: https://www.bluetooth.org**

Vedoucí bakalářské práce: **Ing. Rudolf Drga**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Práce se zabývá bezdrátovou technologií Bluetooth, způsobem zabezpečení komunikace mezi zařízeními a zneužitím bezpečnostních chyb k neoprávněnému získávání dat a odposlechu. Vysvětluje metody používané k přenosu a principy známých typů útoků. Řeší možnosti využití této technologie v průmyslu komerční bezpečnosti.

Klíčová slova: Bluetooth, bezpečnost, bezdrátová, komunikace

ABSTRACT

Bachelor thesis deals with wireless Bluetooth technology, data transfer security and abuse of vulnerability to unauthorized eavesdropping and data retrieval. It explains the methods used to data transfer and principles of known types of attacks. It offers solutions using this technology in commercial security industry.

Keywords: Bluetooth, security, wireless, communication

Děkuji vedoucímu bakalářské práce Ing. Rudolfu Drgovi za odborné vedení a poskytnuté rady. Dále bych chtěl poděkovat mé přítelkyni a rodičům za jejich velkou podporu, kterou mi při studiu poskytovali.

Motto:

Nečekejte na motivaci před vlastní činností - pusťte se do práce a motivace se dostaví!

A.A Lazarus

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Technologie Bluetooth je dnes jedním z nejrozšířenějších způsobů bezdrátové komunikace na krátkou vzdálenost. Každý týden je vyrobeno více než 30 milionů Bluetooth modulů, které jsou implementovány do různých typů zařízení. Bluetooth se tedy nevyužívá jen v mobilních telefonech, ale můžeme se s ní setkat i v automobilech, periferiích počítače či dokonce v domácí elektronice. Základními vlastnostmi této technologie jsou nízká cena, miniaturní rozměry, nízké energetické nároky a především snadná implementace. Proto je specifikace Bluetooth s oblibou používána všude tam, kde jsou nežádoucí kabely, a často jsou s její pomocí přenášeny i citlivé informace. Své uplatnění najde i v průmyslu komerční bezpečnosti. Proto se technologií Bluetooth zabývám ve své bakalářské práci, která je rozdělen do dvou částí.

V teoretické části je nejprve popsána historie a důvody vzniku této technologie. Dále jsou vysvětleny funkce jednotlivých vrstev a protokolů specifikace ve verzi 2.1+EDR. Také se v teoretické části zabývám bezpečností komunikace, způsoby jakými je řešeno šifrování a dalšími prostředky k ochraně přenášených dat. Samozřejmě existují i nedostatky v zabezpečení či chyby v implementaci, které jsou zneužívány k různým typům útoků. Tyto útoky a softwarové prostředky k jejich realizaci jsou popsány v závěru teoretické části.

V praktické části je uvedeno několik případů využití technologie Bluetooth v průmyslu komerční bezpečnosti a následně je také popsán návrh na její další využití. V návrhu jsou použity Bluetooth zařízení s dlouhým dosahem, kterým se následně také věnuji. V závěru praktické části jsem stanovil zásady pro bezpečnou komunikaci prostřednictvím Bluetooth a používání headsetu bez rizika odposlechu.

I. TEORETICKÁ ČÁST

1 VZNIK A VÝVOJ

1.1 Technologie Bluetooth

Technologie Bluetooth je definovaná standardem IEEE 802.15.1. Spadá do kategorie osobních počítačových sítí, tzv. PAN a je implementována ve většině zařízení jako jsou např. mobilní telefony, notebooky, či MP3 přehrávače. Základními možnostmi a funkcemi jsou:

Ultimate headset – Usnadnění práce s telefonem v kanceláři, autě nebo doma.

Internet bridge – Umožní uživateli připojení k internetu prostřednictvím bodu připojení.

3-in-1 phone – Umožní telefonu pracovat jak ve funkci mobilního, tak i přenosného telefonu.

Synchronizace – Zaručí jednoduchou synchronizaci práce mezi zařízeními. Například přesun kontaktů z PDA do počítače, synchronizování kalendáře v telefonu s aplikací pro správu schůzek v počítači.

Obrázek 1. Možné spojení periferií

1.2 Název Bluetooth

Název byl pro tuto technologii zvolen jako připomínka dánského krále Haralda I. (Harald Blaatand), který v 10.století sjednotil Dánsko a Norsko. Podle pověsti měl Harald velmi rád borůvky, což vysvětluje jeho přezdívku – Bluetooth, nebo-li „Modrozub“. Stejně jako král „Modrozub“ spojil dvě znepřátelené země, Bluetooth měla spojit normy ohledně bezdrátového přenosu hlasu a dat. Navíc tak došlo k spolupráci dvou skandinávských konkurenčních firem, ovládající velkou část trhu s mobilními telefony – Nokie a Ericsson. Standardy totiž museli přijmout oba největší výrobci, jinak by se nová technologie neujala.

1.3 Vznik technologie

Hlavní myšlenkou pro vznik této technologie bylo navrhnou levný, bezdrátový způsob komunikace na krátkou vzdálenost, s minimální velikostí modulu a nahradit tak množství kabelů s různými konektory od různých výrobců. Vznik této technologie sahá až do roku 1994, kdy ve firmě Ericsson vznikla studie o náhradě kabelů mezi mobilními telefony a jejich periferiemi. V květnu 1998 vznikla zvláštní zájmová skupina BSIG (Bluetooth Special Interest Group), kterou původně tvořili IBM, Intel, Nokia, Toshiba a Ericsson. První hotovou specifikaci pak BSIG uveřejnilo ve verzi 1.0a v červenci roku 1999. Později se k BSIG připojily další čtyři velké firmy (3Com, Lucent Technologies, Microsoft, Motorola). Dnes má tato skupina přes 14 000 členů a stále se rozrůstá.

Obrázek 2. Bluetooth USB adaptér

Obrázek 3. Značka Bluetooth

1.4 Vývoj verzí

Jako každá technologie se i Bluetooth od svého zrodu stále vyvíjí, jsou doplňovány standardy a zejména v prvních letech byly odstraňovány závažné chyby. Všechny verze specifikace jsou zpětně kompatibilní.

1.0a – První verze 1.0a byla vypuštěna do světa v červenci 1999.

1.0b – Ještě v prosinci téhož roku se objevila verze 1.0b.

1.1 – Standard ve verzi 1.1 existuje od února 2001 a představoval první solidní základ pro první komerčně prodávané produkty. V předchozích verzích se totiž vyskytovalo mnoho nepřesností a chyb. Objevovaly se především problémy s jednoznačným přiřazení rolí Master či Slave, kompatibilitou a čistou implementací pikosítí.

1.2 – V listopadu roku 2003 se objevila verze 1.2, která představovala od základu přepracovanou specifikaci. Architektura Bluetooth byla definována naprosto transparentně a rozšířila se o možnost rychlého vytvoření připojení. Vývojáři vybavili Bluetooth technologií „Frequency Hopping“ a povolili vylepšenou kvalitu hovoru v rámci připojení „Extended SCO“.

2.0 – Standard ve verzi 2.0 pochází z roku 2004. Největší změnou bylo rozšíření „Enhanced Data Rate“ (EDR), umožňující dosáhnout přenosové rychlosti až 2,2 Mbit/s.

2.1+EDR – V červenci 2007 byla zveřejněna verze standardu s označením 2.1+EDR, která mimo jiné přinesla podporu pro „Near Field Communications“ a umožnila i rychlejší párování zařízení.

3.0 – Bluetooth ve verzi 3.0 bylo představeno v dubnu 2009 a je založeno na protokolu 802.11 PAL, který vychází ze standardu Wi-Fi. Dosahuje maximální přenosové rychlosti 24 Mb/s. Pokud obě spárovaná zařízení podporují Bluetooth 3.0 a zároveň Wi-Fi, využije se této rychlejší přenosové cesty. Další výhodou jsou nižší energetické nároky než u starších verzí.

4.0 – Rok po představení předchozí verze se objevila specifikace Bluetooth 4.0. Zásadní změnou je zde způsob řízení spotřeby energie. Verze 4.0 byla přizpůsobena malým zařízením kde dochází jen k malému přenosu dat. Maximální rychlost se v takovém případě potřeby sníží až na 1 Mb/s a při komunikaci na krátkou vzdálenost by měla pro napájení postačovat knoflíková baterie. Přidána byla také podpora šifrování AES-128. [12]

2 STRUKTURA PROTOKOLU

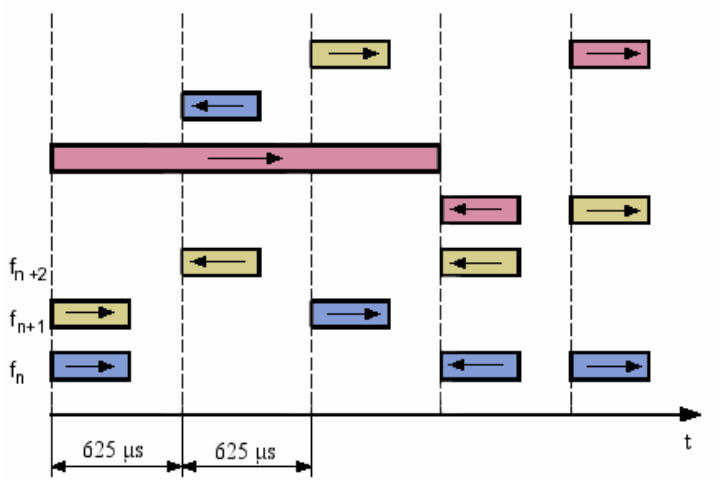
2.1 Fyzická vrstva

2.1.1 Frekvenční pásmo

Jedním z hlavních požadavků byla možnost využití technologie po celém světě, především z tohoto důvodu bylo pro přenos zvoleno bezlicenční ISM pásmo, určené pro průmyslové, vědecké a lékařské aplikace. V USA a v Evropě (kromě Francie a Španělska) se toto pásmo rozkládá mezi 2400 a 2483,5 MHz, v Japonsku mezi 2471 a 2497 MHz. Protože ISM je volné pásmo, Bluetooth musí tento rozsah sdílet s mnoha dalšími technologiemi. Aby se minimalizovala možnost vzájemného rušení s jinými rádiovými zařízeními (bezdrátové bezpečnostní systémy, WiFi, dokonce i mikrovlnné trouby), používají moduly Bluetooth k přenosu metodu FHSS.

2.1.2 FHSS

FHSS (frequency hopping spread spectrum) je jedna z metod přenosu v rozprostřeném spektru. Ve státech s ISM pásmem o šířce 80 MHz využívá tato metoda celkem 79 kmitočtů, se vzájemným odstupem 1 MHz. Po nich přeskakuje nosná vlna, modulovaná binární modulací GFSK. Počet přeskoků za sekundu, tedy jejich frekvence, je f = 1600. Každý interval na dílčí nosné vlně trvá vždy 625μs. Toto ovšem platí pouze pro základní pakety. V některých případech jsou vyžadovány delší pakety s trojnásobnou a pětinásobnou délkou, k jejich přenesení je potřeba delší časový interval a tedy i pomalejší změna nosné frekvence.



Obrázek 4. FHSS metoda

2.1.3 Typy výkonostních tříd

Podle výstupního výkonu se zařízení Bluetooth dělí do tří tříd.

Třída	Maximální povolený výkon		Přibližný dosah
	mW	dBm	
Třída 1	100	20	100 m
Třída 2	2,5	4	10 m
Třída 3	1	0	1 m

Tabulka 1. Typy výkonostních tříd

2.1.4 Typy spojení

Bluetooth využívá hvězdicovou topologii sítě. Dvě zařízení sdílející stejný kanál tvoří jednotku zvanou „piconet“. Každá pikosíť se skládá maximálně z osmi jednotek, z nichž centrální se nazývá „master“ (pán) a ostatní jednotky „slave“ (otrok) jsou mu podřízené. Několik piko sítí spolu může vytvořit seskupení zvané „scatternet“. Tím je v sítí umožněna komunikace na delší vzdálenosti přeposíláním přes několik jednotek. Zařízení mezi sebou mohou tvořit spojení bod-bod nebo bod–více bodů. Každá pikosíť je dána jiným schématem frekvenčních skoků a všechna zařízení pikosítě se s ním synchronizují. Bluetooth

nevyžaduje přímou viditelnost mezi jednotkami jak je tomu například u komunikace pomocí infračerveného portu.

2.2 Základní vrstva

2.2.1 Adresování jednotek

Každé jednotce Bluetooth je přiřazena unikátní 48bitová adresa BD_ADDR. Ta se skládá ze dvou částí: významové a nevýznamové (NAP). Významová část se dále dělí na 24bitovou dolní část (LAP) a 8bitovou horní část (UAP). Celá významová část slouží především k autentizaci a šifrování, LAP je použita pro vytvoření přístupového kódu paketu. K adresování podřízených jednotek slouží 3bitová adresa aktivního člena AM_ADDR. V případě že AM_ADDR obsahuje samé nuly, je tento paket určen všem aktivním členům pikosítě.

Obrázek 5. Schéma adresy

2.2.2 Provozní kanály

Spojení mezi zařízením master a slave může být zprostředkováno pomocí dvou kanálu. Synchronní spojově orientovaný kanál (SCO) je typu bod-bod. Pakty jsou vysílány v pravidelných intervalech s pevně danou periodou. Z tohoto důvodu jsou vhodné především pro přenos časově kritických informací, jako je hlas. Řídící jednotka umožňuje spojení třemi kanály SCO k jedné, nebo více podřízeným jednotkám. Podřízená jednotka může přijímat dva kanály SCO od různých řídících jednotek, nebo tři kanály SCO od jedné řídící jednotky. Pokud nastane chyba při přijetí paketu, vysílání není opakováno.

Druhým typem je asynchronní bezspojově orientovaný kanál (ACL). Po tomto kanálu jsou posílány pakety jen tehdy, když není aktivní SCO kanál. Mezi jednotkami existuje vždy jen jeden kanál ACL. Podřízená jednotka může s nadřízenou komunikovat pouze v následujícím časovém úseku po přijetí paketu od řídicí jednotky. V případě chyby je většina paketů na kanálu ACL vysílána znova, aby byla zajištěna kompletnost dat.

2.2.3 Pakety

Jelikož je bluetooth paketová síť, k přenosu dat se používají pakety. Základní struktura peketu je složena ze tří částí: přístupového kódu, záhlaví a informačního pole. Existují i pakety bez záhlaví, v některých případech jsou použity pakety bez informačního pole. Přístupový kód slouží k synchronizaci, kontaktování, průzkumu a v neposlední řadě také identifikuje všechny pakety posílané v rámci jedné pikosítě.

Záhlaví je složeno z šesti polí a obsahuje zásadní informace pro řízení spojení. Najdeme zde adresu aktivní jednotky které je paket určený, typ paketu, identifikátor řízení toku a potvrzení, sekvenční číslování a 8bitové zabezpečení záhlaví. Řízení toku slouží k informování vysílající jednotky o plné vyrovnávací paměti přijímajícího zařízení. Po přijetí takového paketu dojde k pozastavení vysílání dokud přijímač neinformuje vysilač o volné vyrovnávací paměti. Jednobitové pole sekvenčního číslování je s každým dalším paketem invertováno, aby mohl přijímač odlišit, zda se jedná o nový paket, nebo jde o opakované vysílání paketu předchozího.

Informační pole rozlišujeme hlasové (synchronní) a datové (asynchronní). Hlasové pole na rozdíl od datového neobsahuje záhlaví a má pevně danou délku. Datové pole je složeno ze záhlaví informačního pole, těla informačního pole a z pole pro CRC kód. V případě že paket zabírá jeden časový úsek má záhlaví velikost jeden bajt. V ostatních případech jsou to bajty dva. Stejně jako záhlaví paketu obsahuje i záhlaví informačního pole jednobitovou položku pro řízení toku logického kanálu.

Obrázek 6. Schéma paketu

2.2.3.1 Typy paketů

Všechny data v pikosíti jsou přenášena pomocí paketů. Pro synchronní kanál je definováno 9 typů paketů a pro asynchronní kanál 11 typů paketů, z nichž 5 řídících je společných pro oba kanály. K odlišení jednotlivých typů paketů slouží v záhlaví paketu 4bitová položka TYPE.

Řídící pakety

ID paket – Slouží například k procedurám kontaktování a průzkumu. Díky jeho délce (68 bitů) mohou být během jednoho časového úseku přeneseny dva pakety, čímž je tato procedura urychlena. Paket obsahuje pouze zkrácenou formu přístupového kódu

Null paket – Paket pro přenos informací důležitých při řízení spojení. Neobsahuje informační pole a je složen pouze z přístupového kódu a záhlaví. Bity v záhlaví nesou informace o stavu vyrovnávací paměti přijímajícího zařízení a informují o úspěšném přijetí předchozího paketu. Proto tento paket nemusí být potvrzován.

Poll paket – Vlastnosti „Poll“ paketu jsou podobné jako v případě paketu „Null“ jen s tím rozdílem, že neslouží k realizaci zpětné vazby a zařízení na tento paket musí odpovědět i v případě že nemá žádná data k odeslání.

FHS paket – Tento speciální paket nese v informačním poli 144 bitovou informaci o adrese a vnitřních hodinách jednotky Bluetooth. Paket slouží k synchronizaci frekvenčních skoků při vytváření pikosítě, nebo při změnách v ní. Dále je využíván při změně řízení, nebo jako odpověď na kontaktování či průzkum.

DM1 paket – Paket pro přenos jak řídících informací, tak i uživatelských dat. Pokud je tento typ paketu použit na provozním kanálu SCO, může přerušit synchronní tok informací a umožnit tak poslání řídicích informací.

Pakety Pro synchronní kanál SCO

HV1 paket – Informační pole tohoto paketu je dlohé 240 bitů. Přenáší 10 informačních bajtů zabezpečených kódováním 1/3 FEC. Slouží pro přenos synchronních dat a hlasu ve vysoké kvalitě. Jeden paket dokáže přenést 1,25 ms řeči při rychlostí 64 kb/s. Tyto pakety zabírají dva časové úseky.

HV2 paket – Přenáší 20 bajtů uživatelské informace zabezpečených 2/3 FEC. Informační pole má pevnou délku 240 bitů. Paket HV2 dokáže přenést 2,5 ms řeči rychlostí 64 kb/s. Paket je dlouhý čtyři časové úseky.

HV3 paket - Nese 30 bajtů uživatelské informace bez kódového zabezpečení. Informační pole tohoto paketu je dlohé 240 bitů. Jeden paket dokáže přenést 3,75 ms řeči rychlostí 64 kb/s. Paket zabírá šest časových úseků.

DV paket – Název paketu je odvozen ze slov data a „voice“. Tento paket tedy umožňuje současný přenos hlasu i dat, přičemž pro hlas je vyhrazena 80bitová část informačního pole, a datové pole pojme až 150 bitů. Hlasové pole není chráněno proti chybám na rozdíl od datového pole, které je kódováno 2/3 FEC a obsahuje 16bitovou ochranu cyklickým kódem. Kvůli synchronní části musí být tento paket vysílán pravidelně, a proto jej řadíme mezi pakety SCO. Jednotka Bluetooth pak s každou částí zachází odlišně. Na datové pole se vztahuje kontrola chyb a v případě nutnosti je odesláno opakovaně, kdežto synchronní pole je posíláno pouze jednou.

Pakety Pro asynchronní kanál ACL

DM1 paket – Paket má jednobajtové záhlaví a umožňuje přenos až 17 bajtů uživatelských dat zabezpečených 16bitovým cyklickým kódem. Používá 2/3 dopřednou kontrolou chybovosti FEC, což vyžaduje doplnění nulovými bity na velikost o násobku deseti. Paket DM1 je dlouhý jeden časový úsek.

DH1 paket – Značně se podobá paketu DM1 s tím rozdílem, že tento paket přenáší až 28 bajtů informací a není zde použito FEC zabezpečení, pouze 16bitový CRC kód.

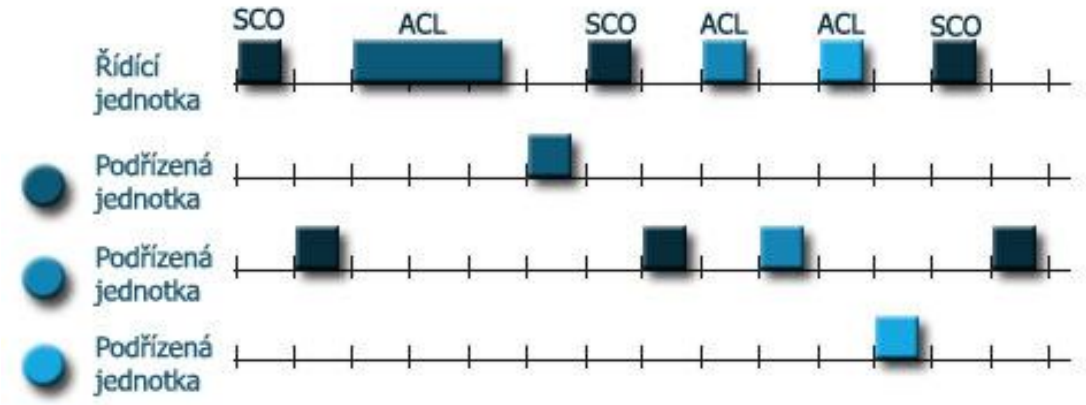
DM3 paket – V podstatě paket DM1 s delším informačním polem které dokáže pojmout až 123 bajtů. Paket je vysílán ve třech časových úsecích a jeho nosná frekvence musí být po celou dobu vysílání stejná. Zabezpečení je taktéž stejné jako u paketu DM1.

DH3 paket – Obdoba paketu DH1 vysílaná ve třech časových úsecích. Včetně dvoubajtového záhlaví může přenést až 185 bajtů. Paket je zabezpečen pouze CRC kódem.

DM5 paket – Pětiúseková obdoba paketu DM3 či DM1 umožňující přenášet až 226 informačních bajtů včetně dvoubajtového záhlaví. Zabezpečení je shodné s pakety DM3 a DM1.

DH5 paket - Pětiúseková obdoba paketu DH3 či DH1 umožňující přenášet až 341 informačních bajtů včetně dvoubajtového záhlaví. Paket je zabezpečen pouze pomocí cyklického kódu.

AUX1 paket – Tento paket je podobný DH1 paketu. V jednom časovém intervalu přenese 30 bajtů informací, přičemž není zabezpečen cyklickým kódem, ani kontrolou chybovosti.



Obrázek 7. Komunikace podřízených jednotek s řídící jednotkou

2.2.4 Detekce a oprava chyb

Pro detekci a opravu chyb v paketech, vzniklých především rušením, používají zařízení Bluetooth tři různé metody. V případě komunikace v prostředí s nízkou chybovostí není nutné používat FEC kódování a jednotka zvolí takový typ paketu, ve kterém tato metoda není používána. Informační pole je tak maximálně využito pro přenos informace, což má za následek zvýšení propustnosti kanálu.

2.2.4.1 Kódování FEC 1/3

Tento způsob zabezpečení spočívá v trojnásobném opakování každého informačního bitu. FEC 1/3 je použito pouze u paketu HV1 a umožňuje opravit jednu chybu v dané trojici.

2.2.4.2 Kódování FEC 2/3

Tento způsob zabezpečuje skupiny deseti bitů, a proto je nutné aby byla délka zabezpečované části násobkem deseti. Pokud tomu tak není, potřebný počet je doplněn nulovými bity. Z každé skupiny deseti bitů jsou vytvářena 15bitová kódová slova pomocí generačního polynomu $(x+1).(x^4+x+1)$. Tato metoda umožňuje opravit jednu chybu a detekovat dvě chyby v dané skupině bitů. Kódování FEC 2/3 je použito v paketech DM, FHS, HV2 a v datové části DV paketu.

2.2.4.3 Rozhodovací zpětná vazba

Při použití rozhodovací zpětné vazby musí být paket posílán opakovaně až do chvíle, kdy je potvrzen přijímající jednotkou. K tomu slouží položka ARQN v záhlaví paketu, ve které přijímač informuje vysílač zda byl poslední vysílaný paket přijat v pořádku. Aby mohlo dojít k ověření správného přijetí paketu, musí být informační část paketu opatřena 16bitovým cyklickým CRC kódem. Rozhodovací zpětná vazba je použita u paketů DM, DH, FHS a u datové části paketu DV.

2.2.5 Logické kanály

Specifikace Bluetooth definuje pět typu logických kanálů, z nichž dva jsou řídící a tři slouží pro přenos uživatelských dat.

LC kanál – Tento řídící kanál se nachází v hlavičce paketu a přenáší informace o doručení paketu nebo řízení toku. LC kanál je přenášen ve všech paketech obsahujících hlavičku. Jediný typ paketu který LC kanál nenese je ID paket.

LM kanál – Kanál správy spojení je přenášen položkou hlavičky informačního pole a nese informace které si vyměňují správci spojení zařízeních master a slave.

UA/UI kanál – Tyto kanály přenášejí asynchronní a izochronní data vyšší vrstvy L2CAP, která umožňuje přenos delších zpráv, nepodporovaných základní vrstvou a fragmentaci paketů.

US kanál – Kanál je využívaný SCO spojením pro transparentní přenos uživatelských dat synchronním způsobem.

2.2.6 Stavy jednotky Bluetooth

Základním stavem jednotky Bluetooth je pohotovost, neboli Standby. V tomto stavu má jednotka velmi nízkou spotřebu energie, protože fungují pouze vnitřní hodiny. Z tohoto výchozího stavu může jednotka přejít do stavů následujících.

2.2.6.1 Průzkum

Jednotka v tomto stavu prohledává okolí a sbírá adresy a hodnoty vnitřních hodin blízkých zařízení. Prostřednictvím ID paketu jednotka vysílá průzkumnou zprávu na různých skokových frekvencích. Paket obsahuje obecný přístupový kód, nebo

specializovaný přístupový kód, určený jen vybraným jednotkám. Prohledávající jednotka opakovaně vysílá na dvou skokových sekvencích, z nichž každá je tvořena šestnácti frekvencemi. Za předpokladu nulové chybovosti v daném prostředí, musí prohledávající jednotka každou sekvenci projít 256krát. Minimální čas pro vykonání průzkumné sekvence je 10,24 s. Přítomnost synchronních provozních kanálů může tento čas ještě více prodloužit.

2.2.6.2 Příjem průzkumu

Zařízení v pravidelných časových intervalech vstupuje do tohoto stavu a naslouchá na jedné vybrané frekvenci, aby mohla z průzkumné skokové sekvence zachytit kód odvozený z její adresy. V tomto stavu setrvá potřebnou dobu aby nepropásla jí určenou průzkumnou zprávu.

2.2.6.3 Odpověď na průzkum

Po přijetí průzkumného paketu odpoví zařízení FHS-paketem, obsahujícím adresu jednotky a stav vnitřních hodin. Nedochází k tomu ovšem okamžitě, ale až po náhodně dlouhé době, aby se tak zabránilo konfliktu s zařízeními, které přijali průzkumný paket na stejné frekvenci. Po odvysílání FHS-paketu zůstává jednotka dále ve stavu příjmu průzkumu a nečeká na odpověď.

2.2.6.4 Kontaktování

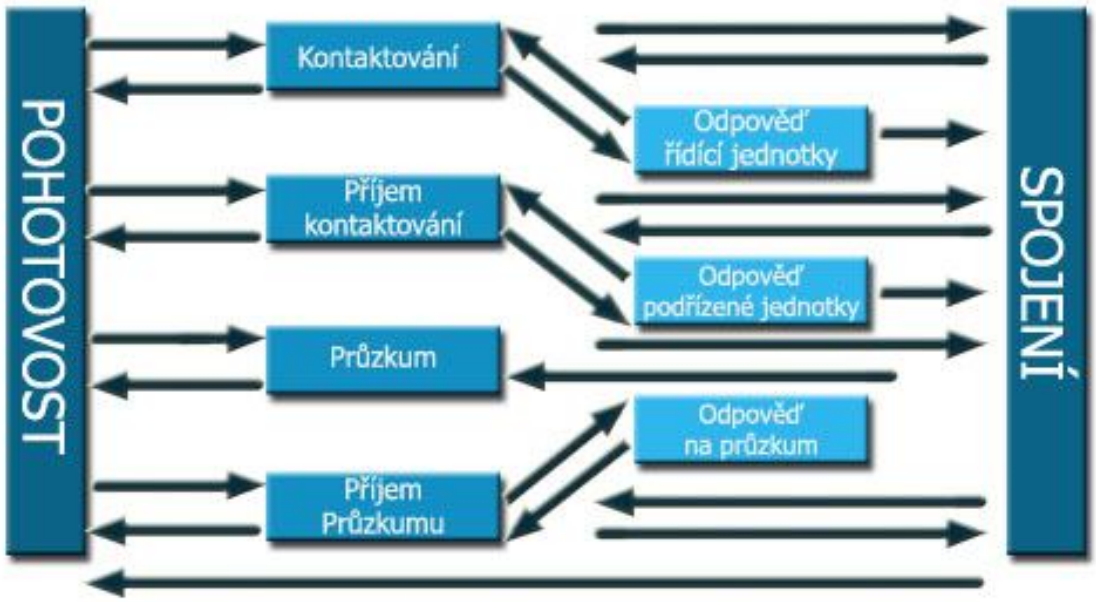
V případě že si řídící jednotka přeje navázat spojení s jinou jednotkou, přechází do režimu kontaktování. Proces je podobný prohledávání s tím rozdílem, že ID-paket nese přístupový kód vypočtený z adresy zařízení. Ze stejné adresy se řídící jednotka snaží odhadnout frekvenci, na které kontaktovaná jednotka pravděpodobně přijímá. Tento odhad může být přesnější v případě že řídící jednotka zná hodnotu vnitřních hodin kontaktované jednotky získanou z průzkumu, který většinou kontaktování předchází.

2.2.6.5 Příjem kontaktování

V tomto stavu podřízená jednotka poslouchá na zvolené frekvenci a očekává příjem ID-paketu s přístupovým kódem. Zvolená doba po kterou jednotka naslouchá na stejné frekvenci musí být delší než doba potřebná k průzkumu šestnácti frekvencí.

2.2.6.6 Odpověď na kontaktování

Po přijetí kontaktního ID-paketu přechází podřízená jednotka do stavu „odpověď na kontaktování“. V následujícím časovém úseku pošle podřízená jednotka na stejné frekvenci ID-paket se svým přístupovým kódem řídící jednotce. Od tohoto okamžiku je už řídící jednotce známá frekvence, na které podřízená jednotka přijímala a může jí tak poslat FHS-paket s informacemi o stavu svých vnitřních hodin, s použitím přístupového kódu podřízené jednotky. Paket dále obsahuje tříbitovou adresu aktivního člena, sloužící k identifikaci v pikosíti. Podřízená jednotka odpoví ID-paketem a z přijatého FHS-paketu vypočítá přístupový kód pikosítě a synchronizuje se s frekvenční skokovou sekvencí řídicí jednotky. Poslední částí této procedury je přijetí POLL-paketu od řídící jednotky, který je už adresován pomocí adresy aktivního člena a obsahuje přístupový kód dané pikosítě. Podřízená jednotka na tento paket odpoví libovolným paketem (nejčastěji NULL), a poté už dochází k výměně samotných informací pomocí protokolu pro správu spojení – LMP.



Obrázek 8. Přechody mezi provozními stavy jednotky Bluetooth

2.2.7 Režimy ve stavu připojení

2.2.7.1 Aktivní režim

Řídící jednotka v aktivním režimu plánuje podle požadavků podřízených jednotek přenos dat a stará se o synchronizaci podřízených jednotek s fyzickým kanálem. Aktivní

podřízená jednotka poslouchá v intervalech určených od řídící jednotky, zda momentálně není přenášen jí adresovaný paket. V případě že tomu tak není, nemusí neadresované jednotky naslouchat až do dalšího časového úseku vyhrazeného pro přenos ve směru od řídicí jednotky.

2.2.7.2 Režim Sniff

Podřízená jednotka v tomto režimu nenaslouchá fyzickému kanálu. Toto opatření má za následek snížení spotřeby energie v době kdy jsou přenášeny pakety mezi jiným jednotkami. Pokud se ale podřízená jednotka podílí na provozním kanálu ACL, musí naslouchat ve všech možných časových úsecích, v kterých začíná přenos od řídící jednotky. Řídící jednotka může začít přenos pouze v daných, periodicky se opakujících časových úsecích.

2.2.7.3 Režim přidržení

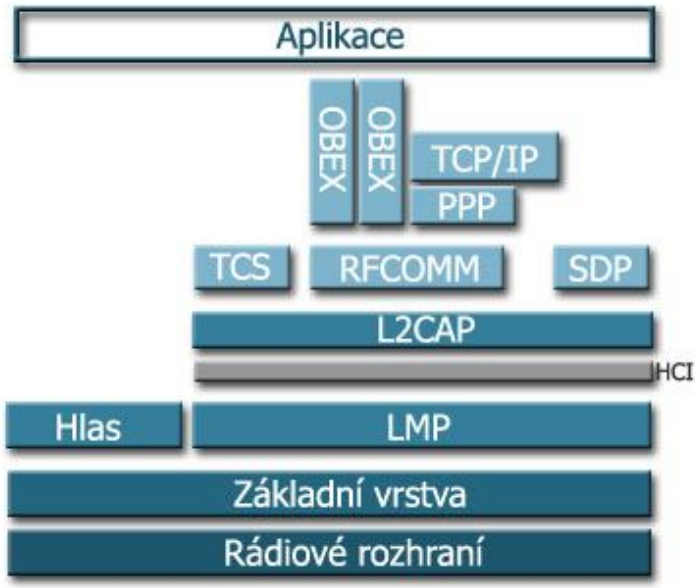
Během režimu přidržení nejsou podporovány pakety na provozním kanále ACL a uvolněná kapacita je využita například pro procedury průzkumu, kontaktování nebo pro účast v jiné pikosíti. Při přechodu do tohoto režimu se řídící jednotka domluví s podřízenou jednotkou na délce jeho trvání a po uplynutí této doby přejde podřízená jednotka do aktivního režimu a očekává další instrukce. V průběhu přidržení neztrácí podřízená jednotka adresu aktivního člena.

2.2.7.4 Režim parkování

Tento režim je charakteristický nejnižší spotřebou energie a taktéž nejmenší aktivitou podřízené parkující jednotky. Režim parkování také umožňuje připojení více než sedmi jednotek „slave“ k jednotce „master“. Aby mohla být připojena další podřízená jednotka, zařízení vstupující do tohoto režimu odevzdá svou adresu aktivního člena a dostane přiděleny dvě osmibitové adresy – adresu zaparkovaného člena a adresu žádosti o přístup. Podřízená jednotka vstupující do pikosítě tak získá jeho adresu aktivního člena a může začít vyměňovat informace. Parkující zařízení může být pomocí adresy zaparkovaného člena voláno řídící jednotkou pro změnu režimu, nebo může poslat adresu žádosti o přístup samotná parkující podřízená jednotka. Aby mohlo parkující zařízení přijmout požadavek na změnu režimu, musí v pravidelných intervalech poslouchat fyzický kanál.

2.3 Protokol správy spojení - LMP

Mezi základní funkce tohoto protokolu patří například správa spojení, řízení párování, šifrování, kontrola kvality spojení či volba vhodných typů paketů. Zprávy LMP protokolu jsou provedeny a odfiltrovány na přijímající straně správcem spojení, takže se nešíří do vyšších vrstev. Pakety linkového manageru mají vyšší prioritu než data, a proto nejsou brzděny provozem na kanálu. Pakety LMP a L2CAP se od sebe liší dvoubitovou hodnotou v hlavičce paketu. Dalšími částmi LMP paketu jsou „Transaction ID“, operační znak a obsah. „Transaction ID“ je jednobitová položka nesoucí informaci o původu transakce, kterou mohla začít řídící či podřízená jednotka. Sedmibitový operační znak určuje druh konkrétní zprávy a obsah nese konkrétní parametry zprávy. Po navázání spojení pomocí kontaktování dochází k cyklickému dotazování na úrovní LM. Pomocí těchto procesů získá dotazující se zařízení informace o vzdáleném zařízení, možnosti kódování a autorizace.



Obrázek 9. Vrstvy systému Bluetooth

2.4 Protokol pro řízení a adaptaci logických spojení – L2CAP

L2CAP propojuje protokoly vyšších vrstev s operacemi prováděnými na základní vrstvě. Definuje ovšem spojení pouze pro kanály ACL, jelikož provozní kanály SCO jsou posílány přímo základní vrstvě. Tyto kanály jsou plně duplexní a jsou jednoznačně

identifikovány adresou zařízení, ke kterému kanál vede a identifikátorem kanálu, určeným pro potřeby konkrétní aplikaci. Mezi funkce L2CAP protokolu patří:

Segmentace a spojování paketů – Velikost paketů základní vrstvy je omezena v závislosti na daném typu paketu. L2CAP ovšem umožňuje přenést pakety o velikosti až 64 kB a je tedy zodpovědný za rozdělení a skládání informačního pole paketu.

Multiplexování protokolů vyšších vrstev – Spravuje přepínání mezi protokoly SDP, RFCOMM a TCS.

Kvalita služeb – Musí zajistit dodržování dohodnutých parametrů služeb, definovaných při procesu navázání spojení.

2.5 Protokol pro zjišťování služeb – SDP

Pomocí tohoto protokolu jsou aplikacím poskytovány prostředky pro zjištění dostupnosti služeb a jejich charakteristik. Jednotka poskytující informace o těchto službách se nazývá SDP-server. Jednotka žádající o přístup k seznamu služeb poskytovaných serverem se nazývá SDP-klient. Na jednotce Bluetooth může být provozováno ve stejný okamžik několik SDP-klientů, avšak jen jeden SDP-server.

2.6 Protokol pro řízení telefonie - TCS

Protokol TSC definuje sestavení a řízení linky pro přenos hlasu, a dále také umožňuje využívat funkce typické pro telefonní přístroje přistupující do sítí GSM či PSTN. Protokol nerozlišuje stranu uživatele a stranu sítě, ale podle toho kdo zahájil hovor rozlišuje stranu příchozí a odchozí. Protokol definuje dva druhy signalizace. Signalizace bod – bod je použita v případě, kdy je spojení adresováno jedné konkrétní jednotce. Naopak signalizace bod – body je použita například při spojení několika bezdrátových telefonů s jednou základnovou stanicí.

2.7 Protokol RFCOMM

Jedná se o protokol emulující sériové rozhraní RS232. Slouží jako nosný protokol pro aplikační protokoly mezi které řadíme protokol TCP/IP pro přístup počítačových sítí, nebo protokol OBEX, sloužící k výměně elektronických vizitek a kontaktů. RFCOMM umožňuje až 60 současných spojení mezi zařízeními Bluetooth.

3 BEZPEČNOST TECHNOLOGIE BLUETOOTH

3.1 Způsob zabezpečení

Zabezpečení technologie Bluetooth je realizováno pomocí tří základních služeb:

- a*utentizace* – ověření totožnosti komunikujících stran
- *důvěrnosti* – ochrana před odposloucháváním
- *autorizace* – povolení přístupu ke službám.

Specifikace poskytuje tři úrovně bezpečnosti, dvě úrovně důvěry vůči zařízení a tři úrovně bezpečnosti služby. Zařízení Bluetooth může pracovat v jednom ze tří bezpečnostních režimu:

- *bez zabezpečení* – zařízení v tomto režimu umožňuje navázat komunikaci jakékoliv blízké jednotce
- *bezpečnost na úrovni služeb* – je vyžadována autorizace přístupu k službám
- *bezpečnost na úrovni spoje* – před navázáním spojení jsou iniciovány bezpečnostní postupy (autentizaci a šifrování)

Jednotce Bluetooth je dovoleno jiné zařízení s podporou Bluetooth objevit, ovšem k tomu aby s dosud neznámým zařízením mohla komunikovat je nutný zásah uživatele ve fázi inicializace, kdy dochází k párování. Do obou zařízení je nutné zadat identický PIN dlouhý 8 až 128 bitů. Poté se z PIN kódu, adresy jednotky iniciující párování a náhodného čísla odlišného pro každou transakci vygeneruje inicializační klíč. S pomocí tohoto klíče se vygeneruje klíč spoje, který dvojice sdílí a nikdy jej nevysílá. [2]

3.1.1 Autentizace

Technologie Bluetooth umožňuje autentizovat zařízení, nikoli uživatele. K autentizaci je použit klíč spoje. Tím může být buď klíč zařízení, kombinační klíč, či hlavní klíč.

Klíč zařízení – Klíč je generován při instalaci zařízení a aplikace při inicializaci zvolí, který z klíčů bude použit jako klíč daného spoje . V případě zařízení s omezenou pamětí musí být použít jeho klíč, protože další klíč se do paměti už nevejde.

Kombinační klíč – Tento typ klíče se generuje ve fázi inicializace z obou klíčů zařízení komunikujících jednotek. Použití kombinačního klíče je bezpečnější, protože jednotka nepoužívá stále stejný klíč pro komunikaci s různými jednotkami.

Hlavní klíč – Hlavní klíč je využíván pro mnohobodovou komunikaci, kde všechny připojené jednotky sdílejí jeden klíč, nahrazující jednotlivé klíče spoje.

Proces autentizace funguje na principu výzva-odpověď. Vyzyvatel zašle svoji adresu a od druhé komunikující strany dostane náhodné číslo. Na základě těchto hodnot a sdíleného klíče spoje se pomocí autentizační funkce spočítá výsledek, který si obě strany porovnají. Každé z zařízení si tak ověří, zda druhá strana zná sdílený klíč. V případě automatické autentizaci, ke které dojde jakmile se zařízení octnou v dosahu, je tento proces uživateli skryt.

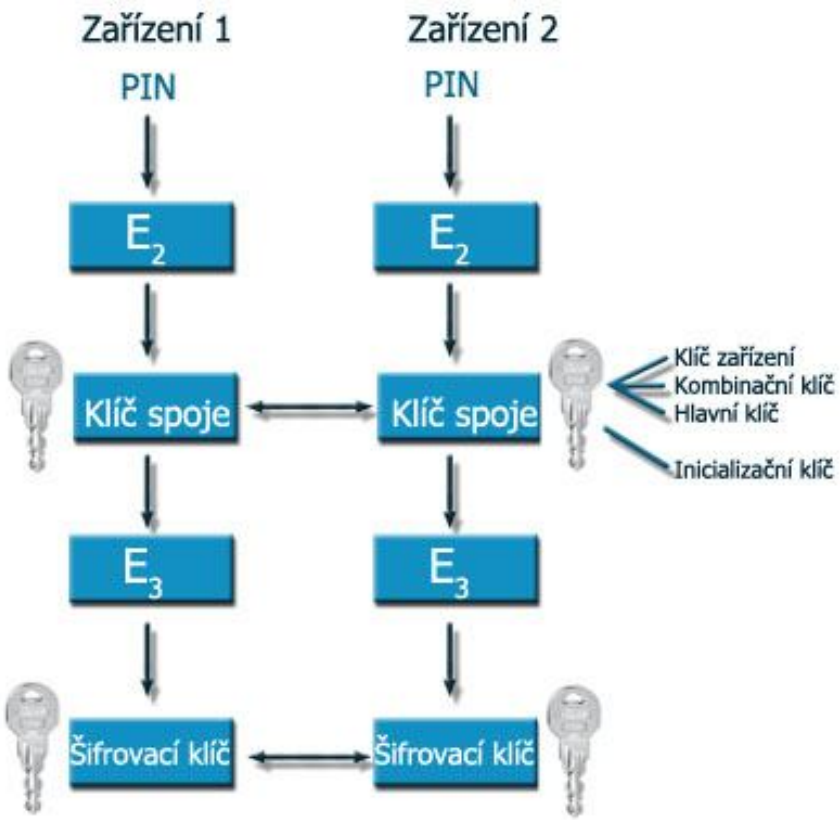
3.1.2 Šifrování

Pro každý paket se odvozuje z autentizačního klíče nový šifrovací kód s délkou 8 až 128 bitů. Na velikosti klíče se obě strany předem dohodnou, což umožňuje použít slabší zabezpečení paketů, aniž by byla ovlivněna síla autentizace. Šifrovací klíč je generován z klíče spoje, náhodného čísla, adresy zařízení a hodnoty vnitřních hodin řídící jednotky.

3.1.3 Bezpečnostní postup

Z bezpečnostního hlediska postupují jednotky při komunikaci následujícím způsobem:

1. Pomocí algoritmu E_{21} jsou vygenerovány klíče dvou zařízení.
2. Dojde k vygenerování inicializačního klíče (E_{22}), procesu autentizaci (E_1) a výměně klíčů spoje podle E_{21}.
3. Je vygenerován šifrovací klíč (E_3) a komunikace je dále šifrována (E_0).



Obrázek 10. Schéma generování a použití klíčů

Verze 1.0 specifikace Bluetooth ponechávala část řešení způsobu zabezpečení na výrobci. Zařízení od různých výrobců pak nebyla schopna navázat spojení, neboť se obě komunikující strany domnívali, že jsou řídící jednotkou a generovali tak různé klíče. Specifikace 1.1 vyžadovala od podřízené jednotky potvrzení, že je v podřízené roli, a tím byl problém vzájemné spolupráce vyřešen. [1]

3.2 Nedostatky v zabezpečení Bluetooth

Krátký PIN – Délka klíče se vybírá podle maximální podporované společné délky obou zařízení. Pokud tedy jedna z jednotek podporuje pouze čtyřmístný PIN, je komunikace mezi zařízeními šifrována velmi slabě. Nejrizikovější je komunikace se zařízením s pevně daným PIN kódem, jehož hodnota je většinou „0000“ nebo „1234“.

Distribuce PIN – Tato metoda ve specifikaci Bluetooth chybí. Ve větších sítích může být problematické ruční zadávání PIN a přenášení tohoto kódu bezdrátově není z bezpečnostních důvodů vhodné.

Šifrovací klíč – Dělka šifrovacího klíče se musí předem dohodnout a často je používána minimální délka 1 byte. Šifrovací klíč je generován mimo jiné z hodnoty vnitřních hodin řídící jednotky. Pokud trvá spojení déle než 23,3 hodin, hodnota hodin se bude opakovat a zařízení tak bude generovat stejné šifrovací klíče, jaké už byly jednou použity.

Klíč zařízení – Tento klíč je stále stejný i v případě komunikace s jinou jednotkou, a při prvním použití se tedy stává veřejným. Vhodnější by bylo použít jej pro generování náhodného klíče, nebo používat sadu klíčů místo jediného klíče zařízení.

Hlavní klíč - Hlavní klíč je při vícebodové komunikaci sdílený všemi jednotkami, a nahrazuje tak jednotlivé klíče spoje.

Autentizace – Autentizuje se pouze zařízení, nikoli uživatel. V případě, kdy je známa identita uživatele i neměnná adresa jeho zařízení, může být této informace využito k zaznamenávání jeho aktivit v sítí, což způsobí ztrátu soukromí. Autentizace na základě výzvy-odpovědi navíc nabízí možnost útoku „man in the middle“.

Šifrovací algoritmus E_0 – Tento algoritmus byl podrobně analyzován komunitou, nicméně slabinou algoritmu E_0 je prvek s generátorem sum, jenž by mohl být zneužit při korelačních útocích. Jsou známy i přímé útoky na tento algoritmus, ale ty jsou příliš složité. Při použití jednoho z těchto útoků je známo, že se maximální efektivní délka klíče 84 bitů sníží, když útočník zná 132 bitů šifrovaného proudu dat. A pokud je známo 243 bitů šifrovaného proudu dat, může se maximální účinná délka klíče snížit až na 73 bitů. [6]

3.3 Útoky na Bluetooth

Technologie Bluetooth poskytuje velké množství služeb a její implementace dnes využíváme v různorodých zařízeních. Výhody Bluetooth ovšem nejsou poskytovány bez rizika. Stejně jako jiné bezdrátové technologie je i Bluetooth náchylná na odposlouchávání, neoprávněné získávání informací, či jiné útoky.

3.3.1 Bluesnarfing

Bluesnarf obchází proces párování před vlastní komunikací, takže útočník může získat přístup k datům bez vědomí majitele telefonu. Bluesnarf útok využívá chyb v implementaci Bluetooth na některých mobilních telefonech. K tomuto útoku je zneužíván především OBEX protokol, sloužící výhradně k výměně vizitek a posílání kontaktů. Pomocí SDP protokolu útočník nejdříve zjistí, zda cílové zařízení podporuje potřebné profily OBEX protokolu. V případě že zná útočník strukturu souborů cílového zařízení, vyšle požadavek OBEX GET na konkrétní soubor a získá tak přístup k telefonnímu seznamu, přijatým zprávám či jiným informacím uchovaným v soborech, jejichž umístění a název jsou veřejně známe. Zprvu bylo možné provést útok jen na zařízení ve viditelném režimu, dnes jsou ale známy úspěšné útoky i na zařízení ve skrytém režimu.

Obrázek 11. Logo Bluesnarfing útoku

3.3.2 Bluejacking

Bluejacking je útok při kterém nedochází k získávání informací, ale naopak jsou zprávy útočníkem rozesílány. Bluejacking spočívá v rozesílání vizitek, které se ve většině případech zobrazí na displeji telefonu s dotazem, zda má být uložena či nikoliv. Bluejacking je zpravidla chápán jako zábava. V místě většího výskytu lidí bluejacker rozesílá žertovné zprávy na okolní zařízení a případně i sleduje reakci lidí, nechápajících jak se zpráva octla na displeji jejich telefonu.

Bluejacking nemusí vždy sloužit jen k rozesílání vtipných hlášek. Skutečnost že útočník může odeslat zprávu na zažízení jehož telefoní číslo ani adresu Bluetooth jednotky nemusí znát přímo vybízí k sociálnímu inženýrství. Útočník může odeslat vizitku pojmenovanou „zadej 0000“ a po chvíli se pokusí s zařízením spárovat. Je velmi pravděpodobné že narazí na člověka, který neví že má Bluetooth aktivní, nebo k čemu vlastně slouží a příkaz poslechne.

Zatímco dříve se vizitky museli psát a odesílat ručně, dnes už pro každou platformu existuje řada aplikací, které automaticky rozesílají vizitky na všechna zařízení v okolí. Jediný

mobilní telefon umístěný u dveří obchodního centra tak může rozesílat reklamu a jiné nevyžádané informací na stovky zařízení denně.

Obrázek 12. Zpráva od bluejackera

Obrázek 13. Logo české komunity bluejackerů

3.3.3 Bluebugging

Tato metoda útoku využívá chyb firmwaru některých starších telefonů a pomocí protokolu RFCOMM emulujícího sériový port se útočník připojí na kanál 17, který je u těchto zranitelných telefonů zadními vrátky. Útočník pak může pomocí AT-příkazů, jejichž provádění nevyžaduje autentifikaci, doslova převzít kontrolu nad telefonem. AT-příkazy umožňují telefon ovládat stejně jako je ovládán tlačítky. Útočník může číst a posílat SMS zprávy, volat na jakákoliv čísla a dokonce i přesměrovat příchozí hovor na své zařízení. Tuto metodu lze využít i za účelem zisku. Stačí aby si útočník zřídil vlastní placenou linku a z napadených zařízení na ni dlouhé minuty telefonoval.

3.3.4 Bluesmack

Bluesmack je útok typu „Denial of Service“ a je podobný útoku „Ping of Death“ v počítačové síti. Útočník pošle cílovému zařízení L2CAP-paket o velikosti 600 bytů, což způsobí přetečení zásobníku. Následky tohoto útoku jsou u jednotlivých zařízení různé. V některých případech dojde k zamrznutí zařízení nebo dočasné nefunkčnosti Bluetooth a rychlému vybití akumulátoru baterie.

3.3.5 HeloMoto

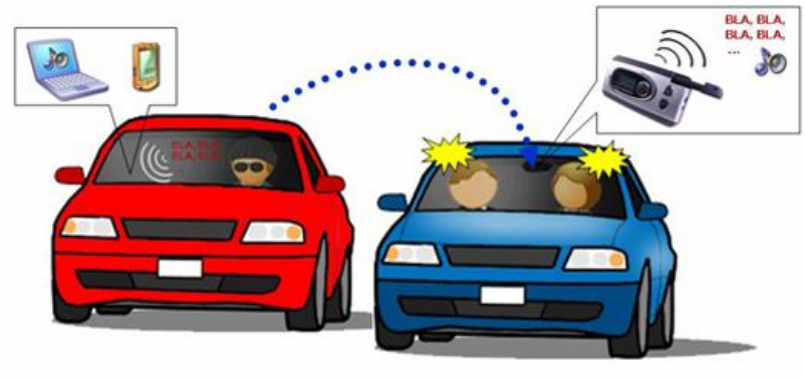
Jedná se o kombinaci Bluesnarf a Bluebug útoku a využívá chyby v implementaci obsluhy důvěryhodných zařízení u některých starších telefonu značky Motorola. V první fázi útoku je cílovému zařízení poslána vizitka pomocí OBEX protokolu a následně je tento požadavek záměrně zrušen. V důsledku chyby je útočníkovo zařízení umístěno do seznamu důvěryhodných zařízení. V další fázi se připojí k headset profilu, a to mu umožní převzít kontrolu nad telefonem pomocí AT-příkazů.

3.3.6 BlueDump

Pomocí této metody může útočník přinutit zařízení, aby zahodilo uložený klíč spoje a následně byl vytvořen nový, který již bude útočníkovy znám. Podmínkou pro provedení BlueDump útoku je znalost adresy jednotky v seznamu důvěryhodných zařízení oběti. Útočník se pak s touto adresou připojí k oběti a jakmile přijde požadavek na autentizaci, dostane se mu odpovědi „HCI_Link_Key_Request_Negative_Reply“. Následkem toho cílové zařízení zahodí jeho vlastní klíč spoje a zopakuje párovaní proces za účelem získání nového klíče. [7]

3.3.7 Car Whisperer

Car Whisperer využívá pevně daného PIN kódu v některých Bluetooth zařízeních bez displeje či klávesnice, nutné k zadání PIN kódu. Studie byla zaměřena konkrétně na připojení a odposlech bluetooth handsfree, které jsou používány v automobilech. Útočník se připojí k zařízení s třídou Headset nebo handsfree pomocí protokolu RFCOMM. Z prvních tří bytů adresy jednotky je určen výrobce zařízení a poté zvolen odpovídající PIN s hodnotou „0000“, nebo „1234“. Po navázání spojení může být na zařízení odeslána zvuková zpráva ve formátu „raw“, nebo může útočník komunikaci zachycenou mikrofonem handsfree nahrávat. [13]



Obrázek 14. Průběh CarWhisperer útoku

3.4 Nástroje na provádění útoků a Bluetooth audit

Nástrojů pro testování zranitelnosti Bluetooth zařízení existuje celá řada. Většina z nich je napsána pro Linux, ale dostupných je také několik aplikací pro platformy Windows, Java či Palm. Nejvíce nástrojů pro Bluetooth audit sdružuje linuxová live-cd distribuce Back Track. Najdeme v ní přes 30 aplikací na skenování služeb cílového zařízení, integrujících základní typy útoků.

3.4.1 Btscanner

Užitečný nástroj podporující souběžné používání více Bluetooth zařízení k skenování okolních jednotek. Podporuje inquiry, brute force scan, HCI a SDP info včetně exportu výsledků. Obsahuje IEEE OUI tabulky s čísly a třídami zařízení na jejichž základě dokáže poměrně přesně identifikovat zachycené zařízení. Výsledky skenování jsou automaticky ukládány a velkou výhodou je i přehledné rozhraní aplikace. [15]

```
RSSI:    +0   LQ:  000    TXPWR:  Cur   +0
Address:       6C:9B:02:FF:97:2F
Found by:      00:24:2C:DB:C0:22
OUI owner:
First seen:    2010/09/06 09:59:20
Last seen:     2010/09/06 09:59:51
Name:          Nokia Test BT
Vulnerable to:
Clk off:       0x2d78
Class:         0x520204
               Phone/Mobile
Services:      Networking,Object Transfer,Telephony

HCI Version
-----------
LMP Version: 2.1 (0x4) LMP Subversion: 0x1673
```

Obrázek 15. Btscanner – informace o nalezeném zařízení

3.4.2 Tbsearch

Aplikace pro detekci skrytých BlueTooth zařízení pomocí brute force útoku na posledních šest bajtů Bluetooth adresy jednotky a „read_remote_name()“. Tbsearch je původně součástí balíku T-bear pro Bluetooth audit, avšak v distribuci Back Track jsou jen další dva programy z tohoto balíku. Tanya – nástroj pro DoS útoky a skenovací aplikace tbear. Tbsearch umožňuje nastavení rozsahu hledaných adres a použití více Bluetooth adaptérů, nicméně proces hledání je i tak velmi zdlouhavý.

Obrázek 16. Tbsearch - použití čtyř zařízení současně

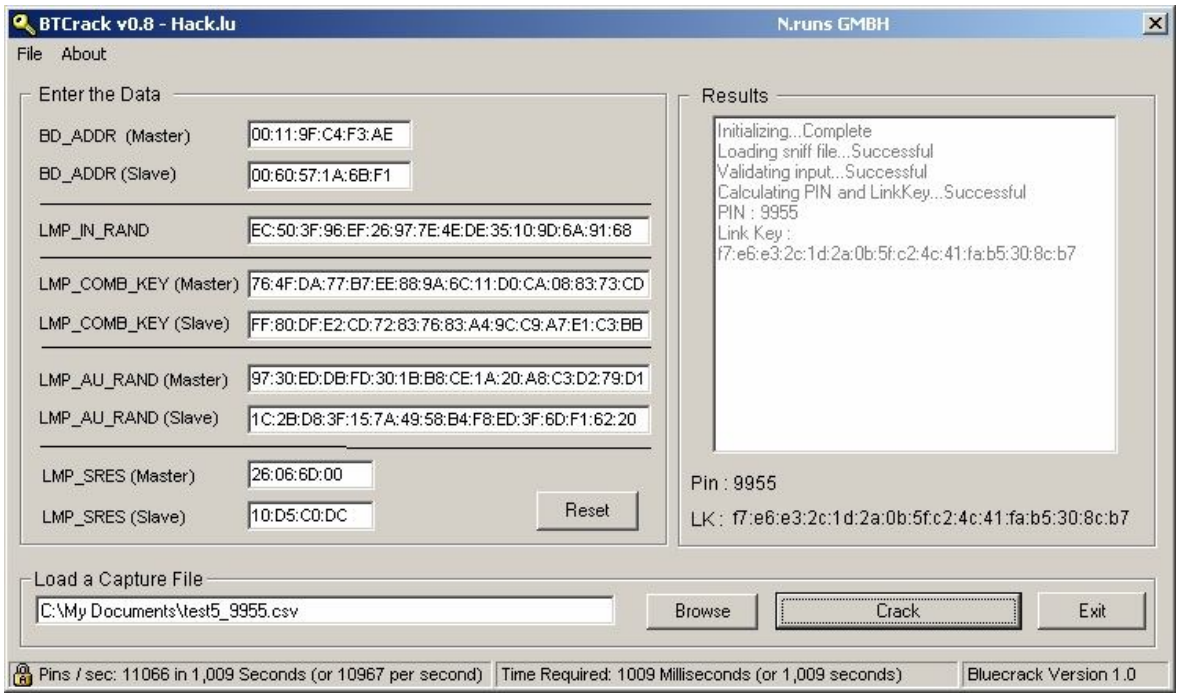
3.4.3 Bluediving

Bluediving je sada aplikací pro testování zranitelností BlueTooth. Implementuje útoky jako BlueSnarf, BlueBug, BlueSmack. Nástroje obsažené v této sadě umožňují spoofing Bluetooth adresy, AT a RFCOMM socket shell. Další nástroje obsažené v balíku jsou carwhisperer, resetátor spojení L2CAP, generátor paketů L2CAP či RFCOMM skener. [16]

Obrázek 17. Bluediving - úvodní obrazovka

3.4.4 BTcrack

BTcrack je aplikace s grafickým rozhraním pro pasivní útok na párovací proces mezi zařízeními. Na počítači s procesorem Pentium IV pracuje rychlostí 200 000 klíčů za sekundu. Aplikace je schopná vypočítat PIN a klíč spojení ze zachycené výměny dat, probíhající při procesu párování. Pro odchycení dat je nutné použít profesionální zařízení nebo USB Bluetooth adaptér, podporující RAW mode. [14]



Obrázek 18. BTcrack - zjištění klíče spoje a PIN kódu

II. PRAKTICKÁ ČÁST

4 VYUŽITÍ TECHNOLOGIE BLUETOOTH V BEZPEČNOSTNÍCH SYSTÉMECH

S technologií Bluetooth se v bezpečnostních systémech nesetkáváme příliš často. Ke komunikaci mezi bezdrátovými prvky systému volí výrobce raději vlastní technologii, ať už z bezpečnostních důvodů, nebo kvůli nevyhovujícím vlastnostem této specifikace. V některých případech je však technologie Bluetooth využívána k stažení dat a aktuálního nastavení systému do počítače. Příkladem může být Jablotron JA-80BT, sloužící k propojení systémů řady JA-8x a JA-6x s počítačem. Zařízení se připojuje do konektoru digitální systémové sběrnice pomocí přiloženého kabelu. Poté jej stačí spárovat s Bluetooth adaptérem v počítači kde je nainstalována aplikace ComLink. [18]

Obrázek 19. Jablotron JA- BT

V mé práci bych se ovšem zaměřil na výrobky, které využívají přednosti technologii Bluetooth jiným způsobem než jako pouhé nahrazení kabelu mezi počítačem a samotným zařízením.

4.1 Konkrétní příklady využití

4.1.1 iBox BT

Lockbox je malý klíčový trezor, který s oblibou používají realitní kanceláře v USA, kde je způsob prodeje nemovitostí poněkud odlišný. Základní funkcí lockboxu je umožnit více agentům vstup do domu, aniž by si museli předávat klíče. Ve většině případech se

lockbox umísťuje na dveřní kouli podobně jako visací zámek. Do schránky chráněné zámkem nebo kódem se umístí klíče, karty nebo kód zabezpečovacího systému a každý agent oprávněný vstoupit do objektu zná kód nebo způsob, jakým lockbox otevřít. Moderní elektronické lockboxy je možné programovat a nastavit tak, že může být otevřen jen v pracovní dny, případně i v daném časovém rozmezí. Dalšími pokročilými funkcemi je logování nebo informování emailem o otevření lockbox. Tyto funkce mají zabránit tomu, aby agent v domě pořádal párty či jej jinak využíval. Díky logování je také možné dohledat, který z agentů je zodpovědný za ztrátu klíčů a jiné situace.

Lockbox iBox BT nabízí společnost Supra, která je největším výrobcem těchto zařízení. K otevření stačí PDA nebo jiné podporované zařízení s nainstalovanou aplikací, umožňující agentům identifikaci a vložení kódu. Jeden typ kódu slouží k otevření schránky, pro uvolnění zámku je nutné zadat tzv. „shackle code“. Podporována jsou zařízení s operačním systémem Black Berry, Palm, Windows mobile, Android a iOS.

Vlastnosti:

Rozměry:	7,9 x 6,4 x 22,2 cm
Váha:	1,15 kg
Komunikační vzdálenost BT:	1 m
Komunikační vzdálenost IR:	0,3 m
Paměť přístupů:	100
Provozní teplota:	-30°C až 75°
Výdrž baterie:	minimálně 6 let

Obrázek 20. Supra iBox BT

4.1.2 ECKey

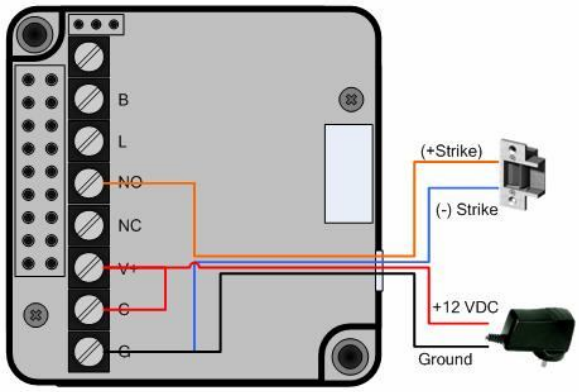
ECKey je společnost zabývající se využitím mobilního telefonu s podporou Bluetooth jako klíče k otevírání dveří, garážových vrat a jiných elektrických zámků. Zařízení stačí nainstalovat k zámkovému systému a spárovat jej s mobilním telefonem. Při následném přiblížení telefonu ke dveřím jednotka ECKey sepne relé a uživatel tak může vstoupit do objektu bez nutnosti hledání správného klíče či manipulace s kartou, aniž by vytáhl telefon s kapsy. Další výhodou je skutečnost, že zařízení je bezpečně umístěno v objektu a není tak nutné řešit odolnost vůči počasí nebo mechanickému poškození vandaly. V nabídce společnosti najdeme několik typů těchto zařízení, lišících se především technickými parametry a způsobem využití.

EK2 – virtual keypad

Funkce jednotky EK2 je podobná jako funkce klávesnice umístěné u vstupních dveří objektu. Vždy když se s spárovaným mobilním telefonem přiblížíme na definovanou vzdálenost, na displeji se objeví požadavek na zadání PIN kódu. V případě že je zadán správný kód, EK2 otevře dveřní zámek. Po uplynutí tří sekund jsou dveře opět zamčeny. Zařízení nevyžaduje instalaci žádných aplikací na mobilním telefonu. [17]

Vlastnosti:

Napájecí napětí:	12/24 V DC
Pohotovostní odběr:	20 mA
Zatížení relé:	5A / 12V
Délka pinu:	1 – 8 znaků
Komunikační vzdálenost BT:	nastavitelná 1 – 10 m
Výstupy:	Common, N/C, N/O
Rozměry:	50 x 70 x 20 mm



Obrázek 21. EK2 - schéma zapojení

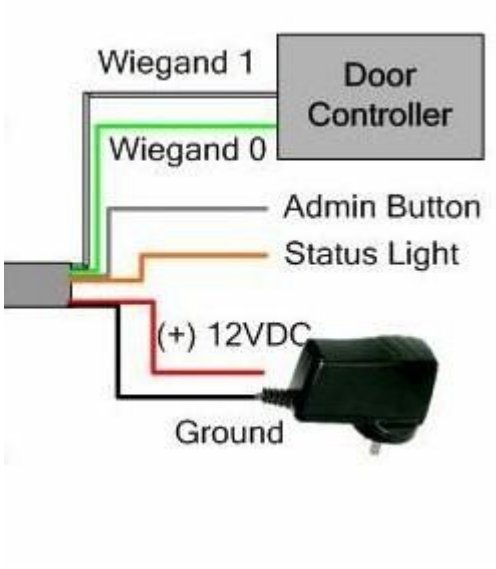
Obrázek 22. Jednotka EK2

EK5 - Access Control Leader

Jednotka EK5 funguje jako čtečka bezpečnostních karet. Z unikátní adresy Bluetooth jednotky vytváří kód ID karty a komunikuje přes standardní „wiegand protokol“. Mobilní telefon s Bluetooth v tomto případě zastupuje bezpečnostní kartu a společnosti tak odpadají problémy s distribucí a správou těchto karet. Nastavení umožňuje „hands free“ přístup nevyžadující manipulaci s telefonem, nebo přístup po zadání platného PIN kódu na klávesnici telefonu. [17]

Vlastnosti:

Napájecí napětí:	12 V DC
Pohotovostní odběr:	15 mA
Komunikační vzdálenost BT:	nastavitelná 1 – 10 m
Výstupy:	Wiegand 26/28 bit
Rozměry:	100 x 35 x 20 mm



Obrázek 23. EK5 - schéma zapojení

Obrázek 24. Jednotka EK5

4.1.3 Nio

Toto zařízení od společnosti Tenbu slouží k hlídání zavazadel, notebooku, klíčů a jiných věcí, které s sebou běžně člověk nosí. Nio se spáruje s mobilním telefonem a pomocí aplikace v něm nainstalované se nastaví možnosti střežení, jako způsob varování nebo maximální dovolená vzdálenost mezi zařízeními. Pokud je tato hranice překonána, je na obou zařízeních signalizován poplach. Zařízení tedy chrání nejen před zapomenutím hlídaného předmětu, ale také před jeho odcizením. Využít jej mohou i rodiče v situacích kdy se s dětmi pohybují v davu, nebo když jsou zaneprázdněni a mohou ztratit přehled o dětech. Nio je kompatibilní s telefony s operačním systémem Black Berry, Windows mobile, Android, Symbian nebo s podporou Javy. [19]

Vlastnosti:

Nastavitelná vzdálenost: 2 – 25 m

Max. počet současný zařízení: 5

Konektor nabíjení: miniUSB

Doba nabíjení: 40 minut

Obrázek 25. Nio - možnosti využití

4.2 Navrhovaný způsob využití

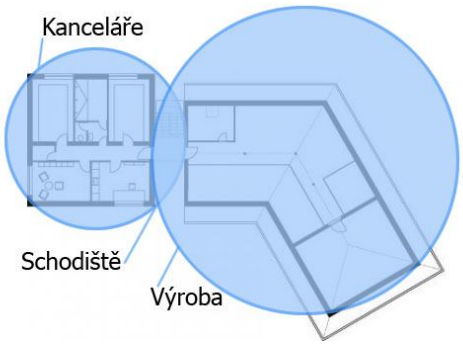
4.2.1 Bluetooth lokalizace

Podobně jako může mobilní operátor zjistit přibližnou polohu aktivního mobilního telefonu, může být určena i přibližná pozice zařízení s aktivním Bluetooth. Telefonní číslo je ale v tomto případě nahrazeno unikátní adresou Bluetooth jednotky. Přesnost vypočítané polohy by závisela pouze na hustotě Bluetooth vysilačů. Tento systém může být nasazen v budovách a ve větším měřítku i areálech, nebo dokonce městech. Jeho výhodou je především nezávislost na službách mobilního operátora a GPS. Sledovaným předmětem může být jakékoli zařízení s technologií Bluetooth, což nám umožní používat k tomuto účelu mobilní telefon, a není proto nutná distribuce dalších zařízení.

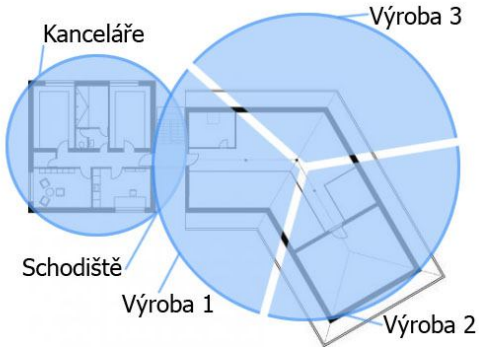
4.2.1.1 Princip určení pozice

Systém by se skládal z několika přijímačů, které by v určitých intervalech skenovali okolí a adresy nalezených Bluetooth zařízení by se zapisovaly do databáze spolu s časem a identifikačním číslem přijímače. Pokud by bylo zařízení zachyceno dvěma nebo více vysilači zároveň, určení jeho polohy by bylo ještě přesnější. Technologie Bluetooth umožňuje měřit sílu signálu, ovšem tento ukazatel je natolik nepřesný, že jej pro určování polohy není možné použít. Dalším možným řešením by byla instalace více přijímačů v jednom bodě, z nichž každý by pokrýval pouze určitý sektor (Obr 27). Toho by se docílilo použitím sektorové antény. Přesnost je tedy přímo úměrná počtu rozmístěných přijímačů. Na obrázku (Obr. 28) je znázorněna instalace tohoto sytému, umožňující určení místnosti, ve které se sledované zařízení nachází.

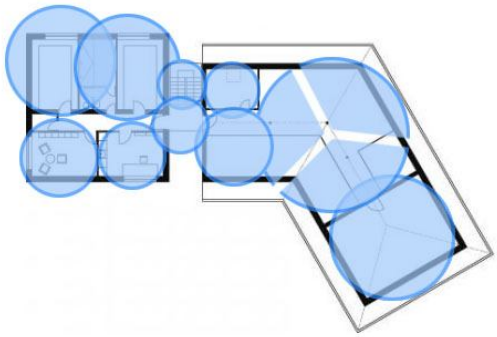
Jako zařízení, které by bylo sledováno a jednoznačně by tak identifikovalo osobu, by mohl být použit mobilní telefon, nebo speciální přívěšky s jednotkou Bluetooth. Díky nízké spotřebě kterou se pyšní specifikace 4.0, by takový přívěšek vydržel fungovat rok na knoflíkovou baterii.



Obrázek 26. Lokalizace – dva přijímače



Obrázek 27. Lokalizace – použití sektorů



Obrázek 28. Lokalizace – použití více přijímačů

4.2.1.2 Využití

V rozsáhlých budovách a areálech najdeme pro takový systém spoustu využití. Může například sloužit jako dohled nad zaměstnanci. Zaměstnavatel by tak měl přehled o pohybu pracovníků během celého dne. Tyto informace by pak mohli sloužit nejen ke kontrole zda pracovník netráví příliš moc času na toaletách nebo v šatně, ale mohli by tak sloužit jako důkazní materiál v případě způsobení škody na výrobním stroji, výrobku či jiném majetku firmy.

Tento systém by dále našel uplatnění při evakuaci a jiných situacích, kdy je potřeba vyklidit budovu a zjistit zda se v ní už nikdo nevyskytuje. V případě havárie by tak záchranný tým nemusel prohledávat budovu pokud by v ní systém neregistroval žádného uživatele. Kdyby naopak všichni uživatelé nestihli opustit budovu, dostali by alespoň záchranáři informace o přibližné poloze a počtu osob v objektu.

Možná by byla také spolupráce s poplachovým zabezpečovacím systémem. Pokud by se v blízkosti střežené místnosti pohybovala oprávněná osoba, byla by tato místnost dočasně odstřežena, aby při vstupu do ní nebyl vyvolán poplach. Jednotlivým uživatelům by tak byla přidělena práva, na jejichž základě by systém vyhodnocoval, zda bude po vstupu do místnosti vyhlášen poplach či nikoliv.

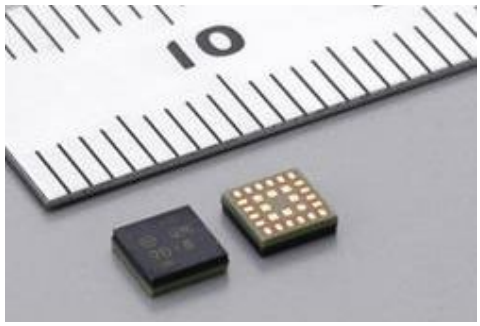
4.2.1.3 Použití ve větším měřítku

Systém pro určování pozice pomocí technologie Bluetooth by ve větším měřítku bylo možné použít ve městech, případně i v celé zemi. Náklady na zřízení takového systému by ovšem byly velmi vysoké. Na obrázku (Obr. 29) je k pokrytí větší části města Zlína použito 22 přijímačů s dosahem jeden kilometr.

Obrázek 29. Lokalizace - použití ve městě

Možným řešením by byla instalace více přijímačů s malým dosahem v městech a poblíž hlavních dopravních tepen. Naopak v neobydlených oblastech by se nacházelo méně přijímačů s velkým dosahem.

Způsobů využití takového systému je celá řada. Díky miniaturním rozměrům, nízké energetické náročnosti a nízké ceně by Bluetooth jednotka mohla být umístěna do všech předmětů jejichž pohyb chceme sledovat. Takovým předmětem může být poštovní balík, automobil či drahé vybavení bytu, které by v případě vloupání mohlo být odcizeno. Nalezení takto odcizeného předmětu by netrvalo nijak dlouho. K přesnému zaměření by mohl být použit přenosný přijímač s volitelným dosahem. K informacím o poloze by měl přístup pouze majitel tohoto zařízení. Takovýto systém by ale mohl být velmi snadno zneužit ke sledování osob a Bluetooth jednotka by se tak vkládala do kapsy podobně jako štěnice.



Obrázek 30. Nejmenší Bluetooth modul (3,5 x 3,5 x 1 mm)

Vzhledem k zřizovacím nákladům a rizikům ztráty soukromí není příliš pravděpodobné, že by systém určování polohy pomocí technologie Bluetooth byl někdy použit v takovém velkém měřítku.

5 MAXIMÁLNÍ DOSAH BLUETOOTH

5.1 Úprava Bluetooth adaptéru

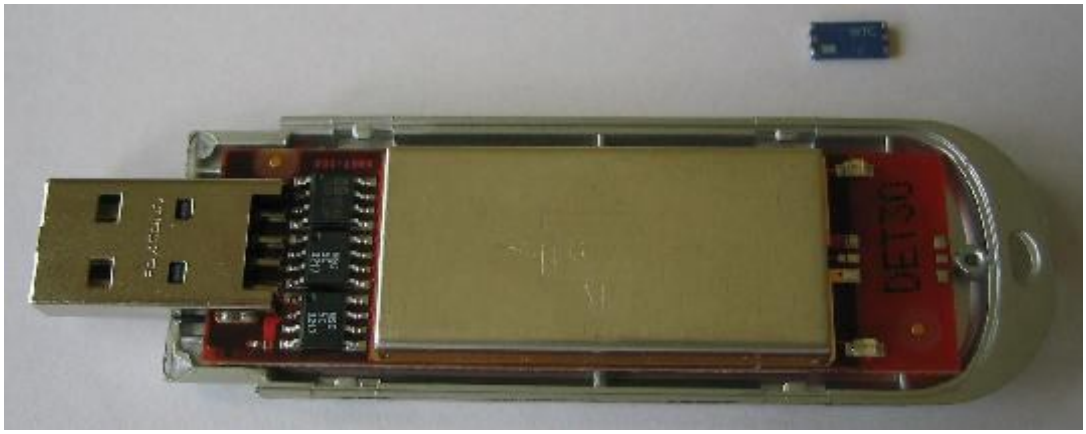
Standardní adaptér třídy jedna má pod plastovým krytem malou vnitřní anténu s jejíž pomocí dokáže komunikovat s dalším zařízením Bluetooth až na vzdálenost 100 m. Avšak maximální dosah adaptéru může rapidně vzrůst po nahrazení originální antény externí anténou pro frekvenční pásmo 2,4 GHz. Takové antény jsou běžně používány při budování WiFi sítí. Ještě většího výkonu je možné dosáhnout přidáním RF zesilovače. Maximální dosah takto upraveného adaptéru pak závisí především na zisku přidané antény a také na třídě druhé Bluetooth jednotky. K testu byly použity následující zařízení.

- USB 2.0 Bluetooth adaptér MSI-6967: Bluetooth v1.1 (Třída 1)
- Pocket PC LG Expo: Bluetooth 2.1 + EDR (Třída 2)

5.1.1 Postup

Na obrázku (Ob. 30) je Bluetooth adaptér bez plastového krytu. V zadní části se nachází malá SMT anténa o velikosti přibližně 3 x 5 mm. Anténa je připájena na obou koncích třemi vývody. Ty co se nacházejí dále od USB konektoru slouží pouze k upevnění antény. Zbylé tři slouží k vedení signálu, z nichž krajní dva jsou uzemnění.

Obrázek 31. MSI-6967 bez krytu



Obrázek 32. MSI-6967 po odstranění SMT antény

Na místo původní antény byl do předvrtaných děr připevněn MMCX pigtail a připájen k odpovídajícím vývodům adaptéru.

Obrázek 33. MSI-6967 po připojení konektoru externí antény

Obrázek 34. MSI-6967 po opětovném složení

5.1.2 Výsledky měření

Originální SMT anténa

Bez jakýchkoliv úprav adaptéru bylo možné druhé zařízení „vidět“ na vzdálenost 25 m. Toto je typická maximální vzdálenost pro komunikace mezi zařízením první třídy a zařízením s nižší třídou. Skenovací oblast originálního Bluetooth adaptéru je tedy přibližně 1964 m^2.

Všesměrová anténa 12 dBi

S použitím 12 dBi 38 cm vysoké externí antény se maximální možná vzdálenost pro komunikaci mezi zařízeními zvýšila na 85 m. Skenovací oblast takto upraveného adaptéru je přibližně 22 700 m^2.

Parabolická anténa – síto 24 dBi

S připojenou parabolickou anténou s ziskem 24 dBi byla maximální naměřená vzdálenost 275 m. Tomuto údaji odpovídá skenovací oblast o obsahu 237 580 m^2.

5.2 AIRcable Host XR3

Samozřejmě existují také profesionální Bluetooth adaptéry s vysokým výkonem, takových zařízení ale není mnoho. Jedním z nich je zařízení Host XR3 od společnosti AIRcable. Tento extrémně citlivý Bluetooth vysílač dokáže při použití 9 dBi antény komunikovat s druhým zařízením na vzdálenost 2 km. S použitím 18 dBi se maximální vzdálenost zvýší až na 10 km. Dosah závisí také na výkonu Bluetooth vysilače druhého zařízení. Při dodržení zásad profesionální instalace a s použitím 24 dBi externí parabolické antény udává výrobce maximální dosah až 30 km za dobrých podmínek. [20]

Vlastnosti

Podporované OS:	Windows, Liux, Mac OS
Rozměry:	70 x 57 x 15 mm
Napájení:	z USB, 5V, 300mA
Konektor antény:	RP-SMA
Bluetooth:	2.1 + EDR
Provozní teplota:	-40°C až 85°

Obrázek 35. Aircable Host XR3

6 BEZPEČNOSTNÍ ZÁSADY PŘI POUŽÍVÁNÍ BLUETOOTH

Z popsaných nedostatků v zabezpečení technologie Bluetooth a jiných bezpečnostních chyb vyplývají tyto zásady, při jejichž dodržení je komunikace prostřednictvím této technologie bezpečná a riziko odposlouchávání či neoprávněného přístupu k informacím je sníženo na minimum.

6.1 Bezpečnost pikosítí

- Ujistěte se, že uživatelé pikosítě jsou si vědomi bezpečnostních rizik a odpovědnosti související s používáním technologie Bluetooth.
- V pravidelných intervalech provádět komplexní posouzení bezpečnosti Bluetooth.
- Většina zařízení umožňuje aktualizaci firmware, aby mohli být odstraněny případné bezpečnostní chyby. Je nutné kontrolovat zda nejsou dostupné nové aktualizace.
- Bluetooth zařízení mohou podporovat i jiné bezdrátové technologie, umožňující připojení do pikosítě. Ujistěte se, že i tyto technologie jsou dobře zabezpečeny.
- Měl by být veden seznam všech zařízení a adres jejich Bluetooth modulu. Tento seznam bude následně použit při provádění auditu a bude tak možné zjistit neoprávněné používání Bluetooth.
- Výchozí nastavení zařízeních podporujících Bluetooth často nebývá bezpečné. Mělo by se tedy zajistit aby bylo v souladu s bezpečnostní politikou společnosti.
- Pokud to umožňuje nastavení zařízení, výkon vysílače by měl být nastaven na nejnižší možnou hodnotu, dostačující na pokrytí požadovaného prostoru.
- PIN kódy používané v párovacím procesu by měly mít největší možnou podporovanou délku a měly by být náhodně generované.
- Ujistěte se že při komunikaci je jako klíč spojení použit kombinační klíc namísto klíče zařízení.
- Většina Bluetooth zařízení podporuje více profilů a služeb. Povoleny by ovšem měly být pouze potřebně profily a služby.

- S výjimkou párovacího procesu by jednotky Bluetooth měly být nastaveny do nezjistitelného módu. Jména zařízení by měla být volena tak, aby neumožňovaly identifikaci typu a modelu zařízení.
- Pro přenos citlivých informací by mělo být použito zabezpečení na aplikační vrstvě.
- Spárované zařízení má přístup do pikosítě bez nutnosti další autentizace. Proto by i samotná zařízení měla být chráněna autentizaci, aby se zabránilo neoprávněnému připojení do sítě s kradeným zařízením.
- V případě že není funkce Bluetooth používána, měla by být úplně vypnuta.
- Proces párování by měl být prováděn v bezpečném prostředí bez přístupu veřejnosti. Uživatel by zároveň neměl reagovat na nečekaný požadavek na zadání PIN kódu.
- V případě že je spárované zařízení ztraceno či odcizeno, ostatní uživatelé by jej měly okamžitě odstranit ze seznamu důvěryhodných zařízení.

6.2 Bezpečnost handsfree

- V obou zařízeních by měla být specifikace Bluetooth ve verzi 1.2 nebo novější. V těchto verzích se už jako klíč spojení nepoužívá klíč zařízení. Dále je také od verze 1.2 podporována metoda FHSS, která značně ztěžuje odposlouchávání.
- Výkon jednotky Bluetooth v handsfree by měl odpovídat třídě 2 nebo 3. Vyšší výkon vysilače umožní útočníkovi odposlouchávání na delší vzdálenost.
- Zařízení typu headset by měla být stále v nezjistitelném režimu, protože zjištění adresy jednotky a offsetu vnitřních hodin je vždy prvním krokem útoku. Zařízení by mělo podporovat jen služby vyžadované pro použití jako headset.
- Zařízení by měla podporovat jen jedno spojení typu headset mezi náhlavní soupravou a telefonem.
- Pokud není headset spárován s mobilním telefonem měl by být vypnut. Toto opatření znemožní útočníkovi odposlouchávání metodou Car Whisperer.
- Vyhněte se používání headsetů pro jejichž spárování s mobilním telefonem je používán pevně daný PIN „0000“ nebo „1234“.

ZÁVĚR

Přestože je v práci popsáno několik metod útoku, technologie Bluetooth se mi jeví jako bezpečný způsob komunikace, za předpokladu že jsou dodrženy všechny bezpečnostní zásady uvedené v závěru praktické části. Bezpečnostní chyby, které jsou pro tyto útoky zneužívány, vznikly chybnou implementací této technologie v cílovém zařízení. Tyto chyby byly většinou odstraněny v další verzi firmware. Aktualizaci si ovšem uživatel musel provézt sám a často se o závažnosti vzniklé situace ani nedozvěděl. Proto není neobvyklé, když na tyto mobilní telefony s původní verzí firmware, narazíme ještě dnes.

Výrobci mobilních telefonů často prodávají zařízení, která mají aktivní Bluetooth v zjistitelném módu již od prvního spuštění. Nezkušený uživatel tak ani nemusí vědět k čemu tato funkce slouží a že ji má trvale zapnutou. Tito uživatelé se pak mohou stát snadným cílem útočníka a nevědomě mu tak poskytnout obsah telefonního seznamu, v horším případě i údaje k bankovnímu účtu.

V době vzniku této bakalářské práce nebyla specifikace ve verzi 3.0 a 4.0 zdaleka tak rozšířená, jako právě verze 2.1+EDR, kterou se především zabývá. I když s sebou verze 4.0 přináší podporu šifrování AES, stále budou ještě používány zařízení s implementovanou starší verzí tohoto standardu. V penetračních testech by tak technologie Bluetooth neměla být ani v příštích letech opomíjena.

Stejně jako každá bezdrátová technologie, i Bluetooth s sebou nese jistá rizika. Většinou jsou ale způsobena nedostatečnou informovaností samotného uživatele. Přestože je proudová šifra E_0 slabá, v kombinaci s metodou přenosu v rozprostřeném spektru je její prolomení prakticky nemožné, za předpokladu že útočník nezachytil celý proces párování obou zařízení.

Masové rozšíření technologie Bluetooth způsobilo, že se sní setkáváme i v oblastech, pro které nebyla vůbec navržena, a používána je přitom způsobem, se kterým vývojáři rovněž nepočítali. Příkladem mohou být výrobky společnosti ECKey. Vzhledem k počtu zařízení s technologií Bluetooth, nízké ceně, miniaturním rozměrům, nízké energetické náročnosti a univerzálnosti je tedy jisté, že tato technologie bude ještě dlouhou dobu nejpoužívanější bezdrátovou technologií pro přenos dat na krátkou vzdálenost.

ZÁVĚR V ANGLIČTINĚ

Although the work described several methods of attack, Bluetooth seems to me to be a safe way of communication, provided it complies with all the security principles listed at the end of a practical part. Security issues that these attacks are abused, occurred due to incorrect implementation of this technology in the target device. These issues have been mostly removed in the next firmware. Therefore, it is not uncommon for these mobile phones with original firmware version, we face today.

Mobile phone manufacturers often sell devices that have an active Bluetooth device in discoverable mode, from the first run. The inexperienced user so not even know what this feature is used and that it is permanently enabled. These users can then become an easy target for the attacker and unknowingly provide him the content of the phone book or worse, bank account details.

At the time this bachelor thesis was the specification version 3.0 and 4.0, nearly so widespread as being version 2.1 + EDR, which mainly deals with. Although version 4.0 supports AES encryption, a device with an older version will still be used. Bluetooth technology in the coming years should not be left out of penetration tests.

Like any wireless technology, Bluetooth introduces a number of security vulnerabilities. But mostly due to insufficient awareness of the user. Although the stream cipher E_0 is weak, in combination with the method of transmission in the spread spectrum is it almost impossible to break, assuming that the attacker did not capture whole pairing process.

Due to the number of devices with Bluetooth technology, low cost, miniature size, low power cost and versatility it is certain that this technology will be a long time the most widely used short distance wireless technology.

SEZNAM POUŽITÉ LITERATURY

[1] GEHRMANN, Christian; PERSSON, Joakim; SMEETS, Ben. *Bluetooth Security.* Norwood : ARTECH HOUSE, 2004. 204 s. ISBN 1-58053-504-6.

[2] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace*. Brno : CP Books, a.s., 2005. 184 s. ISBN 80-251-0791-4.

[3] SVOBODA, J. *Principy a perspektivy technologie Bluetooth. Sdělovací technika*. 2004, roč. 52, č. 8, s. 3-6. ISSN 0036-9942.

[4] ČÁNSKÝ, Jiří . *Bluetooth* [online]. 2006. 4 s. Semestrální práce. České vysoké učení technické, Elektrotechnická fakulta . Dostupné z WWW: <http://radio.feld.cvut.cz/personal/mikulak/MK/MK06_semestralky/Bluetooth_CanskyJ.pdf>.

[5] PENN, Ivo. *Bezdrátová Bluetooth technologie* [online]. 2005. 6 s. Semestrální práce. Technická Univerzita Ostrava, Fakulta elektrotechniky a informatiky. Dostupné z WWW: <http://fei1.vsb.cz/wofex/2003/paper/p2612/penn_ivo.pdf>.

[6] SCARFONE, Karen; PADGETTE, John. *Guide to Bluetooth Security* [online]. Gaithersburg : National Institute of Standards and Technology, 2008 [cit. 2011-05-22]. Dostupné z WWW: <http://bluetooth-pentest.narod.ru/doc/guide_to_bluetooth_security.pdf>.

[7] BECKER, Andreas. *Bluetooth Security & Hacks*. 2007. 28 s. Seminární práce. Ruhr-Universität Bochum.

[8] *Palowireless* [online]. 2007 [cit. 2011-05-22]. Bluetooth Glossary. Dostupné z WWW: <http://www.palowireless.com/infotooth/glossary.asp>.

[9] *Wikipedie otevřená encyklopedie* [online]. 2000 [cit. 2011-05-22]. Dostupné z WWW: <http://cs.wikipedia.org>.

[10] *The Official Bluetooth SIG Member Website* [online]. 2001 [cit. 2011-05-22]. Dostupné z WWW: <https://www.bluetooth.org>.

[11] *PCWorld* [online]. 2009 [cit. 2011-05-22]. Základy technologie Bluetooth: komunikace a zabezpečení. Dostupné z WWW:

<http://pcworld.cz/hardware/Zaklady-technologie-Bluetooth-komunikace-a-zabezpeceni-6636>.

[12] *PCWorld* [online]. 2009 [cit. 2011-05-22]. Základy technologie Bluetooth: původ a rozsah funkcí. Dostupné z WWW: <http://pcworld.cz/hardware/Zaklady-technologie-Bluetooth-puvod-a-rozsah-funkci-6635>.

[13] *Trifinite.org* [online]. 2004 [cit. 2011-05-22]. Dostupné z WWW: <http://trifinite.org/>.

[14] *Airdump.cz* [online]. 2007 [cit. 2011-05-22]. Bluetooth – Bluejacking a Bluesnarfing. Dostupné z WWW: <http://airdump.cz/bluetooth-bluejacking-bluesnarfing/>.

[15] *A day with Tape* [online]. 2010 [cit. 2011-05-22]. Bluetooth mayhem . Dostupné z WWW: <http://adaywithtape.blogspot.com/2010/09/bluetooth-mayhem.html>.

[16] *A day with Tape II* [online]. 2010 [cit. 2011-05-22]. Bluetooth mayhem part II . Dostupné z WWW: <http://adaywithtape.blogspot.com/2010/09/bluetooth-mayhem-part-ii.html>.

[17] *ECKey - Turn your phone into a key* [online]. 2005 [cit. 2011-05-22]. Dostupné z WWW: <http://www.eckey.com/>.

[18] *Jablotron* [online]. 2008 [cit. 2011-05-22]. JA-80BT bluetooth adaptér. Dostupné z WWW: <http://www.jablotron.cz/cz/Katalog/zabezpeceni+domu/oasis+868mhz/prislusenstvi/ja80bt+bluetooth+adapter/>.

[19] *Nio - know it* [online]. 2009 [cit. 2011-05-22]. Dostupné z WWW: <http://www.bluenio.com/>.

[20] *AIRcable* [online]. 2010 [cit. 2011-05-22]. AIRcable - Long Range Bluetooth Devices. Dostupné z WWW: <http://www.aircable.net/products/host-xr3.php>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACL *Asynchronous Connection-Less*

Asynchronní bezspojově orientovaný provozní kanál

AES *Advanced Encryption Standard*

Pokročilý šifrovací standard. Jedná se o symetrickou proudovou šifru.

AM_ADDR *Active Member Address*

Adresa aktivního člena, umožňující adresování podřízených jednotek.

ARQN *Automatic Repeat Request Numer*

Indikace potvrzení, sloužící k informování o správném doručení paketu.

AT *ATtention*

AT příkazy slouží k řízení a konfiguraci sériových telefonních modemů.

BD_ADDR *Bluetooth Device Address*

Unikátní adresa Bluetooth jednotky

CRC *Cyclic Redundancy Check*

Cyklický redundantní součet je hašovací funkce, sloužící k detekci chyb.

DC *Direct Current*

Stejnosměrný elektrický proud

FEC *Forward Error Check*

Dopředná kontrola chyb

FHSS *frequency hopping spread spektrum*

Metoda přenosu v rozprostřeném spektru

GFSK *Gaussian Frequency-Shift Keying*

Gaussovská modulace s frekvenčním klíčováním

GPS *Global Positioning Systém*

Globální družicový polohový systém pro určení pozice na zemi.

GSM *Groupe Spécial Mobile*

Globální systém pro mobilní komunikaci

HCI *Host Controller Interface*

Hostitelské řídící rozhranní

ISM *Industrial, Scientific and Medical*

Volná pásma pro rádiové vysílání v oborech průmyslovém, vědeckém a zdravotnickém. Pásma bez licenčních poplatků a bez garance proti rušení.

L2CAP *Logical Link Control and Adaptation Protocol*

Protokole pro řízení a adaptaci logických spojení

LAP *Lower Address Part*

Dolní část významové části adresy Bluetooth jednotky.

LC *Link Kontrol*

Logický řídicí kanál pro řízení spojení

LM *Link Manager*

Logický řídicí kanál pro správu spojení

LMP *Link Manager Protocol*

Protokol pro správu spojení

MMCX *micro-miniature coaxial*

Menší verze MCX konektoru. Používá se pro externí GPS a Wi-Fi antény v menších zařízeních (PDA, notebook).

MP3 *Motion Picture experts group - layer 3 (MPeg layer 3)*

Komprimovaný zvukový soubor založený na principu ořezávání frekvenčních složek v neslyšitelném pásmu.

N/C *Normally-closed*

N/C relé je v klidu sepnuté a při aktivaci dojde k rozepnutí.

N/O *Normally-open*

N/O relé je v klidu rozepnuté a při aktivaci dojde k sepnutí.

NAP *Non-significant Address Part*

Nevýznamová část adresy Bluetooth jednotky.

OBEX *Object Exchange Protocol*

Komunikační protokol, který umožňuje výměnu objektů mezi zařízeními

PAN *Personal Area Network*

Osobní počítačová síť tvořená komunikujícími zařízeními jako mobilní telefon, PDA nebo laptop, která jsou v blízkosti jedné osoby.

PIN *Personal Identification Numer*

Tajné číslo jehož znalost opravňuje osobu k využití chráněné služby.

PSTN *Public Switched Telephone Network*

Veřejná telefonní síť

RF *Radio Frequency*

RF zesilovač - Radio-frekvenční zesilovač.

RFCOMM *Radio Frequency Communications port*

Radio-frekvenční komunikační port emulující sériové rozhraní RS232.

RS232 *Recommended Standard 232*

Komunikační rozhraní osobních počítačů a další elektroniky umožňující propojení a vzájemnou sériovou komunikaci dvou zařízení.

SCO *Synchronous Connection-Oriented*

Synchronní spojově orientovaný provozní kanál

SDP *Service Discovery Protocol*

Protokol pro zjišťování služeb

SMS *Short Message Service*

Služba krátkých textových zpráv

SMT *Surface Mounted Technology*

	Technologie povrchové montáže
TCP/IP	*Transmission Control Protocol/Internet Protocol*
	Primární transportní protokol - TCP/protokol síťové vrstvy – IP. Rodina protokolů TCP/IP obsahuje sadu protokolů pro komunikaci v síti.
TCS	*Telephony Control protocol Specification*
	Protokol pro řízení telefonie
UA	*User Asynchronous data*
	Uživatelský kanál asynchronních dat
UAP	*Upper Address Part*
	Horní část významové části adresy Bluetooth jednotky.
UI	*User Isochronou data*
	Uživatelský kanál izochronních dat
US	*User Synchronous data*
	Uživatelský kanál synchronních dat
USB	*Universal Serial Bus*
	Univerzální sériová sběrnice pro připojení periferií k počítači.

SEZNAM OBRÁZKŮ

SEZNAM PŘEVZATÝCH OBRÁZKŮ

SEZNAM TABULEK